ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ADVOCACIA JOSÉ DEL CHIARO
BAKER & MCKENZIE, WONG & LEOW
BIRD & BIRD
CLEY GOTTLEIB STEEN & HAMILTON LLP
CMS RUSSIA
ELVINGER HOSS PRUSSEN
HOGAN LOVELLS BSTL, SC
LATHAM & WATKINS LLP
LEE AND LI, ATTORNEYS-AT-LAW
SORAINEN
TRAPLE KONARSKI PODRECKI & PARTNERS
URÍA MENÉNDEZ
WEBB HENDERSON
ZHONG LUN LAW FIRM
# CONTENTS

PREFACE........................................................................................................................................................... v

*John P Janka*

LIST OF ABBREVIATIONS............................................................................................................................... vii

Chapter 1  AUSTRALIA.................................................................................................................................................. 1

*Angus Henderson, Richard Dampney and Irene Halfory*

Chapter 2  BELARUS............................................................................................................................................... 25

*Kirill Laptev and Pavel Lashuk*

Chapter 3  BRAZIL.................................................................................................................................................. 36

*Ademir Antonio Pereira Junior, Luiz Felipe Rosa Ramos and Yan Villela Vieira*

Chapter 4  CHINA............................................................................................................................................... 47

*Jihong Chen*

Chapter 5  ESTONIA.............................................................................................................................................. 59

*Mihkel Miidla, Liisa Maria Kuuskmaa and Oliver Kuusk*

Chapter 6  EU OVERVIEW................................................................................................................................... 79

*Marco D’Ostuni, Gianluca Faella and Manuela Becchimanzi*

Chapter 7  FRANCE.............................................................................................................................................. 99

*Myria Saarinen and Jean-Luc Juhan*

Chapter 8  ITALY.................................................................................................................................................. 117

*Marco D’Ostuni, Marco Zotta and Manuela Becchimanzi*

Chapter 9  JAPAN............................................................................................................................................... 140

*Hiroki Kobayashi, David Lai and Takaki Sato*
Chapter 10  LATVIA.............................................................................................................................. 161  
Andris Tauriņš and Madara Meļņika

Chapter 11  LITHUANIA..................................................................................................................... 179  
Stasys Drazdauskas

Chapter 12  LUXEMBOURG............................................................................................................... 189  
Linda Funck

Chapter 13  MEXICO .......................................................................................................................... 214  
Federico Hernández Arroyo

Chapter 14  POLAND......................................................................................................................... 226  
Xawery Konarski and Michał Matysiak

Chapter 15  RUSSIA.......................................................................................................................... 236  
Maxim Boulba and Elena Andrianova

Chapter 16  SINGAPORE................................................................................................................... 248  
Ken Chia and Daryl Seetoh

Chapter 17  SPAIN............................................................................................................................. 272  
Pablo González-Espejo and Nerea Sanjuan

Chapter 18  TAIWAN.......................................................................................................................... 288  
Patrick Marros Chu, Vick Chien and Sam Huang

Chapter 19  UNITED ARAB EMIRATES ....................................................................................... 299  
David Bintliff, Lena El-Malak, Christopher Ekland, Mayowa Olusola, and Ayah Abdin

Chapter 20  UNITED KINGDOM......................................................................................................... 312  
John D Colahan, Gail Crawford and Lisbeth Savill

Chapter 21  UNITED STATES.............................................................................................................. 365  
John P Janka, Matthew T Murchison, and Michael H Herman

Appendix 1  ABOUT THE AUTHORS............................................................................................... 387  

Appendix 2  CONTRIBUTORS’ CONTACT DETAILS........................................................................... 405
As it has since inception, this tenth edition of The Technology, Media and Telecommunications Review provides a survey of evolving legal constructs in 21 jurisdictions around the world. It remains a business-focused framework rather than a legal treatise, and strives to provide a general overview for those interested in evolving law and policy in the rapidly changing TMT sector.

More than ever, broadband connectivity goals are the focus of policymakers and are driving law and policy in this sector. New technologies and new ways of connecting people call for decision-makers to move away from old paradigms and embrace new ones. Indeed, facilitating digital inclusion, extending the economic and social benefits of connecting all citizens, and growing local economies by ensuring that affordable connectivity is available, are universal goals that require bold decisions and new approaches.

New expectations of being connected everywhere, and at all times, are driving the development of broadband service on aeroplanes, vessels, motor vehicles and trains, to support the needs of passengers, crew and the airlines themselves as they move to digitise their fleets and transmit the massive amounts of operational data generated by today’s aircraft. Accommodating these new mobility services create pressures on the existing spectrum environment. And the different technologies that seek to meet these mobility needs are not always compatible with one another. As a result, regulators (1) sometimes provide more flexibility to allow spectrum to be used to provide a broader range of services, and (2) sometimes ‘reform’ existing spectrum bands so that new services and technologies can access spectrum previously set aside for other purposes.

The World Radio-communication Conference (WRC) of the International Telecommunication Union (ITU), being held this month in Sharm-El-Sheikh, will address many of these key issues, and make changes in some long-standing radio spectrum allocations, particularly the ‘millimetre-wave’ bands that offer the promise of providing untold amounts of capacity and even faster service speeds by a variety of technologies. As with most policy choices, the conference likely will include some political decisions. Indeed, political pressures already exist around the world in decisions being made by national regulators outside of the ITU process.

Many governments are investing in or subsidising broadband networks to ensure that their citizens can participate in the global economy, and have universal access to the vital information, educational, health-related and entertainment services now available over the internet. Many governments are re-evaluating how to regulate broadband providers, whose networks have become essential to daily life. However, many policymakers still have not solved the problem caused when their incumbent service providers fail to extend service to all of their citizens for business reasons – because those businesses deem ‘unprofitable’ those
who are the hardest to serve. Curiously, policymakers sometimes exacerbate this failure by resorting to spectrum auctions to award the right to provide service in a given frequency band to the highest bidder, failing to require service availability to everyone in the auctioned area, and then making the auction winner the gatekeeper for anyone else who wants to use the same spectrum. Too often, decisions are based (explicitly or implicitly) on expected auction revenues, which consumers end up paying for in the end through higher costs of service. But even this may start to change as the wireless providers who once relished auctions are coming to realise that the price they have to pay via auctions is just too high.

Far too infrequently do policymakers factor in the benefits of ensuring ubiquitous connectivity: new jobs, economic growth, security, social inclusion, and improvements in healthcare, education and food production, to name a few. Indeed, treating spectrum as a property right rather than as the valuable public resource it is often leads to undesirable results in the marketplace.

Convergence, vertical integration and consolidation can also lead to increased focus on competition and, in some cases, to changes in the government bodies responsible for monitoring and managing competition in the TMT sector. Similarly, many global companies now are able to focus their regulatory activities outside their traditional home base, and in jurisdictions that provide the most accommodating terms and conditions.

Changes in the TMT ecosystem, including increased opportunities to distribute video content over broadband networks, have led to policy focuses on issues such as network neutrality: the goal of providing stability for the provision of the important communications services on which almost everyone relies, while also addressing the opportunities for mischief that can arise when market forces work unchecked. While the stated goals of that policy focus may be laudable, the way in which resulting law and regulation are implemented has profound effects on the balance of power in the sector, and also raises important questions about who should bear the burden of expanding broadband networks to accommodate capacity strains created by content providers and to facilitate their new businesses.

The following chapters describe these types of developments around the world, as well as the liberalisation of foreign ownership restrictions, efforts to ensure consumer privacy and data protection, and measures to ensure national security and facilitate law enforcement. Many tensions exist among the policy goals that underlie the resulting changes in law. Moreover, cultural and political considerations often drive different responses at the national and the regional level, even though the global TMT marketplace creates a common set of issues.

I thank all of the contributors for their insightful contributions to this publication, and I hope you will find this global survey a useful starting overview of these fascinating developments in the TMT sector.

John P Janka
Latham & Watkins LLP
Washington, DC
November 2019
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G</td>
<td>Third-generation (mobile wireless technology)</td>
</tr>
<tr>
<td>4G</td>
<td>Fourth-generation (mobile wireless technology)</td>
</tr>
<tr>
<td>5G</td>
<td>Fifth-generation (mobile wireless technology)</td>
</tr>
<tr>
<td>ADSL</td>
<td>Asymmetric digital subscriber line</td>
</tr>
<tr>
<td>AMPS</td>
<td>Advanced mobile phone system</td>
</tr>
<tr>
<td>ARPU</td>
<td>Average revenue per user</td>
</tr>
<tr>
<td>BIAP</td>
<td>Broadband internet access provider</td>
</tr>
<tr>
<td>BWA</td>
<td>Broadband wireless access</td>
</tr>
<tr>
<td>CATV</td>
<td>Cable TV</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code division multiple access</td>
</tr>
<tr>
<td>CMTS</td>
<td>Cellular mobile telephone system</td>
</tr>
<tr>
<td>DAB</td>
<td>Digital audio broadcasting</td>
</tr>
<tr>
<td>DECT</td>
<td>Digital enhanced cordless telecommunications</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed denial-of-service</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial-of-service</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital subscriber line</td>
</tr>
<tr>
<td>DTH</td>
<td>Direct-to-home</td>
</tr>
<tr>
<td>DTTV</td>
<td>Digital terrestrial TV</td>
</tr>
<tr>
<td>DVB</td>
<td>Digital video broadcast</td>
</tr>
<tr>
<td>DVB-H</td>
<td>Digital video broadcast – handheld</td>
</tr>
<tr>
<td>DVB-T</td>
<td>Digital video broadcast – terrestrial</td>
</tr>
<tr>
<td>ECN</td>
<td>Electronic communications network</td>
</tr>
<tr>
<td>ECS</td>
<td>Electronic communications service</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced data rates for GSM evolution</td>
</tr>
<tr>
<td>FAC</td>
<td>Full allocated historical cost</td>
</tr>
<tr>
<td>FBO</td>
<td>Facilities-based operator</td>
</tr>
<tr>
<td>FCL</td>
<td>Fixed carrier licence</td>
</tr>
<tr>
<td>FTNS</td>
<td>Fixed telecommunications network services</td>
</tr>
<tr>
<td>FTTB</td>
<td>Fibre to the building</td>
</tr>
<tr>
<td>FTTC</td>
<td>Fibre to the curb</td>
</tr>
<tr>
<td>FTTN</td>
<td>Fibre to the node</td>
</tr>
<tr>
<td>FTTP</td>
<td>Fibre to the premises</td>
</tr>
<tr>
<td>FTTx</td>
<td>Fibre to the x</td>
</tr>
<tr>
<td>FWA</td>
<td>Fixed wireless access</td>
</tr>
</tbody>
</table>
List of Abbreviations

Gb/s  Gigabits per second
GB/s  Gigabytes per second
GSM  Global system for mobile communications
HDTV  High-definition TV
HITS  Headend in the sky
HSPA  High-speed packet access
IaaS  Infrastructure as a service
IAP  Internet access provider
ICP  Internet content provider
ICT  Information and communications technology
IoT  Internet of things
IPTV  Internet protocol TV
IPv6  Internet protocol version 6
ISP  Internet service provider
kb/s  Kilobits per second
kB/s  Kilobytes per second
LAN  Local area network
LRIC  Long-run incremental cost
LTE  Long Term Evolution (4G technology for both GSM and CDMA cellular carriers)
Mb/s  Megabits per second
MB/s  Megabytes per second
MMDS  Multichannel multipoint distribution service
MMS  Multimedia messaging service
MNO  Mobile network operator
MSO  Multi-system operator
M2M  Machine-to-machine
MVNO  Mobile virtual network operator
MWA  Mobile wireless access
NFC  Near field communication
NGA  Next-generation access
NIC  Network information centre
NRA  National regulatory authority
OTT  Over-the-top (providers)
PaaS  Platform as a service
PNETS  Public non-exclusive telecommunications service
PSTN  Public switched telephone network
RF  Radio frequency
SaaS  Software as a service
SBO  Services-based operator
SMS  Short message service
STD–PCOs  Subscriber trunk dialling–public call offices
UAS  Unified access services
UASL  Unified access services licence
UCL  Unified carrier licence
UHF  Ultra-high frequency
UMTS  Universal mobile telecommunications service

© 2019 Law Business Research Ltd
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USO</td>
<td>Universal service obligation</td>
</tr>
<tr>
<td>UWB</td>
<td>Ultra-wideband</td>
</tr>
<tr>
<td>VDSL</td>
<td>Very high speed digital subscriber line</td>
</tr>
<tr>
<td>VHF</td>
<td>Very high frequency</td>
</tr>
<tr>
<td>VOD</td>
<td>Video on demand</td>
</tr>
<tr>
<td>VoB</td>
<td>Voice over broadband</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over internet protocol</td>
</tr>
<tr>
<td>W-CDMA</td>
<td>Wideband code division multiple access</td>
</tr>
<tr>
<td>WiMAX</td>
<td>Worldwide interoperability for microwave access</td>
</tr>
</tbody>
</table>
I OVERVIEW

The TMT sectors in Australia are currently in the middle of several transitions, among the most significant of which is the transition to the wholesale-only, government-owned national broadband network: nbn™ network. This is creating a significant shift in the fixed telecommunications industry structure as Australia moves to a structurally separated model focused on services-based competition.

Convergence within the TMT sectors continues to take place, with traditional broadcast media facing increasing competition from OTT, on-demand media providers that use broadband networks to deliver their content. However, as outlined below, Australia retains separate regulatory regimes for broadcasting and telecommunications (despite having a converged regulator in the form of the Australian Communications and Media Authority (ACMA)).

II REGULATION

i The regulators

The ACMA, established in 2005, is the converged regulator for the internet, broadcasting, telecommunications and radiocommunications sectors. The key responsibilities of the ACMA include:

a licensing and regulating telecommunications carriers, carriage service providers and content service providers;
b licensing and regulating RF spectrum;
c regulating television and radio broadcasting, including content regulation;
d regulating telecommunications and radiocommunications equipment; and
e regulating telephone and email marketing, and online content.

The structure and powers of the ACMA are set out in the Australian Communications and Media Authority Act 2005. The key pieces of legislation administered by the ACMA are the Telecommunications Act 1997, which regulates carriage and content services; the Radiocommunications Act 1992, which regulates RF spectrum; the Broadcasting Services Act 1992, which regulates television and radio broadcasting; and the Telecommunications (Interception and Access) Act 1979, which regulates interception and access to telecommunications services.

1 Angus Henderson is a partner, Richard Dampney is a senior associate and Irene Halforty is a lawyer at Webb Henderson.
Act 1992, which regulates television and radio industry structure and content; the Do Not Call Register Act 2006; and the Spam Act 2003, which regulates direct marketing by telemarking and electronic means.

The Australian Competition and Consumer Commission (ACCC) is responsible for access regulation in the telecommunications sector, and also oversees the telecommunications-specific anticompetitive conduct and consumer protection provisions within the Competition and Consumer Act 2010 (CCA). The ACCC will also be given a number of new roles in relation to the consumer data right (see Section VII).

The Office of the Australian Information Commission is responsible for privacy and freedom of information laws, and will, along with the Data Standards Body, support the ACCC in regulating the consumer data right.

The Department of Communications and the Arts is the principal government department responsible for developing policy relevant to the TMT sectors.

The National Data Commissioner, currently part of the Department of the Prime Minister and Cabinet, will provide oversight and regulation of Australia's proposed national data sharing and release legislation.

### ii Regulated activities

A carrier licence is required for owners of network units that are used to provide fixed, mobile or satellite services to the public. A network unit includes line links (e.g., optical fibre and copper links) as well as radiocommunications transmitters and receivers (e.g., mobile telephony base stations and satellite-based facilities). The owner of the network unit must apply to the ACMA for a carrier licence. The application must be accompanied by a non-refundable application fee of A$2,122 (as at September 2019). The ACMA has 20 business days to make a decision in respect of issuing a carrier licence and must consult with the Communications Access Coordinator (Attorney General's Department). If no decision is made within 20 business days, the application is deemed to have been refused, unless the ACMA issued a request for further information or the Attorney General's Department issued a notice to the ACMA that it must not grant the carrier licence in respect of the application, in which case different time limits for refusal will apply.\(^2\) Carriers must pay an annual licence fee to the ACMA comprising a fixed amount as well as a variable amount based on the carrier's eligible revenue (being the gross sales revenue of the carrier and related entities, less any proscribed revenue and expense deductions).\(^3\) A carrier licence has no set duration, and remains in force until it is either surrendered by the licensee or cancelled by the ACMA.

No licence is required for entities that provide telecommunications services to the public without owning any network units. These entities are classified as carriage service providers and must comply with a range of regulatory obligations, including wholesale access, interception and data retention obligations. A similar regime applies to entities providing content services to the public (e.g., pay-TV services) without owning any network units. Such entities are classified as content service providers and are subject to certain regulatory obligations without requiring a licence.

Carriage service providers and content service providers that provide standard telephone services, public mobile telecommunications services or internet access services must also join the Telecommunications Industry Ombudsman (TIO) scheme. In addition, providers of

---

\(^2\) See Division 3 of the Telecommunications Act 1997 (Cth).

\(^3\) See Part 5 of the Telecommunications (Eligible Revenue) Determination 2015.
standard telephone services must provide access to local, national and international calls, emergency service numbers, operator-assisted and directory services, and itemised billing (including itemised local calls on request).

Since April 2015, pre-selection obligations only apply to providers of fixed-line telephony services over the legacy PSTN or integrated services digital networks, rather than all fixed-line telephony providers. These changes were effected through the Telecommunications Legislation Amendment (Deregulation) Act 2015, which more broadly seeks to remove outdated regulation of the telecommunications sector.

There are three types of radiocommunications licences overseen by the ACMA. A spectrum licence is required for the use of a particular RF band within a particular geographic area. The spectrum licensing regime is being reviewed by the ACMA (see Section IV). Currently, spectrum licences are allocated using a market-based approach, typically an auction, and are issued for up to 15 years. Spectrum licences are technology-neutral, allowing licensees to operate any type of equipment for any purpose as long as they comply with licence conditions and certain technical standards.

An apparatus licence is an individual licence required for the operation of radiocommunications devices under specific technical conditions of use relating to such matters as frequency, power and geographic area. There are a number of apparatus licence types, including, inter alia, for aircraft, broadcasting, datacasting, defence and scientific transmitters, as well as defence, fixed and space receivers.

The operation of certain radiocommunications devices is regulated through a class licence (rather than an individual apparatus licence). Following industry consultation, the ACMA has introduced the Radiocommunications (Intelligent Transport Systems) Class Licence 2017 to support intelligent transport systems (ITS), which will enable vehicle-to-vehicle, vehicle-to-person or vehicle-to-infrastructure communications through the use of complying wireless technologies and devices.4 The ACMA also introduced the Radiocommunications (Body Scanning – Aviation Security) Class Licence in 2018 following industry consultation to authorise the use of body scanners at Australian airports for security screening processes, and which replaces the previous apparatus licensing arrangements applicable to body scanners used at international airports. Other devices that the ACMA currently authorises through a class licence include satellite communications equipment and Wi-Fi devices.

iii Ownership and market access restrictions

There are now three key restrictions on cross-ownership of media companies:

- the two-to-a-market radio rule, which prevents control of more than two commercial radio licences in the same licence area;
- the one-to-market TV rule, which prevents control of more than one commercial TV licence in the same licence area; and
- the number of voices rule, which prevents cross-media mergers or acquisitions that result in the number of independent media operations falling below five voices in metropolitan radio licence areas and four voices in regional radio licence areas (the four/five rule).

4 The ITS class licence was made under Section 132 of the Radiocommunications Act 1992 and is consistent with the ITS arrangements in other jurisdictions. This harmonisation with wider global developments will likely facilitate the introduction of the latest transport communications technology in Australia’s ITS arrangements with wider global developments.
These restrictions on cross-ownership of media companies were watered down significantly by the Broadcasting Legislation Amendment (Broadcasting Reform) Act 2017. That legislation repealed, from 17 October 2017, the following key restrictions on media control and diversity rules that previously applied: (1) the two out of three rule, which prevented a person from being in a position to exercise control of more than two of the three media platforms (commercial television, commercial radio and newspapers) in the same licence area; and (2) the 75 per cent reach rule, which prevented a person from being in a position to exercise control of commercial television broadcast licences whose total licence area populations are greater than 75 per cent of the Australian population.

Foreign ownership restrictions depend on the specific sector in which the target entity is located. For foreign investments in the telecommunications sector, the Foreign Investment Review Board must be notified if a foreign person (or several foreign people) acquires a substantial interest in an Australian corporation whose assets exceed A$266 million (indexed annually). A substantial interest will have been acquired if a single foreign person holds 20 per cent or more, or several foreign persons hold 40 per cent or more, of the issued shares, units or voting power of the target corporation.

For investments in the media sector, the Foreign Investment Review Board must be notified if a foreign person seeks to acquire 5 per cent or more of an Australian media business, regardless of value. A foreign person is defined as an individual who is not ordinarily a resident in Australia or a corporation where one or more foreign persons hold a combined total of 20 per cent or more of the issued shares, units or voting power.

In addition, from September 2018, a foreign person with company interests of 2.5 per cent or more in an Australian media company is required to notify the ACMA of its interests within 30 days.\(^5\) The ACMA includes details of these notifications in a publicly available register of foreign owners of media assets.

The foreign investment notification rules for the media and telecommunications sectors apply even to investors from countries that have free trade agreements with Australia, such as Chile, China, Japan, New Zealand, South Korea and the United States.

\(\text{iv \ Transfers of control and assignments}\)

A carrier licence cannot be assigned or transferred, since it is granted to a particular entity. Spectrum can be freely traded in the form of spectrum trading units (STUs), which refer to a particular block of bandwidth within a given geographic area. A spectrum licensee can transfer some or all of the STUs within the scope of its licence. This means that spectrum licences can effectively be divided or amalgamated to respond to market-based needs.

Apparatus licences are also generally transferrable. An application must be lodged to the ACMA and be signed by both the original licensee and the proposed new licensee. The ACMA has the power to declare that particular types of apparatus licence are not transferrable or that, in specified circumstances, an apparatus licence is not transferrable.

Mergers and acquisitions in the TMT sectors are subject to the general merger control regime overseen by the ACCC. Under this regime, there is no requirement for parties to a merger to notify the ACCC before completing a merger. However, under Section 50 of the CCA, the ACCC (or a third party) can investigate a merger and take court action if a merger or acquisition would have the effect or likely effect of substantially lessening competition

\(^5\) Broadcasting Legislation Amendment (Foreign Media Ownership, Community Radio and Other Measures) Act 2018, Section 74F.
in any market. If the parties to a merger want to obtain greater certainty in relation to the competition risks of the merger, there are two optional pre-merger approval processes that a party may apply for:\(^6\)

\(a\) merger authorisations: the ACCC will grant a merger authorisation if either the proposed acquisition would not be likely to substantially lessen competition, or the likely public benefit from the proposed acquisition outweighs the likely public detriment. If the ACCC grants a merger authorisation, the ACCC or a third party cannot take any action in respect of the merger under Section 50 of the CCA. The ACCC must make a determination within 90 days (unless that time period is extended with the consent of the applicant). Failure by the ACCC to make a determination within the 90-day time limit is deemed as a refusal to grant authorisation.

\(b\) informal merger review: the ACCC provides an indication of its views on whether a merger is likely to breach Section 50 of the CCA. While an informal merger clearance may provide merger parties with a significant level of comfort regarding the ACCC’s position, it does not prevent the ACCC or a third party from taking action against the merger parties at a later date under Section 50 of the CCA. There are no formal time frames within which the ACCC must provide informal clearance; however, the indicative time frame for this process is six to eight weeks.

In undertaking a media merger assessment, the ACCC will consider the impact of the proposed merger on competition and media diversity, access to key content, the impact of technological change, two-sided markets and network effects, bundling and foreclosure, and minority shareholdings. An applicant or person who has a sufficient interest in a merger authorisation may appeal an ACCC determination to the Australian Competition Tribunal.

Following its Inquiry into Digital Platforms, the ACCC has recommended changes to Australia’s merger laws to expressly require consideration of the likelihood that an acquisition could remove a potential competitor from a market (e.g., the acquisition of start-ups by large digital platforms) and the amount and nature of assets, including technology and data, that may be acquired through the acquisition.\(^7\) The ACCC also recommended that large digital platforms agree to a notification protocol, under which they would be required to provide advance notice of the acquisition of any business with activities in Australia.\(^8\)

### III TELECOMMUNICATIONS AND INTERNET ACCESS

The government does not directly subsidise the construction of broadband infrastructure or the use of retail broadband services. However, in 2009, the government set up a state-owned corporation, NBN Co (known as nbn) to design, build and operate a wholesale-only

---

\(^6\) These processes were amended by the introduction of the Competition and Consumer Amendment (Competition Policy Review) Act 2017 and the Competition and Consumer Amendment (Misuse of Market Power) Act 2017 in November 2016.

\(^7\) Recommendation 1, the Australian Competition and Consumer Commission, Digital Platforms Inquiry Final Report, June 2019.

next-generation network. Currently, nbn relies on government funding, and earns revenue primarily by selling wholesale (Layer 2 bitstream) access to its network to retail telecommunications operators.

i  Internet and internet protocol regulation

The ACMA considers providers of managed VoIP services to be carriage service providers. This is the same regulatory category that mobile and fixed telephony providers sit within, and involves a range of regulatory obligations, including membership of the TIO scheme, consumer protection obligations, obligations to comply with the numbering plan and provide number portability, and lawful access and interception obligations.

Moreover, VoIP services that allow users to make calls to, and receive calls from, traditional PSTN telephony services are treated as standard telephone services. This entails certain additional obligations, such as providing operator and directory assistance services, access to emergency call services, access to the National Relay Service, and itemised billing.

OTT VoIP services (provided over an existing carriage service), as well as OTT messaging services, are not subject to the same degree of regulation. OTT IP-based services will be subject to new industry assistance and access laws (see Section III.iv), but the Department of Communications and the Arts and the ACMA do not currently have any other definitive plans to regulate these services more broadly.

ii  Universal service

A universal service regime was created by the Telecommunications (Consumer Protection and Service Standards) Act 1999. The regime requires Telstra, which has been designated as the default universal service provider, to ensure that standard telephone services and payphones are reasonably accessible to all Australians on an equitable basis (referred to as the Universal Service Obligation (USO)). The supply of standard telephone services under the USO is subject to a range of minimum performance standards and benchmarks, including maximum periods for connecting a new service and for rectifying a fault.

The statutory USO is implemented through the Telstra Universal Service Obligation Performance (TUSOP) Agreement entered into between the government and Telstra in July 2012. The TUSOP Agreement lasts for a period of 20 years, and involves the government paying Telstra A$253 million per annum for the supply of standard telephone services and A$44 million per annum for the supply, installation and maintenance of payphones under the USO.

The costs of the universal service regime are funded through the telecommunications industry levy, which is imposed on all carriers with eligible revenue in excess of A$25 million. The universal service regime has been overseen by the Department of Communications and the Arts since 1 July 2015. It was previously administered by the Telecommunications Universal Service Management Agency.

According to the government’s ‘Telecommunications infrastructure in new developments’ policy (issued in March 2015), nbn has an infrastructure provider of last resort (IPOLR) obligation in relation to new property developments that are within its fixed network footprint (or that will be within the next 12 months), or where a development has 100 lots or more. The IPOLR obligation requires nbn to roll out high-speed broadband infrastructure to these developments on request from the developer.

On 22 October 2015, the Regional Telecommunications Independent Review Committee (RTIRC) released its final report. The RTIRC was established by the government
to review the adequacy of telecommunications services in regional, rural and remote parts of Australia. The final report made a series of recommendations, including a proposal to reform the universal service regime and to provide subsidies for nbn’s non-commercial fixed wireless and satellite services through a new consumer communication fund.

Following the release of the RTIRC’s final report, the government requested the Productivity Commission to hold an inquiry into the future direction of the USO, the final report of which was released in June 2017. The report provides a range of recommendations regarding the future of universal access to a minimum level of retail telecommunication services, with its key findings including the fact that the USO should be wound up by 2020; broadband via the nbn™ network and mobile networks will increasingly be the main medium for voice services; and to the extent that there is any remaining availability, accessibility or affordability gaps, these should be addressed by specific government programmes rather than by way of an industry levy.

In December 2017, the government released its response to the Productivity Commission’s report outlining its intention to establish a universal service guarantee (USG). The USG will provide all Australian premises (regardless of their location) with access to both voice and broadband services delivered on a commercial basis by the market in the first instance, or targeted government measures where warranted. The USG will leverage the nbn™ network, with access to the network underpinned by the proposed statutory infrastructure provider legislation. The government established a USO Taskforce responsible for developing delivery options for the USG, including examining the feasibility and cost implications of providing alternative means for providing voice services to premises in nbn’s satellite footprint, the potential impact on nbn costs and its network design if premises serviced by Telstra under the USO migrate to the nbn™ network, and where and when it may be appropriate for Telstra to reduce the number of payphones provided under the USO.

In connection with the release of the Productivity Commission’s report, in June 2017, the government also introduced into Parliament the Telecommunications Reform Package (TRP). The TRP includes the Telecommunications Legislation Amendment (Competition and Consumer) Bill 2018, which aims to establish statutory infrastructure provider (SIP) obligations to ensure that all Australians have access to a high-speed broadband network, with nbn becoming the default SIP; clarify the wholesale-only rules that apply to high speed broadband networks; and enforce functional separation for other wholesale and retail carriers.

Additionally, the TRP proposes to establish a regional broadband scheme (RBS) via the Telecommunications (Regional Broadband Scheme) Charge Bill 2017. The RBS is intended to provide sustainable industry funding for the loss-making fixed wireless and satellite networks in regional Australia that are owned by nbn. This funding, which is expected to amount to A$9.8 billion over 30 years, will have a 95 per cent reliance on internal cross-subsidies within nbn, with the remaining 5 per cent paid for by competing nbn-comparable wholesale broadband networks. Both the Telecommunications Legislation Amendment (Competition and Consumer) Bill 2018 and the Telecommunications (Regional Broadband Scheme) Charge Bill 2018 lapsed before the Senate at the end of the previous parliamentary term, but the Minister has indicated that it will be reintroduced during the 2019 winter/spring parliamentary sitting.

---

The government (in partnership with the state and territory governments) has also invested in the improvement of mobile coverage in remote and regional Australia through its mobile black spot programme, which was launched in June 2015. The mobile black spot programme is over halfway complete, with 713 base stations activated (as at 28 June 2019), and all 867 base stations funded under the first three rounds of the programme are expected to be operational by 30 June 2019, and all base stations funded under the fourth round are scheduled to be operational by 30 June 2020.

In May 2018, the Department for Communications and the Arts appointed an independent committee to undertake a review of regional telecommunication services (2018 Regional Telecommunications Review), as is required every three years by Part 9B of the Telecommunications (Consumer Protection and Service Standards) Act 1999. The 2018 Regional Telecommunications Review considered how rural Australians could maximise the economic and social benefits that modern telecommunication services provide and undertook an analysis of the coverage achieved under the mobile black spot programme.10 The committee’s report was delivered to the Minister for Regional Communications on 30 September 2018, and published in December 2018. The committee made 10 recommendations, including that the government make no changes to the current USO arrangements until there are fit-for-purpose alternative voice options for consumers served by satellite; that the government commits to a large-scale, multi-year Stronger Regional Connectivity Package to improve broadband and mobile services in areas of high economic, social and public safety significance; and that industry bring forward new and innovative solutions for providing voice services in rural and remote Australia.

In March 2019, the Australian government published its response to the 2018 Regional Telecommunications Review and, as part of its response, announced that it will invest a further A$160 million towards the mobile black spot programme.

### iii Restrictions on the provision of service

There is currently no price regulation of retail telecommunications services. On 18 March 2015, the Minister of Communications revoked retail price control arrangements that applied to Telstra’s fixed-line voice services. However, the Minister retains the power to reintroduce retail price regulation at a future date.

Wholesale access regulation is effected through the telecommunications-specific access regime in Part XIC of the CCA. The ACCC has the power to declare a listed carriage service or a service that facilitates the supply of a listed carriage service. Once a service is declared by the ACCC, all providers of that service are subject to a range of standard access obligations. These include an obligation to supply the service on request (with certain exceptions) and to take all reasonable steps to ensure that the technical and operational quality of the service (and of fault detection, handling and rectification) that is equivalent to that which the access provider provides to itself.

The telecommunications services declared by the ACCC include, among others, fixed origination and termination, mobile termination, unconditioned local loop service, line sharing service, wholesale line rental, wholesale ADSL service, and domestic transmission capacity service.

---

On 31 August 2018, the ACCC announced an inquiry seeking views on the future of the existing declarations, due to expire on 31 July 2019, in respect of the unconditioned local loop service, line sharing service, wholesale line rental, PSTN originating access (OA) and PSTN terminating access (TA). The ACCC is considering whether these declarations should be remade, further extended, revoked, varied, allowed to expire, or extended and then allowed to expire. Consultation closed on 12 October 2018.

In October 2017, the ACCC decided not to declare wholesale domestic mobile roaming services. Legal proceedings commenced by Vodafone challenging aspects of the conduct of the inquiry were dismissed by the Federal Court on 21 December 2017.

On 7 August 2018, the ACCC commenced an inquiry into whether to extend, vary, revoke or re-make the domestic mobile terminating access service (MTAS) declaration. The MTAS is a wholesale service that allows consumers on different mobile networks to make calls and send SMSs to each other. On 28 June 2019, the ACCC concluded its inquiry into the MTAS and released its final report on its findings, including that it will continue the declaration for voice terminating services until 2024, but will not extend declaration of the SMS MTAS service beyond the expiry of the current declaration on 1 January 2020.\(^{11}\)

The nbn™ network, which is a wholesale-only network, is subject to a slightly different set of access obligations. As the network operator, nbn has an obligation to supply any declared services that relate to nbn on request to an access seeker (with limited exceptions), and to not discriminate between access seekers in doing so. In November 2017, the ACCC announced a public inquiry into nbn’s wholesale service standard levels. The inquiry is still ongoing; however, the ACCC accepted a court-enforceable undertaking (on 11 September 2018) by nbn to make changes to its wholesale service level commitments and associated rebates.

There is no net neutrality-style regulation in Australia that prohibits carriage service providers from favouring or excluding certain content, applications, services or devices.

The Spam Act 2003, administered by the ACMA, makes it illegal to send commercial electronic messages with an Australian link without the express or inferred consent of the recipient. Electronic messages include emails, instant messages and messages sent using the SMS and MMS services. Commercial electronic messages must also contain a functional unsubscribe mechanism and accurate information about who authorised the sending of the message. Exemptions from these rules apply for purely factual messages, as well as messages from government bodies, registered political parties, registered charities and educational institutions (sent to current and past students and their households).\(^ {12}\)

In addition, the ACMA administers a Do Not Call Register, designed to prevent unsolicited telemarketing calls being made to fixed and mobile telephone numbers as well as marketing faxes. Users can register their telephone or fax number on the Do Not Call Register for free. Once a number is registered, it is prohibited to make unsolicited telemarketing calls or send marketing faxes to that number. Exemptions apply for public interest calls and faxes, including from government bodies, registered political parties, registered charities, educational institutions and political candidates.\(^ {13}\) In 2017, the ACMA introduced the Telemarking and Research Calls Standard 2017, establishing minimum requirements for those making telemarketing and research calls, including a requirement to ensure calling line

---

12 Spam Act 2003 (Cth), Schedule 1.
13 Do Not Call Register Act 2006 (Cth), Schedules 1 and 1A.

© 2019 Law Business Research Ltd
identification is enabled and operational for at least 30 days from the date the call was made; minimum information that must be provided when making a telemarketing or research call; calling times during which a telemarketing or research call is permitted to be made; and a requirement to immediately terminate a call in certain circumstances.

The Telecommunications Legislation Amendment (Unsolicited Communications) Bill 2019, currently before the Senate, will amend various legislation, including, inter alia, the Do Not Call Register Act 2006 to enable a consumer who registers on the Do Not Call Register to opt out of receiving phone calls from charities and the Spam Act 2003 to require political parties to provide an unsubscribe function for all unsolicited electronic communications containing political content.

The ACMA also administers a number of other standards and codes of practice, including the Telecommunications Consumer Protections Code, which set out various specific requirements that carriage service providers and other entities are required to comply with (as applicable). In 2018, the ACMA introduced a range of new rules relating to the supply of telecommunications services, which were designed to improve the overall experience of end-users acquiring telecommunications (including nbn) services. These include:

\[a\] the Consumer Complaints Handling Industry Standard,\(^{14}\) which came into effect on 1 July 2018 and introduced new complaints handling rules designed to ensure carriage service providers effectively manage complaints in relation to consumer problems with telecommunications services;

\[b\] the Consumer Complaints Record Keeping Rules,\(^{15}\) which came into effect on 1 July 2018 and introduced minimum record-keeping and reporting requirements to the ACMA, designed to allow carriage service providers and the ACMA to monitor industry complaints-handling performance and to identify new trends driving complaints;

\[c\] the NBN Consumer Information Standard,\(^{16}\) which came into effect on 21 September 2018 and introduced minimum information requirements, is designed to ensure carriage service providers give all the necessary information to consumers to allow them make informed choices about nbn services; and

\[d\] the NBN Continuity of Service Standard,\(^{17}\) which came into effect on 21 September 2018 and puts in place new rules to make sure that consumers are not left without a working telecommunications service during their migration to the nbn™ network.

The ACMA registered the revised TCP Code in June 2019, which commenced on 1 August 2019.\(^{18}\) The revised TCP Code contains new credit assessment provisions, requiring carriage service providers to assess new customers and those moving from pre to post-paid services capacity to pay for contracts greater than A$1,000; stricter obligations on carriage service providers to ensure selling practices are fair and transparent, clearer rights for consumer access to records relating to their contracts, and aligns complaints rules with the Consumer Complaints Handling Industry Standard.

---


\(^{15}\) Telecommunications (Consumer Complaints) Record-Keeping Rules 2018.

\(^{16}\) Telecommunications (NBN Consumer Information) Industry Standard 2018.

\(^{17}\) Telecommunications (NBN Continuity of Service) Industry Standard 2018.

iv Security

Lawful access and interception is governed by the Telecommunications (Interception and Access) Act 1979. Law enforcement agencies have the power to intercept telecommunications provided that they obtain a warrant from an eligible judge or member of the Administrative Appeals Tribunal. The Australian Security Intelligence Organisation (ASIO) only requires a warrant from the Attorney General to engage in the same activities. The interception regime is technology-neutral and applies to voice calls, faxes, SMS and MMS messages and IP-based communications (including email).

Carriers and carriage service providers are obliged to provide and maintain facilities enabling them to execute interception warrants. Carriers and carriage service providers must also lodge annual interception capability plans with the ACMA and the Attorney General’s Department. The costs of maintaining interception capabilities must be covered by carriers and carriage service providers, even though the requesting agencies pay for the costs of accessing the intercepted communications.

Australia acceded to the Council of Europe Convention on Cybercrime in March 2013. To implement its obligations under the Convention, a number of amendments were made to the existing legislation. These amendments allow law enforcement agencies and ASIO to issue notices to carriers that require them to store communications (including the content of communications) that assist in a specified domestic or foreign criminal or national security investigation. Unlike interception requests, these preservation notices do not require a warrant. However, the stored communications can only be accessed through a warrant issued by a judge or member of the Australian Appeals Tribunal.

From 18 September 2018, following the introduction of the Telecommunications and Other Legislation Amendment Act 2017, all carriers, carriage service providers and carriage service intermediaries are legally required to do their best to protect telecommunications networks and facilities owned, operated or used by the carrier or provider from unauthorised interference or unauthorised access to ensure the confidentiality of communications carried on, and of information contained on, telecommunications networks or facilities; and the availability and integrity of telecommunications networks and facilities. For carriers and carriage service providers, this obligation includes a requirement to maintain competent supervision of, and effective control over, telecommunication networks and facilities owned or operated by them. In addition, carriers and carriage service providers are required to notify the Communications Access Co-ordinator of proposed changes to their networks and services that could have a material adverse impact on their ability to comply with these new obligations.

Carriers and carriage service providers are also subject to a mandatory metadata retention regime. This requires them to retain, for a period of two years, metadata relating to the communications of their subscribers (e.g., the phone numbers of the parties to a call or message, the time and duration of a call, the email address of the sender and recipient, and the time the email message was sent). The regime does not require retention of the content of a communication or web-browsing history. The Parliamentary Joint Committee on Intelligence and Security (PJCIS) commenced a review of the mandatory data retention regime, due to report by 13 April 2020, as prescribed by Part 5-1A of the Telecommunication (Interception and Access) Act 1979.

19 Cybercrime Legislation Amendment Act 2012 (Cth).
20 Telecommunications (Interception and access) Amendment (Data Retention) Act 2015 (Cth).
On 8 December 2018, the government enacted new industry assistance and access laws under the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018. Under these industry assistance and access laws, domestic and foreign designated communication providers can be requested to provide voluntary assistance (via a technical assistance request), or be required to provide assistance (via a technical assistance notice), including, where required, to develop a capability to provide the assistance requested (via a technical capability notice), to law enforcement and security agencies to access certain communications. The PJCIS referred the Assistance and Access Act for independent review by the Independent National Security Legislation Monitor, which will consider whether the Assistance and Access Act contains appropriate safeguards for protecting the rights of individuals, remains proportionate to the threat to national security and remains necessary. The Independent National Security Legislation Monitor will report to the PJCIS by 1 March 2020.

Personal information is regulated through the Privacy Act 1988 and the Australian Privacy Principles (APPs), which came into force in March 2014. The APPs apply to both government and private entities. In particular, the APPs require that, before an entity discloses personal information overseas, it must take reasonable steps to ensure that the recipient of the personal information does not breach the APPs (e.g., through a contractual obligation). Since 22 February 2018, APP entities have been required to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals of eligible data breaches in respect of personal information. Under the Notifiable Data Breaches Scheme, APP entities can undertake remedial action to reduce the risk of serious harm of a data breach and the associated obligation to notify affected individuals (although the OAIC will still need to be notified). There are also a range of exceptions to the notification obligation, including where:

- the data breach has been reported by another entity holding that personal information;
- notification would likely prejudice an enforcement-related activity;
- the requirement to notify would be inconsistent with the secrecy provisions; or
- the Commissioner has declared that an entity does not need to provide such a notification.

In addition, Part 13 of the Telecommunications Act 1997 requires carriers, carriage service providers, number database operators and emergency service operators to protect the confidentiality of certain information. This includes information or documents relating to the content of communications that have been, or are being, carried by carriers or carriage service providers, the carriage services supplied or proposed to be supplied to another person, as well as the affairs or personal particulars of other persons (protected information). Use and disclosure of protected information is a criminal offence unless permitted in certain limited circumstances, such as where authorised by law enforcement agencies or where reasonably

---

21 An eligible data breach arises when there is unauthorised access to, or disclosure or loss of, personal information, and a reasonable person would conclude that the unauthorised access to, or disclosure or loss of, personal information would likely result in serious harm to one or more individuals to whom the personal information relates. See: Privacy Act 1988 (Cth), Section 26WE.
23 Privacy Act 1988 (Cth), Section 26WF.
24 ibid., Sections 26WM to WQ.
necessary to prevent threats to life and health. Disclosure of protected information to ASIO and criminal law enforcement agencies is permitted in response to a valid authorisation made by ASIO or a criminal law enforcement agency and notified to the carrier or carriage service provider under Chapter 4 of the Telecommunications (Interception and Access) Act 1979 and which complies with the Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2018.

Compliance with the Privacy Act 1988 is overseen by the OAIC and compliance with Part 13 of the Telecommunications Act 1997 is overseen by both the OAIC and the ACMA.

IV SPECTRUM POLICY

i Development

The government is in the process of overhauling the current spectrum management system to replace it with a simplified singular licensing scheme. This aligns with the government’s wider policy of deregulation.

In August 2015, the government announced that it will implement the key recommendations of the Spectrum Review Report undertaken by the Department of Communications and the Arts and the ACMA. The Report found that existing spectrum management arrangements were slow, rigid, administratively cumbersome and unnecessarily costly for users. In May 2017, the government released an exposure draft of the Radiocommunications Bill 2017, with the Department of Communications and the Arts considering submissions to the consultation package and exposure draft bill.

Spectrum pricing, including for Commonwealth-held spectrum, was considered separately from the Radiocommunications Bill 2017. In February 2018, the Department of the Communications and the Arts published the final recommendations accepted by the government with respect to the spectrum pricing review and Commonwealth-held spectrum review. The spectrum pricing review included 11 final recommendations in respect of ACMA’s allocation decisions, market-based allocations, administered allocations and the cost recovery framework. In its latest five-year spectrum outlook for 2019 to 2023, the ACMA confirmed that it will implement the recommendations of the government’s Spectrum Pricing Review, with consultation to commence towards the end of 2019. The ACMA considers that while the recommendations of the government’s Spectrum Pricing Review anticipated a new legislative framework and single licensing framework, much of the policy intent could also be implemented under existing legislation and later transitioned to new legislative arrangement (if required). The ACMA intends to proceed on this basis, and has initiated four substantive programmes of work, including: (1) to further identify bands to transition from administratively set charges to competitive market-based allocation; (2) to develop and publish Spectrum Pricing Guidelines; (3) to review the ACMA’s administratively prices spectrum and the formula used to set current apparatus licence taxes; and (4) to simplify industry’s spectrum management cost recovery arrangement to ensure consistency with the Australian Government Charging Framework.


Separately, the Minister for Communications, Cyber Safety and the Arts indicated in May 2019 that the government expects to pursue legislative reform only where it will deliver tangible improvements to the current administration of spectrum and a more efficient regulatory framework. Any such legislative reforms would likely complement the findings and recommendations of the Spectrum Pricing Review.

The final recommendations with respect to the Commonwealth-held spectrum review included recommendations to establish an advisory committee of relevant government agencies to provide advice to the Minister for Communications on issues of spectrum policy, improve transparency through publishing a consolidated report of Commonwealth spectrum holdings every two years, and exploring a whole-of-government approach to share and trade Commonwealth-held spectrum.

ii Flexible spectrum use

Currently, three types of licences are available under the Radiocommunications Act 1992: spectrum licences, apparatus licences and class licences. The existing licensing schemes are complex and quite rigid. This creates difficulty obtaining, transferring and trading licences.

The proposed Radiocommunications Bill 2017 would introduce a single licensing system that is flexible and simple. The new licensing scheme will encompass core conditions, including the relevant part of the spectrum, geographic information and payment of any applicable charges (including taxes). The proposed Radiocommunications Bill 2017 will integrate broadcasting spectrum into the general spectrum management framework.

A secondary market for spectrum will be encouraged, and assignment, sharing and subdivision will be allowed (subject to any licence restrictions). However, current class licences will not be incorporated into the new licensing system, meaning it may take time for a market to develop as old licences expire. The new licences will be issued for up to 20 years (current licences are limited to 15 years).

Under the new regime, the ACMA will retain legislative power to set licence conditions, subject to a broader set of guiding objectives, so that licences can be tailored to the needs of individual licence holders, accommodate new technologies and be repurposed when they are transferred. To encourage spectrum sharing, the ACMA will be permitted to issue licences or make spectrum authorisations within parts of spectrum that have already been licensed or are subject to an authorisation (provided arrangements are in place to manage interference). Licensees will also be able to authorise third parties to operate devices under their licences.

One of the purposes of this simplified licence regime is to encourage spectrum users to view spectrum rights as a form of property that is able to be regularly traded or leased. The Spectrum Review Report found that encouraging a market for spectrum rights ensures that spectrum is allocated efficiently and may be applied to a variety of uses as demand requires. It also reduces the costs of regulatory intervention.

iii Broadband and next-generation mobile spectrum use

In October 2017, the government released a 5G directions paper, which outlined the immediate actions for government to take in order to support the timely rollout of 5G in Australia, and focused on:
a making spectrum available for 5G in a timely manner;
b actively engaging in international spectrum harmonisation activities;
c streamlining arrangements to allow mobile carriers to deploy infrastructure more quickly; and
reviewing existing telecommunications regulatory arrangements to ensure they are fit for purpose.

Separately, the ACMA has identified meeting unprecedented growth in demand for mobile broadband and next-generation services as a priority for the next decade.

In its five-year spectrum outlook for 2019 to 2023, the ACMA confirmed that its Mobile Broadband Strategy (released in February 2016) remains the basis for the ACMA’s response to address the growth in demand for mobile broadband capacity, a key part of which is the articulation of a spectrum management process for the release of additional spectrum for mobile broadband. The latest five-year spectrum outlook also included an updated mobile broadband work programme, which sets out the various mobile broadband spectrum planning projects being conducted by the ACMA.

The ACMA has also continued to undertake a number of other initiatives to progress spectrum management for 5G. In particular, in October 2016, the ACMA released the Future Use of the 1.5GHz and 3.6GHz bands Discussion Paper, which was designed to seek industry feedback on the increasing demand for mobile broadband services in those bands, largely in anticipation of the future introduction of 5G mobile technology. In August 2017, the ACMA also held a further consultation process on the 3.6GHz band on the basis that it has been identified to be the most favoured spectrum band for 5G mobile broadband.

In April 2018, the ACCC released its Communications Sector Market Study Final Report, detailing a number of recommendations on a wide range of competition and consumer issues in the communications market, including broadband and voice services, aggregation and transmission services, data centres and content delivery networks, and the IoT.

Australia has also been one of the global leaders in flagging national security concerns about the involvement of Chinese companies in the development of 5G networks. On 23 August 2018, the Departments of Home Affairs and Communications and the Arts issued a joint statement that effectively banned Huawei and ZTE from supplying equipment for 5G networks in Australia due to national security concerns inherent in the architecture of 5G. While not specifically listing either company in the statement, the departments stated that:

> the government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian laws, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference [in accordance with their obligations introduced by the Telecommunications and Other Legislation Amendment Act 2017].

iv Spectrum auctions and fees

Currently, the ACMA issues spectrum licences through auction, tender or price negotiation processes. The last spectrum auction for the 3.6GHz band was held in November and December 2018. In July 2018, the government announced allocation limits for participants in this auction. Those limits capped the total amount of spectrum that an auction participant

---

could purchase in the 3.6GHz spectrum and were calculated inclusive of any spectrum in the 3.4GHz to 3.7GHz bands that an auction participant already held. As a result of these limits, carriers with significant holdings in the 3.4GHz to 3.7GHz bands, such as nbn and Optus, were largely precluded from participating in the auction. Separately, Vodafone and TPG announced, in connection with their proposed merger (which was opposed by the ACCC on 8 May 2019), that they formed a joint venture entity (Mobile JV) with the intention of acquiring 5G spectrum at the auction.

There were four winning bidders in the auction: Telstra Corporation Limited (with a winning bid of A$386,008,400); Mobile JV (with a winning bid of A$263,823,800); Optus Mobile Pty Ltd (with a winning bid of A$185,069,100); and Dense Air Australia Pty Ltd (with a winning bid of A$18,492,000).

The ACMA maintains on its website a list of spectrum licences that are due to expire in the next 18 months, with details about whether they will be eligible for reissue. In 2012, the then-Minister for Broadband, Communications and the Digital Economy made a class of services determination that it is in the public interest to reissue licences to incumbent licensees operating mobile voice and data communications services, wireless broadband services and satellite services in certain bands. If these licensees can prove that they have used the spectrum to provide a relevant service, the ACMA will offer the licence for reissue without offering the spectrum at auction.

The Spectrum Review Report expressed concern that under the current model, spectrum prices may not always reflect the true value of spectrum or the way that value changes over time. The Spectrum Review Report noted that if the legislative changes it recommended were to be introduced, the prices for spectrum would need to be transparently reviewed to ensure they remained appropriate and suggested that the ACMA might consider opportunity cost pricing or other forms of administered-incentive pricing.

The Spectrum Review Report also recommended that pricing and taxation arrangements for licences should be consolidated under the new single licence system. Currently, different licences are subject to different charges, taxes and fees. For instance, class licences are not associated with any fees, while apparatus licences incur a cost recovery charge plus a licence fee that differs depending on whether it is a receiver or a transmitter licence. The recommendations of the Spectrum Review Report are proposed to be implemented as part of the proposed Radiocommunications Bill 2017.

V MEDIA

i Australian content requirements

Australian content and commercial television is regulated by the Broadcasting Services Act 1992. The ACMA is responsible for administering the Australian Content Standard and Television Program Standard 23 – Australian Content in Advertising, which applies to commercial free-to-air television licence holders. These standards do not apply to cable television providers or online content distributors such as VOD platforms. The ACMA also administers the Classification (Publications, Films and Computer Games) Act 1995, and sets the Guidelines for Classification of Films and Computer Games that are used by the Classification Board to classify content. Content is assessed based on six classifiable elements and assigned a rating to reflect its likely impact on different viewers. Although technically some online content is considered classifiable, historically classification obligations are not enforced against online providers.
The Australian Content Standard provides that 55 per cent of broadcast transmission between 6am and midnight must be Australian programming, with sub-quotas for drama, documentaries and children’s programmes. The Australian Content in Advertising standard requires that at least 80 per cent of advertising time be used for Australian-produced advertisements.

For radio, under the Commercial Radio Code of Practice and Guidelines 2017, a minimum amount of Australian music content (between 5 to 25 per cent depending on the type of content) is required to be broadcast by commercial radio licensees between 6am and midnight each day. Certain formats of service, such as open-line, news, talk and sport content, are excluded from this requirement. Additionally, radio broadcasters must disclose commercial or other arrangements, such as sponsorships, that could affect reporting of current affairs under the Broadcasting Services (Commercial Radio Current Affairs Disclosure) Standard 2012.

The ACMA also administers the new rules introduced by the Broadcasting Legislation Amendment (Broadcasting Reform) Act 2017, which increased the minimum requirements for broadcasting material of local significance applying to commercial television networks covering more than 75 per cent of Australia’s population. These new requirements commenced on 17 April 2018. For networks not subject to these requirements, the Broadcasting Services (Additional Television Licence Condition) Notice 2014 continues to apply.

ii Classification and censorship
An amendment to the Classification (Publications, Films and Computer Games) Act 1995 was enacted in September 2014 that allowed classification bodies to authorise the use of automated classification tools for certain content. This makes obtaining a classification significantly cheaper and easier. When this amendment was being considered, legislators expressed the hope that this would lead to increased classification rates for apps and online content.

Advertising restrictions are enforced by both the ACMA and the Advertising Standards Bureau. The Advertising Standards Bureau administers several industry- and target-audience-specific codes of practice (such as the Commercial Radio Code of Practice and Guidelines 2017 and the Commercial Television Industry Code of Practice 2015), including advertising codes applicable to children, food and beverages and environmental claims. The ACMA also administers a number of codes of practice applying to commercial free-to-air TV, radio, pay-TV and online services that prohibit gambling advertisements during the broadcast of live sports between 5am and 8.30pm and otherwise restrict gambling advertising during the broadcast of live sports at other times of day. These codes of conduct came into effect on 30 March 2018, except for the code of conduct applying to online services, which came into effect on 28 September 2018.

iii Anti-piracy regulation
An amendment to the Copyright Act 1976 was introduced in 2015 to allow a party to apply to the Federal Court to grant an injunction to require a carriage service provider to take reasonable steps to disable access to a website where the primary purpose of that website is to infringe, or to facilitate the infringement of, copyright. There has been continued action by content owners requiring ISPs to block websites in Australia that host content infringing on copyrights since the introduction of these provisions in 2015. According to the Site Blocking Efficacy: Australia Report released in February 2018, site blocking laws in Australia have
resulted in a 53.4 per cent reduction in usage of blocked sites since the blocking regime began. In February 2018, the Department for Communications and the Arts announced its review of the Copyright Amendment (Online Infringement) Act 2015, including the effectiveness and efficiency of the mechanisms and processes of the site blocking laws.28

In March 2018, the Department of Communications and the Arts commenced consultation on the Copyright Modernisation Review, the result of copyright reform options recommended by the Productivity Commission Inquiry into Australia’s Intellectual Property Arrangements. The focus of the review was to consider whether there is general support for the modernisation of the Copyright Act given the impact of the digital world when creating, accessing and distributing copyright material, including whether defences should be expanded to apply in the technology sphere by introducing a fair dealing defence for incidental or technical use and protection for text and data mining.

iv Internet-delivered video content

In the past few years, traditional broadcasters have been launching online services including catch-up television and VOD offerings. At present, these services still complement rather than replace free-to-air broadcasts, so there is minimal disadvantage to consumers without internet access.

The communications sector market study issues paper released in September 2016 identified the popularity of streamed video content as a significant driver of demand for data services, and flags this as a factor for consideration when assessing the need and incentive for investment to improve data availability. The issues paper noted that video accounted for around 69 per cent of all internet traffic in Australia in 2015, and is expected to increase to 82 per cent by 2020. New and emerging applications, including ultra high-definition video (4K and 8K), 360 video or augmented or virtual reality games, are also expected to increase in popularity in Australia, placing further constraints on data. Although it is expected that advanced video compression techniques may provide some relief. In April 2018, the ACCC released its final report for the communications sector market study and noted that while OTT services bring benefits to fixed and mobile broadband service providers in terms of increasing demand for access and data, service providers may face a relative decline in revenue as OTT content services capture larger proportions of consumers’ spend. The ACCC notes that as a result, broadband service providers continue to acquire and distribute content both to recapture value from OTT providers and to differentiate their service offerings from other broadband service providers and mobile service providers. Traditional content providers, such as Foxtel, have also continued to acquire exclusive rights for premium sports and other content to maintain their audience and advertisement shares and have sought to utilise OTT distribution to expand their reach across increasingly fragmented audiences, though the significant losses recently incurred by Foxtel are expected to lead to a significant reduction in expenditure on this type of content.

Online content is subject to regulation under Schedules 5 and 7 of the Broadcasting Services Act 1992 (Online Content Scheme). This is a light-touch regime compared with the content and classification restrictions imposed on traditional broadcasters discussed above. Responsibility for administering the Online Content Scheme switched from the ACMA to

---

28 See Department of Communications and the Arts, Review of the Copyright Online Infringement Amendment, https://www.communications.gov.au/have-your-say/review-copyright-online-infringement-amendment.
the eSafety Commissioner on 1 July 2015. The remit of the Office of the Children’s eSafety Commission was expanded in June 2017 with the Enhancing Online Safety for Children Amendment Act 2017, which transformed the Children’s eSafety Commissioner into the eSafety Commissioner. The Commissioner has the power to investigate complaints about online content and order that prohibited content be taken down if it is hosted in Australia. Content is determined to be prohibited if it would be refused classification or classified as X18+ under Australia’s content classification regime. The eSafety Commissioner’s responsibilities were expanded in June 2017, including assuming responsibility for the administration of the takedown notice scheme under the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018. In June 2018, civil penalties were introduced in respect of non-consensual sharing of intimate images, with individuals and corporations facing civil and criminal penalties for failing to remove an image when requested to do so by the eSafety Commissioner.

In response to the failure by technology companies to remove the content (including video and livestreaming) associated with the Christchurch terrorist attack, in April 2019 the government enacted the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act. The Act imposes new obligations:

a. on ISPs, content and hosting service providers to notify the Australian Federal Police of the existence or accessibility of abhorrent violent material through its services; and

b. on content and hosting service providers to expeditiously remove or cease to host abhorrent violent material.

Breaches of these obligations are criminal offences attracting significant penalties. In particular, a failure to expeditiously remove or cease to host abhorrent violent material can lead to up to three years’ imprisonment and a fine of up to A$2.1 million for an individual, or a fine of up to A$10.5 million or 10 per cent of annual turnover (whichever is greater) for a corporation.

While some ISPs voluntarily blocked websites that streamed or hosted footage of the Christchurch terrorist attack, the eSafety Commission exercised its powers\(^{29}\) in September 2019, by directing ISPs to block eight websites that were still hosting footage of the attack. This follows a government-convened taskforce (including ISPs and digital platforms representatives) and the establishment of an Australian Taskforce to Combat Terrorist and Extreme Violent Material Online (the Australian Taskforce), which called for legislative amendments to establish a content blocking framework for terrorist and extreme violent material online in crisis events. On 30 June 2019, the Australian Taskforce released a Report providing advice and identifying actions and nine key recommendations,\(^{30}\) consistent with the Christchurch Call to Action, for governments and industry to combat terrorist and extreme violent material online. This included a recommendation for the eSafety Commission to develop a protocol, in consultation with the Communications Alliance, to govern the interim use of the eSafety Commission’s powers to direct ISPs to block websites hosting offending content while a legislative framework is developed.

\(^{29}\) Section 581(2A) of the Telecommunications Act 1997 (Cth).

As noted earlier, there is no net neutrality regulation in Australia, meaning that ISPs are able to reach arrangements that allow them to control, and be compensated for, content transmitted over their networks.

VI THE YEAR IN REVIEW

i nbn™ network

The rollout of the nbn™ network continued in 2018 and 2019 and is on track for a 2020 completion, with FY2019 being the company’s single biggest year for building and activating its network. The number of premises considered ready to connect increased from 7 million in June 2018 to almost 10 million in June 2019. Similarly, the number of premises with active nbn services increased from 4 million in June 2018 to 5.5 million in June 2019.\(^3\)\(^1\)

The rollout continues to make use of the optimised multi-technology mix initially set out in the Minister of Communication’s statement of expectations to nbn of April 2014,\(^3\)\(^2\) and the updated statement of expectations to nbn on 24 August 2016.\(^3\)\(^3\) The multi-technology mix currently involves the use of ‘fibre-to-the-node’ (FTTN), ‘fibre-to-the-building’ (FTTB), ‘hybrid fibre coaxial’ (HFC) and ‘fibre-to-the-curb’ (FTTC) technologies alongside the initial ‘fibre-to-the-premises’ (FTTP), fixed wireless and satellite technologies envisaged in the original design of the nbn™ network.

The multi-technology mix continues to develop, with nbn introducing FTTC technology on 29 March 2018. In October 2017, nbn announced that it intends to use G.fast technology to provide access to faster speeds on the FTTC and FTTB networks. nbn’s trials of G.fast technology to date have achieved speeds of between 500Mbps and 1Gbps in trials. In addition, nbn has announced that it is introducing DOCSIS\(^3\)\(^4\) 3.1 on its HFC network.

During FY2019, nbn has continued its focus on expanding its services to the competitive enterprise markets, primarily through the introduction of nbn™ Enterprise Ethernet in October 2018 and the proposed introduction of nbn™ Business Satellite Services in late 2019. nbn™ Enterprise Ethernet is available within nbn’s fixed line footprint and is supplied using end-to-end fibre network links, which will be built on demand. nbn also launched nbn™ SkyMuster Plus in August 2019 to help meet the ever-growing demand for more data.

The Special Access Undertaking (SAU), accepted by the ACCC on 13 December 2013, applies to wholesale access to the nbn™ network until 2040. In May 2016 and June 2017, nbn submitted proposed variations to its SAU to give effect to the addition of FTTN, FTTB and HFC technologies to the nbn™ network; however, nbn withdrew these variations after the first proposed variation was rejected by the ACCC in March 2017, and following the ACCC’s announcement, in October 2017, that it will delay its decision on the SAU variation.

---

32 Letter from Malcolm Turnbull (Minister of Communications) and Mathias Cormann (Minister of Finance) to Dr Ziggy Switkowski (Executive Chairman of NBN Co), government expectations, 8 April 2014, www.nbnco.com.au/content/dam/nbnco2/documents/soe-shareholder-minister-letter.pdf.
34 Data over cable service interface specifications.
until further progress has been made by nbn in relation to its consultation with customers on its pricing model. Following its continued public comments, and engagement with nbn and industry stakeholders during 2018 and 2019, in relation to potential future pricing and service standards regulation, nbn has not sought further variation of the SAU to give effect to the addition of FTTN, FTTH and HFC technologies to the nbn™ network. nbn separately submitted a variation in March 2019, seeking to extend the dispute resolution, endorsed network change and product development forum processes provisions that expired on 30 June 2019. The ACCC has not made a decision in relation to this proposed variation.

ii 5G spectrum auction
As discussed in Section IV.iv, the ACMA auctioned the 125MHz of available spectrum in the 3.6MHz band in November and December 2018. In preparation for the auction, the Minister for Communications and the Arts has directed the ACMA to impose allocation limits of 60MHz in metropolitan areas and 80MHz in regional areas, limiting the amount of new spectrum that carriers with significant spectrum holding could bid for.

iii Regulatory activity by the ACCC
There has been an increase in regulatory action by the ACCC during 2018 and 2019 with several important regulatory instruments and several regulatory inquiries commenced during the course of the past year:

a On 7 August 2018, the ACCC commenced an inquiry to decide whether to extend, vary or revoke the domestic mobile terminating access service (MTAS) declaration, or whether to make a new declaration. On 28 June 2019, the ACCC announced that MTAS for voice service should be regulated for a further five years and that regulation of MTAS for SMS services should not be extended due to increased competition from messaging services such as iMessage and WhatsApp. On 30 August 2019, the ACCC published its Discussion Paper for its inquiry into Mobile terminating Access Service access determination seeking feedback on whether to extend, vary or revoke the current domestic MTAS final access determination.35

b On 31 August 2018, the ACCC announced an inquiry into existing declarations (due to expire in June 2019) in respect of unconditioned local loop services (ULLS), line sharing services (LSS), wholesale line rentals (WLR), and fixed originating and terminating access services (FOAS and FTAS, formerly known as PSTN OA and PSTN TA respectively). The ACCC extended the declaration of Telstra’s six fixed-line telecommunications, on 26 November 2018. On 12 December 2018, the ACCC commenced an inquiry into making final access determinations for Telstra’s six fixed-line services and for wholesale ADSL, which considered the terms and conditions that should be covered in the final access determination, including the prices for the services and non-price terms and conditions for access. The ACCC released a draft decision, proposing to maintain the same terms of access as the existing final access

determination (as at 30 June 2019) to apply until June 2024. The ACCC is currently consulting with stakeholders on the draft decision for the final access determination, and it is anticipated that the ACCC will release its final decision in November 2019.

c On 12 September 2018, the ACCC accepted a court-enforceable undertaking from nbn to improve its wholesale arrangements with telecommunications retail service providers. The ACCC continued with its next phase of the nbn wholesale service standards inquiry and released a discussion paper on 7 December 2018, which considers whether regulation is required to improve customer experience on the nbn™ network.

d On 23 October 2018, the ACCC released its updated assessment of internet interconnection arrangements, finding that internet interconnection services are available on competitive terms.36

e On 26 October 2018, the ACCC approved Telstra’s proposed variation to the NBN Migration Plan for Special Services.

f On 5 December 2018, the ACCC released a draft report proposing that its declaration or regulation of Australia’s Domestic Transmission Capacity Service (DTCS) continue for further five years after the current arrangement expired on 31 March 2019.

g On 26 July 2019, the ACCC published its final report on its Digital Platforms Inquiry, which investigated the dominance of the leading digital platforms and their impact across Australia’s economy, media and society. The final report concluded that Google and Facebook have substantial market power and made 23 recommendations, including recommending changes to Australia’s merger laws, changes to search engine and internet browser defaults, that a specialist digital platforms branch be established within the ACCC to investigate, monitor and take enforcement against anticompetitive conduct and consumer harm caused by digital platforms, the strengthening of Australia’s privacy laws, and for the harmonisation of Australia’s media regulatory framework.

h On 1 October 2019, the ACCC published its draft decision in relation to its NBN Wholesale Service Standards Inquiry. In its draft decision, the ACCC indicated that it intends to make a final access determination setting out a limited set of terms that relate to the supply of two of nbn’s products, including its primary revenue-generating product, nbn™ Ethernet.

iv Mergers and acquisitions

In August 2018, TPG and Vodafone Australia announced they had entered into a scheme implementation deed for a proposed merger. The A$15 billion merger will combine as TPG Telecom Limited and is subject to approval by the ACCC. On 8 May 2019, the ACCC opposed the proposed merger, stating that Australia already has a very concentrated mobile services market, with the three network operators – Telstra, Optus and Vodafone – having an over 87 per cent share, and that the fixed broadband market is similarly concentrated with Telstra, TPG and Optus having an approximately 85 per cent share. Vodafone and TPG are appealing the ACCC’s opposition to their proposed merger in the Federal Court of Australia.

---

VII CONCLUSIONS AND OUTLOOK

The rollout of the nbn™ network using a multi-technology mix is expected to be completed at the end of 2020, with 100 per cent of the network footprint now in the design or construction stages or completed.

In December 2014, the government released its formal response to the recommendations of the Vertigan Panel, which was appointed to review the regulatory arrangements for the nbn™ network. At the time, the government envisaged a three-stage regulatory reform process for the telecommunications sector to enhance competition, particularly in respect of high-speed broadband networks.

The first stage involved certain transitional measures implemented in 2015 and 2016, such as requiring the functional separation of the wholesale and retail arms of carriers owning superfast fixed-line broadband networks.

The second stage envisaged the establishment of a new telecommunications regulatory framework (intended to have applied from 1 January 2017), which would, among other things, require structural separation between the wholesale and retail businesses of new superfast fixed-line broadband networks and create competitively neutral arrangements for funding nbn’s non-commercial fixed wireless and satellite services. The proposed TRP, described in Section III, seeks to address this stage.

The third stage of the government’s response to the Vertigan Panel’s report involved the lead up to the privatisation of nbn™ network once the network is rolled out and fully operational, and a Productivity Commission review into privatisation has been completed and examined by the government.

Several changes to the regulatory environment for TMT are expected to take place in the short to medium term, including new policy and regulatory interventions in relation to digital platforms, data and privacy. This follows several inquiries into the availability and use of data and digital platforms, including the Productivity Commission’s Inquiry into Data Availability and Use, the ACCC’s Inquiry into Digital Platforms, and the announcement by the Commonwealth Treasury of a consumer data right. The Productivity Commissioner released its Final Report into Data Availability and Use in 2017, with the government accepting the recommendations. The government has progressed with implementing some of these recommendations, including by establishing the National Data Commissioner, legislating the consumer data right, and consulting on the proposed Data Sharing and Release legislation in July 2018.

The government released the draft exposure Treasury Laws Amendment (Consumer Data Right) Bill 2018 on 15 August 2018. The Bill creates a consumer data right (CDR) framework to enable consumers to effectively use data relating to them for their own purposes, including the ability to direct data holders to provide their data to other accredited entities. While the CDR will initially be implemented in the banking sector, the government has indicated that the telecommunications and energy sectors will also be subject to the CDR. The CDR was enacted on 1 August 2019, with the scheme to go live in February 2020.

In July 2018, the Department of Communications and the Arts commenced consultation on the proposed Data Sharing and Release legislation, which would be overseen

and enforced by the National Data Commissioner. The Data Sharing and Release legislation is a legislative framework for the sharing and release of data held by commonwealth entities and commonwealth corporations. The aim of the legislation is to simplify and overcome existing legal impediments to sharing public or government data. Under the existing proposal, the legislation will override other legislative prohibitions on sharing data if certain conditions and safeguards are met, including, for example, protected information under the Telecommunications Act. At the time of writing, a draft exposure bill is yet to be released, but the Office of the National Data Commissioner has published the Best Practice Guide to Sharing Data to promote greater open-data.

The IoT is also expected to develop further in Australia, with likely implications for a range of areas of regulation, including spectrum use, equipment standards, cybersecurity, and privacy and data protection. Regulatory frameworks and policy have not explicitly focused on IoT issues to date, but this is expected to be an area of future development in line with global trends. Programmes such as Adelaide’s smart city initiative announced in 2017, will likely be the testbed for many of these IoT uses in Australia.
Chapter 2

BELARUS

Kirill Laptev and Pavel Lashuk

I OVERVIEW

Building an information society is one of the priorities of the government of the Republic of Belarus. This approach is reflected in the Decision on the Strategy for Collaboration of the CIS States Parties in the Construction and Development of the Information Society for the Period up to 2025 and the Action Plan on its Implementation, adopted on 28 October 2016 in Minsk (CIS Decision). One of the tasks of CIS member states’ cooperation in the construction and development of the information society is the provision of services to citizens and organisations using modern information and telecommunication technologies.

The growth in ICT development approach is a result of the adoption of the State Development Programme of the Digital Economy and Information Society for 2016–2020 (State Programme). The goal of the State Programme is to improve the conditions of transformation of human activities under the influence of ICT, including the formation of the digital economy, the development of the information society and the improvement of e-government.

One of the major innovative developments in Belarus took place on 21 December 2017 when the President signed Decree No. 8 ‘On the Development of the Digital Economy’ fixing progressive and unique regulation in the IT sphere on a global scale, as well as developing a regime for High Tech Park (HTP) residents. HTP has been successfully operating for more than a decade, providing a beneficial taxation system to residents specialising in the IT sector.

The Decree also devotes special attention to the development of blockchain technologies and cryptocurrency payments.

Tokens are recognised as a legitimate object of legal relations. Tax privileges are introduced to operations with tokens, including trade in cryptocurrencies and initial coin offerings. Until 2023, individual revenues from mining and operations with tokens are not subject to declaration and taxation depending on the categories of the subject: a resident of the Belarus HTP, an individual or another entity.

Additionally, the special statuses of cryptographic platform operator and cryptocurrency exchange have been introduced. The Decree sets for them a minimum security value to be stored at Belarusian banks of not less than 1 million and 200,000 rubles respectively (approximately US$500,000 and US$100,000).

Among other privileges and benefits, HTP residents use simplified rules of company document control and a simplified system for foreign founders and employees, which

1 Kirill Laptev is a senior associate and Pavel Lashuk is an associate at Sorainen.
additionally boosts the development of the ICT sector. Foreign employees and founders of HTP resident companies are entitled to visa-free entry to Belarus for the duration of their temporary stay of 180 days.

II REGULATION

i The regulators

The central management body that is responsible for state regulation, coordination of work and development of the telecommunications sector is the Ministry of Communications and Informatisation of the Republic of Belarus (MinCom).

The MinCom carries out:

a development and implementation of telecommunication development programmes;
b coordination of activities in the field of creation and development of telecommunication networks;
c the long-term planning of the use of the RF spectrum by civil electronic radio facilities;
d establishment of a unified procedure for the interaction of telecommunication networks through the public telecommunication network, as well as monitoring and centralised management of the public telecommunication network;
e the definition of requirements for the construction, numbering, organisational and technical support for the operation of telecommunication networks, their management, to ensure the protection of telecommunication networks from unauthorised access to them and messages transmitted thereon, the use of the RF spectrum, the order of traffic transmission, and the provision of telecommunication services;
f regulation of the activities of telecommunication operators;
g international cooperation in the field of telecommunications, including interaction with international organisations and telecommunications administrations of other states, ensuring the fulfilment of obligations under international treaties of the Republic of Belarus; and
h development and adoption of regulatory legal acts.

The Republican Unitary Enterprise for Telecommunications Supervision ‘BelGIE’ (BelGIE RUE) is a state agency that falls under the auspices of the MinCom. Among others, BelGIE RUE has the following main objectives:

a ensuring the protection of the RF spectrum and its effective use;
b assignment of RFs or RF channels;
c RF monitoring; and
d state supervision of telecommunications, etc.

In accordance with Edict No. 515 (see details in subsection ii, below), an Operational Analytical Centre under the President of the Republic of Belarus (OAC) was designated as an independent regulator in the field of ICT. The OAC, in the role of an independent regulator, focuses on ensuring the successful operation of the Unified Republican Data Transmission
Network, which is expected to be designed by 2020 (URDTN\textsuperscript{2}) and the ICT market in the field of data transmission. It also promotes attraction of investments in the ICT sector and development of the telecommunication services market in terms of providing data and telephony services via IP-protocol and monitors the market for data transmission services and analysis of its condition. In 2019, the Republican Unitary Enterprise ‘National Centre for Traffic Exchange’ published information on its website on a new service – the URDTN protected segment. In our opinion this new feature will allow any organisation that needs to receive or send information that is subject to limited distribution according to local law, to connect and use the protected URDTN segment to interact with its counterparties.

The State Commission on Radio Frequencies under the Security Council of the Republic of Belarus implements a unified state policy in the area of distribution and use of the RF spectrum.

The leading operator of the Republic in the telecommunication services segment is Beltelecom RUE.

\section*{Main sources of law}

The main legislative acts regulating the TMT sector in Belarus are the following:

\begin{itemize}
  \item[a] Law of the Republic of Belarus of 19 July 2005 No. 45-Z ‘On Telecommunications’ (the Telecom Law);
  \item[b] Law of the Republic of Belarus of 15 December 2003 No. 258-Z ‘On Postal Communication’ (the Post Law); and
\end{itemize}

In addition, the President of the Republic of Belarus has adopted a number of decrees regulating the TMT sector. In practice, they all have greater legal force than laws, due to the fact that in accordance with the Law of the Republic of Belarus of 17 July 2018 No. 130-Z ‘On Normative Legal Acts’, in the event of divergence of presidential edict or decree with the law, the law has primacy only when the authority to issue an edict or decree has been granted by law.

Thus, the main regulatory presidential acts in the TMT sector are:

\begin{itemize}
  \item[a] Edict of the President of the Republic of Belarus of 18 April 2006 No. 240 ‘On payment for the use of the radio-frequency spectrum’;
  \item[b] Edict of the President of the Republic of Belarus of 1 September 2010 No. 450 ‘On licensing of certain types of activities’ (the Licensing Law);
  \item[c] Edict of the President of the Republic of Belarus of 1 February 2010 No. 60 ‘On measures to improve the use of the national segment of the Internet’ (Edict No. 60);
  \item[d] Edict of the President of the Republic of Belarus of 30 September 2010 No. 515 ‘On certain measures for the development of the data transmission network in the Republic of Belarus’ (Edict No. 515);
\end{itemize}

\textsuperscript{2} URDTN construction will allow for the centralised management of data transmission networks in Belarus, and create conditions for accelerated economic growth in the field of communications by eliminating administrative barriers. It is also planned that the business sector will be able to use the services of the URDTN.
Edict of the President of the Republic of Belarus of 15 April 2013 No. 192 ‘On the allocation, use of the radio-frequency spectrum and introduction of changes and additions to Presidential Decree of 31 July 2006 No. 473’;

Edict of the President of the Republic of Belarus of 23 January 2014 No. 46 ‘On the use of telecommunication technologies by state bodies and other state organisations’; and

Edict of the President of the Republic of Belarus of 15 March 2016 No. 98 ‘On the improvement of the procedure for the transmission of telecommunications messages’.


The State Security Committee of the Republic of Belarus and the Ministry of Internal Affairs of the Republic of Belarus, having consistently formed the legal framework for ensuring the safety of critical facilities in Belarus, adopted Joint Resolution No. 24/268, which approved the Regulations on Preventive, Regime and Organisational Measures to prevent terrorist activities and minimisation of their consequences at critical objects of the Republic of Belarus.

As part of the work carried out in this field in the Republic of Belarus, on 25 October 2011 Edict of the President of the Republic of Belarus No. 486 ‘On some measures to ensure the safety of critical information facilities’ was signed, which approves the Regulation on the assignment of information objects to critical and security critical objects of informatisation.

The Regulation defines the notion of a ‘critically important object of informatisation’, and establishes the procedure for classifying objects of informatisation as critically important and ensuring the security of critical information objects.

iii Regulated activities

Communications

The TMT sector is strictly regulated by numerous state authorities. In this context, according to the Licensing Law the provision of main telecommunication (TCM) services is subject to obtaining a licence. Such licensed activities include:

a public TCM services:
  • international telephone communication;
  • long-distance (inter-city) telephone communication; and
  • local telephone communication;

b data transfer service;

c VoIP;

d IPTV;

e mobile TCM service (except cellular communication);

f TV transmission;

g wireless sound programme broadcasting;

h fixed and mobile satellite TCM services; and

i cellular communication.

The Licensing Law also outlines the following public postage services:

a mail transfer; and

b receipt of a subscription to a printed mass media and printed media delivery.

The Licensing Law expressly outlines the activities that may be conducted without a licence:

a rendering telematic services (except for VoIP and IPTV services);
The licence for communication services may be granted after an application has been made or as a result of tender proceedings (e.g., for RF spectrum usage). In any case, the licence is issued by the MinCom for a unlimited period.

Media

There are certain additional authorisations needed to carry out activities in the media sector. According to the Mass Media Law, the mass media (e.g., printed mass media, TV or radio programmes and channels) is subject to a state registration procedure. It may be distributed from the date of its inclusion in the State Register of Mass Media.

TV and radio broadcasting in Belarus is additionally subject to obtaining a licence, which may be obtained by the editor of the mass media or by a foreign organisation.

A broadcasting licence is required for mass media editors and foreign companies broadcasting a TV channel or a radio channel in Belarus. The licence is not required if the TV and radio broadcasting is carried out by a telecommunications operator without changing the form and content thereof:

- on the basis of a permit to distribute the products of a foreign mass media;
- under a contract with a legal entity entrusted with the functions of the editor of the mass media; or
- if the foreign organisation has a licence in the field of broadcasting.

iv Ownership and market access restrictions

Belarusian law establishes certain ownership restrictions within the TMT sector.

In the TMT sector certain restrictions apply in the foreign participation and investments area. Generally, a mass media editor cannot register its mass media if a foreign state, entity, individual, international entity or individual without citizenship owns 20 per cent or more of its shares.
So as spectrum is considered a rare resource, its management and use is reserved to the state. It is particularly reflected in the application of a tender procedure for obtaining a licence.

According to the Decision of the Operational Analytical Centre under the President of the Republic of Belarus, the Ministry of Communications and Informatisation of the Republic of Belarus of 10 February 2014 No. 1/2 ‘On approval of the list of telecommunication operators entitled to pass inter-network traffic’ only three state-owned entities are authorised for internetwork traffic transmission. Two of them are additionally authorised for international traffic transmission.

The Order of the Operational Analytical Centre under the President of the Republic of Belarus of 6 December 2012 No. 91 ‘On Approving the List of Telecommunication Operators Eligible to Pass International Traffic and Join Foreign States to Telecommunication Networks’ provides that only two telecom operators are entitled to pass international traffic and join foreign states to telecom networks.

v Transfers of control and assignments
As a general rule, communication licences may not be transferred or assigned to third parties. TMT licences may only be granted to legal entities of Belarus.

Mergers and acquisitions of ICT entities are subject to general antitrust legislation requirements.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation
The internet and internet protocol is a developing sphere of Belarusian law. As a result, Belarusian law is structured as technology-neutral and does not provide specific legislation for internet and internet protocol services. Such services are mainly regulated by the general TMT legislation.

ii Universal service
In accordance with the Decree of the President of the Republic of Belarus No. 130 of 19 March 2015 ‘On the State Non-Budgetary Fund’, Belarus has set up a state target budgetary universal service fund. All telecoms operators operating in Belarus transfer 1.5 per cent of their revenues to the State Non-Budgetary Fund. The fund’s managers are the MinCom and state bodies that are customers of state programmes (subprogrammes), determined by the President. Funds have a special purpose, in particular, compensation for the capital construction of infrastructure for the provision of universal telecommunication services. Universal telecom services include access services to the fixed telecommunication network using the terminal subscriber unit and the internet at points of shared use.

In accordance with the Order of the MinCom dated 19 October 2006 No. 297, the functions of compulsory provision of universal postal services throughout the territory of Belarus are assigned to the Republican Unitary Enterprise Postal Communication Belpochta (Belpochta RUE).
iii Restrictions on the provision of service

Although telecoms operators are generally free to establish the prices for their services, Belarusian law establishes certain price limits charged to end users. The Ministry of Antimonopoly Regulation and Trade (MART) is the main regulatory authority for the specification of such thresholds. It carries out state price regulation for telecommunication services and postal communication of public service according to the list determined by the Resolution of the Council of Ministers of 17 January 2014 No. 35 ‘On approval of lists of socially significant goods (services), prices (tariffs) which are regulated by state bodies, and the recognition of certain decisions of the Council of Ministers of the Republic of Belarus as invalid’ (Price Regulation List). The Price Regulation List has a tendency to liberalisation through the exclusion of the telecom services state pricing regulation applies for. The granting of access to the internet at points of shared use was excluded in 2017 from the Price Regulation List.

As a general rule, telecoms operators are obliged to provide their services to everyone who applies for them, and may not prefer one person to another in relation to the conclusion of a contract for the provision of the services. Refusal to conclude a contract with an opportunity to provide services at hand is prohibited.

Restrictions on access to internet resources and online media shall be made if:

a owners of the internet resource during the year were issued two or more demands, or, for owners of the online media, two or more written warnings from the Ministry of Information (MinInfo);

b it contains information that is prohibited or restricted from distribution in accordance with the legislative acts of the Republic of Belarus, as well as legally enforceable court decisions (hereinafter, ‘information that is prohibited from distribution’); or

c the owners of the internet resource did not comply with the lawful demand of the MinInfo to eliminate violations of the legislation of the Republic of Belarus on the mass media or did not notify MinInfo and did not provide documentary evidence on such elimination.

After the MinInfo decides to restrict access it submits its decision to the BelGIE RUE. Subsequently, BelGIE RUE forms the list of restricted access, which is the ground document to be followed by ISPs in further direct restriction of access procedure.

iv Privacy and data security

The basic confidentiality concept is contained in Article 28 of the Constitution of the Republic of Belarus (Constitution). It provides that everyone has the right to protection from unlawful interference in their private life, including interference with correspondence, telephone and other communications, and protection of their honour and dignity.

Lawful interference is mainly regulated for national security purposes by the Communication Law, the Information Law, the Law of the Republic of Belarus of 15 July 2015 No. 307-Z ‘On Investigative and Search Activity’, the Code of Criminal Procedure and other legislative acts. According to the mentioned legislation, lawful interference covers a broad scope of measures, including reception, transformation and recording of data and messages received, transmitted, processed, stored in telecommunication networks as well as identification of service receivers.

The Communication Law prescribes network operators’ obligations when carrying out investigative and search activity, inter alia:
a to provide information on users of telecom services and on the telecom services rendered to them, as well as other information necessary to fulfil the tasks assigned to investigative bodies;

b to assist in carrying out investigative and search activities and to provide an opportunity to conduct them on TMT networks, to take measures to protect information about organisational and tactical methods for carrying out these activities; and

c to provide access to databases, automated systems, etc.

IV Spectrum Policy

i Development

Regulation of the use of the RF spectrum is the exclusive right of the state. Edict of the President of the Republic of Belarus of 31 July 2006 No. 473 ‘On the State Commission for Radio Frequencies under the Security Council of the Republic of Belarus’ regulates the use of the RF spectrum in Belarus to the State Commission on Radio Frequencies under the Security Council (Commission). The Commission decides on the allocation of RF bands, RF channels and RFs, and organises work on the conversion of the RF spectrum.

Owing to the wide development of modern radio technologies and new RF bands, the government of Belarus amended the procedure for determining the amount of annual, one-time fees and fees for allocating the RF spectrum. The Council of Ministers adopted Resolution No. 853 of 16 November 2017, according to which amendments were made to the amounts of the annual, one-time payments and fees for allocation of the RF spectrum.

The indexes of the commercial value of the K1 RF spectrum, used in calculating the amount of spectrum charges, have been adjusted to create conditions for the successful development of the LTE cellular telecom network in the 2.6GHz band and to encourage the development of the LTE Advanced networks in Belarus.

So the cost index for the spectrum of 2.4835GHz–2.7GHz, where mobile operators operate, has been reduced almost five times – from 5 to 1.1.

ii Flexible spectrum use

Belarusian law does not provide for much flexibility owing to the lack of free space in almost the entire RF range. Hence it is quite heavily regulated.

iii Broadband and next-generation services spectrum use

One of the significant steps in liberalisation of RF spectrum usage was made in 2016. The MinCom, on 29 August 2016, adopted Resolution No. 13, which entered into force on 21 September 2016. With the entry into force of the Resolution, it is possible to use, without registration and permits for the operation of broadband radio access equipment of the IEEE 802.11 group of standards (Wi-Fi technology) both inside buildings and structures and in vehicles, as well as a wide range of low-power devices of GSM, UMTS and LTE technologies, radio stations of seagoing ships that have the right to sail under the Belarus national flag. It is possible to use certain types of satellite subscriber terminals without the need to obtain permits for their operation.

Today in Belarus there is an infrastructure operator called beCloud, which is engaged in the development of LTE networks and allows other companies to operate them to provide services to their subscribers.
iv Spectrum auctions and fees

Belarusian law imposes spectrum usage fees on broadcasters, mobile phone carriers and other businesses that use the RF spectrum. The President of Belarus may stipulate cases when the issuance of licences for the provision of certain components of the licensed services is carried out following the results of a tender for a licence. Pursuant to this, Resolution of the Council of Ministers of the Republic of Belarus No. 1259 of 30 September 2009 establishes the Regulation on the procedure for conducting a tender (competition) for the use of the RF spectrum.

The legislative acts establish both a one-off fee and an annual fee for the use of the RF spectrum.

V MEDIA

i Regulation of media distribution generally

While the Mass Media Law guarantees freedom of opinion, belief and expression to everyone in Belarus, it also establishes certain restrictions on information that may be disseminated through mass media. Among others, the following information is prohibited:

- a the calling for the consumption of narcotic drugs, psychotropic substances, their analogues, toxic and other intoxicating substances, and dissemination of information on the methods of their development, production and consumption;
- b the calling for and promotion of war, extremist activities, pornography or violence; and
- c information, disseminated by the entity without due state registration, if any needed; etc.

Since 1 December 2018 the Mass Media Law has contained a definition of ‘internet resource’: a website, web page, forum, blog, application for a mobile device, other information resource (its component), located on the global computer network internet, through which mass media is distributed. Unless indicated otherwise, the Mass Media Law applies to internet resources. Internet resources may be registered as online media and, consequently, be treated as mass media under the Mass Media Law.

Certain regulations apply specifically to internet resources. The Mass Media Law provides for a number of duties for internet resource owners, including social network owners, which involve the introduction of additional measures for analysing and monitoring information on such internet resources. In particular, further to the Mass Media Law requirement, the Regulation on the procedure for preliminary identification of users of an internet resource, an online media approved by the Resolution of the Council of Ministers of the Republic of Belarus of 23 November 2018 No. 850 ‘On approval of the Regulation on the procedure for preliminary identification of users of an internet-resource, an online media’ elaborates the requirements of user identification. The owner of the internet resource or online media will identify users when leaving a message in the comments or on the forum via the SMS verification mechanism.

ii Internet-delivered video content

Internet services are available in Belarus, including IPTV channels with programming provided by programme providers. Current legislation does not provide for internet delivered video content (OTT) regulation.
The need for OTT services regulation was discussed during a roundtable in Minsk by representatives of the MinInfo, interested departments, television channels, cable operators and the Telecommunications Industry Union. The chairman of the Telecommunications Industry Union outlined that owing to the absence of regulation, telecommunication operators working in the lawful field faced unfair competition from OTT services. They lead away subscribers – the annual outflow of subscribers is at least 10 per cent. In most cases, OTT services do not pay taxes, they are not registered in the register of distributors, that is, they provide TV programmes without contracts with rights holders, do not pay for related rights, do not make contributions to the National Centre of Intellectual Property, and do not distribute mandatory programmes of the public package.

OTT services are planned to be regulated by government rules and regulations in the future.

VI THE YEAR IN REVIEW

Considering the events of the year, we can say that Belarus is charting a course for the development of its IT infrastructure in many areas.

In spring 2019, modern driverless vehicles were tested at the first ‘5G’ test zone in Belarus. According to the publicly announced information, the technologies used by the standards of New Radio and LTE-Advanced Pro allowed specialists to test driverless vehicle control, as well as the operation of dump trucks in robot mode (project ‘Intelligent quarry’). In June 2019, the Draft Law on Personal Data (the Bill on PD) passed first reading by the lower Chamber of Parliament. The Bill on PD is still under review in Parliament and is expected to come in force not earlier than the end of the 2020. Generally, the Bill on PD follows the basic concept of the GDPR, including the main principles of ensuring data privacy, however it is still not very detailed and mostly uses different terminology compared to the GDPR.

In particular, if the Bill on PD enters into force in the wording available now, it will provide for the establishment of a state body (‘the Data Protection Authority’) specially authorised for regulating personal data protection issues. According to the Bill on PD the Data Protection Authority will be appointed by the President of the Republic of Belarus. It also plans to regulate transfer of personal data abroad from Belarus. In particular, the cross-border transfer of personal data to countries not ensuring sufficient measures of personal data protection will be prohibited subject to a limited number of exceptions (e.g., individual permit of the Data Protection Authority).

In August 2019, the Belarusian mobile telecom operator A1 (from A1 Telekom Austria group) started offering eSIMs to its customers – the first among Belarusian telecom operators. Currently Belarus law does not provide specific regulation of the eSIM solution.

The cryptocurrency activities of HTP residents received full comprehensive legislative support from the regulator. The administration of the HTP together with the National Bank, the Department of Financial Monitoring of the State Control Committee, international experts and other bodies developed documents establishing the requirements for the activities with cryptocurrencies. In particular, HTP checks the reputation of the staff and owners of the company, their financial condition, origin of assets and cybersecurity of the residents who want to work in the field of cryptocurrencies.
VII CONCLUSIONS AND OUTLOOK

The development of TMT in Belarus in increasing frequency comes with a lack of relevant legislation while having progressive legislation in particular spheres. During the process of post factum regulation the government is trying to steer a middle course between national interests for TMT infrastructure control and development of the TMT sector by private investors. Depending on the particular approach in different ICT spheres, development of both legislation and the ICT sector itself affects national economy indexes as well as development of the information society. At the same time, Belarus is trying to implement and follow the strategy of front-running rather than pursuing in the field of technology regulation and use.

The 2019 government approach towards formation of law is subject to particular world TMT trends. The data protection, mass media, cryptocurrency and other TMT-related regulations are the primary focus. The business community expects a boost in the development of TMT legislation because of the world technology progress and certain politically sensitive events expected to occur in 2020.
Chapter 3

BRAZIL

Ademir Antonio Pereira Junior, Luiz Felipe Rosa Ramos and Yan Villela Vieira

I OVERVIEW

The regulatory landscape for the technology, media and telecommunications (TMT) industry in Brazil witnessed important changes in 2019. As services converge to distribution via the internet (i.e., ‘over-the-top’ – OTT), broadband infrastructure becomes increasingly critical for access to content and communication.

Furthermore, the Brazilian General Data Protection Act (LGPD) will come into force in August 2020 and will affect TMT companies on nuclear dimensions, dealing with issues common to all industries (such as data in HR departments) and more specific topics such as cookie policies or direct marketing.

Given their experience and knowledge, TMT companies are qualified to play a leading role in the discussions on the interpretation and regulation of LGPD’s legal provisions. The conceptual framework of the LGPD leaves room for an enforcement attentive to both the necessary insertion of Brazil in international best practices regarding data protection and to specificities of the national context.

We present below an overview of the Brazilian landscape, detailing its main changes in 2019 and trends for 2020.

II REGULATION

i The regulators

TMT services are regulated by two different agencies in Brazil. The National Telecommunications Agency (Anatel) regulates telecom services, which include fixed telephony, mobile telephony and internet, fixed broadband and pay-TV distribution. Anatel has powers to grant (and forfeit) licences for regulated services, issue regulations and guidelines, control the use of spectrum and orbital slots, supervise the quality and safety of services and products, oversee compliance with net neutrality rules, authorise transfers of control among telecoms and impose fines for regulatory infringement.

The other agency regulating TMT in Brazil is the National Cinema Agency (Ancine). It regulates audiovisual services, which include making and distribution of films and production, programming and packaging of pay-TV content. Ancine manages the National Audiovisual Fund (FSA), providing resources to foster Brazilian audiovisual productions. The agency also has powers to fight piracy and impose fines for regulatory infringement.

1 Ademir Antonio Pereira Junior is a partner, Luiz Felipe Rosa Ramos is a senior associate and Yan Villela Vieira is an associate at Advocacia José Del Chiaro.
Finally, free-to-air television and radio broadcasting are subject to the direct authority of the Ministry of Science, Technology, Innovations and Communications (MTIC).

ii Main sources of law
The main source of law for telecom services is the General Telecommunications Act (LGT).\(^2\)

It was significantly altered by a bill signed into law in October 2019 (PLC 79).\(^3\) Regulations issued by Anatel are also an important source of rules regulating the industry.

For media services, the main sources of law are the SeAC Act\(^4\) (applicable to pay-TV) and the Brazilian Telecommunications Code\(^5\) (applicable to free-to-air television and radio broadcasting).

iii Regulated activities
Telecom services may be provided under public or private regimes. Those provided under the public regime require a type of licence called ‘concessions’, which are auctioned and heavily regulated, implying substantial costs. In turn, services provided under the private regime require ‘authorisations’, which are less regulated and generally do not need to be auctioned.

Until recently, fixed telephony had to be provided under the public regime, which imposed significant costs over telecommunication companies. However, PLC 79 addressed an old industry request and allowed telecommunication companies to ask Anatel to switch to the private regime, subject to Anatel's approval. As another requirement to switch to the private regime, companies must commit to use the resources they will save with this switch in broadband infrastructure expansion. Thus, all telecom services may be offered under the private regime now, a substantial change in the regulatory landscape.

To obtain an authorisation, companies must submit to Anatel a request with the required documentation. The agency provides specific requirements for each type of service. In general, companies must be in good standing regarding tax obligations and prove they fulfil certain legal, financial and technical qualifications. Authorisations are valid for 20 years and may be renewed for equal periods.

Use of spectrum is also conditioned on authorisations by Anatel, which are auctioned and valid for 20 years, renewable for equal periods. PLC 79 addressed another old industry request and allowed telecoms to transfer spectrum use authorisations among themselves (conditioned to approval by Anatel), thus creating a ‘market’ for spectrum use. The use of orbital slots is conditioned to a grant auctioned by Anatel and valid for 15 years.

Finally, the offer of free-to-air television and radio broadcasting is conditioned to concessions from the MTIC, which are auctioned and valid for 15 years, renewable for equal periods.

iv Ownership and market access restrictions
There are restrictions on foreign ownership of telecommunication companies in Brazil. First, under the LGT, only companies headquartered and incorporated under the laws of Brazil can obtain authorisations to offer telecommunication services.

---

\(^2\) Law No. 9,472/1997.
\(^3\) PLC 79 was signed into Law No. 13,879/2019.
\(^4\) Law No. 12,485/2011.
\(^5\) Law No. 4,117/1962. Decree No. 52,795/1963 provides additional regulation based on this statute.
Similarly, concessions for free-to-air television and radio broadcasting can only be obtained by companies headquartered in Brazil, incorporated under the laws of Brazil and with at least 70 per cent of voting capital owned by Brazilian citizens or companies headquartered and incorporated under the laws of Brazil.

The SeAC Act also prohibits cross-ownership between content producers and telecom operators: free-to-air television broadcasters and pay-TV content producers cannot own more than 50 per cent of the capital of pay-TV distributors. Likewise, pay-TV distributors cannot own more than 30 per cent of the capital of free-to-air television broadcasters and pay-TV content producers. These restrictions have been subject to strong criticism recently and Congress is discussing a bill to eliminate them. Given the advanced stage of debates in Congress, some consider that a bill eliminating restrictions on cross-ownership may pass by the end of 2019 or the beginning of 2020.

v Transfers of control and assignments

Transfer of control over telecommunication companies (e.g., via mergers and acquisitions) requires clearance from Anatel. Under the agency’s regulation, control means ‘the powers to directly or indirectly, internally or externally manage the company’s activities or operations’. Anatel also considers as ‘controllers’ any persons who have powers to indicate members in the board of directors and managers, veto rights, rights to stay deliberations in the board of directors or rights to cast separate votes to fulfil managing positions.

To obtain clearance from Anatel, companies must file a request with the required documentation showing they are in good standing regarding tax obligations and that the acquiring party fulfils certain legal, financial and technical qualifications. The agency will clear the transfer of control if all qualifications are fulfilled and the transaction is not likely to harm competition or degrade the quality of services provided to consumers. There is no time limit for Anatel to conclude its assessment and timing varies significantly according to the complexity of the case.

In contrast, transfer of control of free-to-air television and radio broadcasters does not require a formal clearance procedure and must only be notified to the MTIC.

Finally, it is important to highlight that transfers of control may also be subject to mandatory filing before the Federal Antitrust Agency (CADE). The Brazilian Competition Act establishes that notification of mergers, acquisitions, joint ventures and associative agreements is mandatory where:

\[ a \] the corporate group of one party to the transaction had a turnover of at least 750 million reais in Brazil in the year preceding the transaction; and
\[ b \] the corporate group of another party to the transaction had a turnover of at least 75 million reais in Brazil in the year preceding the transaction.

Parties must provide CADE with all documents and information necessary for the assessment of the transaction’s impacts on competition. The proceeding at CADE is totally independent of the assessment carried out by Anatel and imposes a standstill obligation (parties must not

---

7 As provided by Anatel Regulation No. 101/1999.
8 Law No. 12,529/2011.
consummate the deal before clearance). CADE has up to 240 days to rule on mergers but normally takes less than 30 days in cases eligible for fast-track review (e.g., low overlaps, lack of overlap or vertical integration, etc.).

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

While the provision of internet access (via mobile or fixed broadband) is considered a telecommunication service and thus regulated by Anatel, internet and IP-based services (i.e., OTTs) are considered ‘value added services’ and are not subject to specific regulation. There are ongoing discussions concerning whether OTTs that deliver content in the format of live streaming of TV channels (instead of on-demand or library services) are subject to the same regulation applicable to pay-TV distributors (see Section V below for more detail).

Rights and obligations applicable to the use of internet were established by the ‘Internet Bill of Rights’ passed in 2014.9 Notably, the Bill of Rights established that internet providers must comply with net neutrality rules (i.e., they must treat equally all data packages irrespective of content, origin, destination, service, terminal or application). Traffic discrimination or degradation is only accepted to deal with technical requirements or to prioritise emergency services. Anatel has powers to oversee compliance with these rules.

Finally, it is worth mentioning that the Internet Management Committee (CGI.br), a multi-sectoral organisation, issues recommendations on technical standards for the internet, allocation of IP addresses and management of domain names. CGI is not a regulator and its decisions are not binding. Domain names ending in ‘.br’ and IPv4/IPv6 addresses in Brazil are registered and maintained by NIC.br, a private entity created by CGI.br.

ii Universal service

While access to fixed and mobile broadband has increased significantly over the past decade, universalisation of access to broadband connection remains a challenge in Brazil. The Brazilian government and Anatel have jointly worked on plans to expand broadband infrastructure to peripheral areas, but there is a general perception that these plans achieved limited success.

Construction of broadband infrastructure is mostly handled by the private sector. PLC 79 is expected to spur investments in broadband infrastructure.

iii Restrictions on the provision of service

Generally, prices and conditions of services are freely established by telecommunication companies. However, services offered to the public cannot be unreasonably denied to specific customers. Furthermore, Anatel also issues regulations seeking to guarantee a minimum level of quality and continuity of telecommunication services.

With regard to the provision of internet connection, the Internet Bill of Rights establishes that internet service providers can only discontinue customers’ access in case of payment default. This led to debates in previous years on whether operators could impose data caps for use of fixed broadband connection. In 2016, Anatel issued an administrative

9 Law No. 12,965/2014.
order prohibiting data caps in fixed broadband connection until a regulation on this issue was enacted, but the matter has not evolved since then. Data caps on mobile broadband access are a common market practice and Anatel has not taken issue with that.

Moreover, as seen above, the Internet Bill of Rights establishes that internet service providers must comply with net neutrality rules, so they cannot favour certain services, content or applications. In 2017, CADE closed without charges a probe that investigated whether zero rating agreements infringed competition law. In this proceeding, Anatel and MTIC filed submissions indicating that zero rating does not violate net neutrality rules.

Finally, laws in several states prohibit telemarketing companies from making unsolicited calls to customers who put their phone numbers on lists asking not to be contacted.

iv Privacy and data security
In July 2018, the LGPD was approved. It was later amended by a Provisional Measure converted into law in July 2019.

With the LGPD, Brazil positions itself in a global context of stricter policies regarding data protection. Its framework and principles are largely inspired by the European Data Protection Regulation (GDPR).

The LGPD will come into force in August 2020. Its application is transversal, reaching the most diverse industries. TMT companies will be affected on nuclear dimensions, both on issues common to all industries (such as data in HR departments) and more specific to their business activities (such as cookie policies or direct marketing).

Basic definitions
All processing of personal data, both online and offline, is subject to the LGPD.

Personal data is defined by the LGPD as any information related to an identified or identifiable natural person. This definition encompasses all information that can identify a living human being. If interpreted accordingly to the European experience (whose legislation presents similar wording), personal data means both objective and subjective information regarding an individual. For example, ‘[the employee] is the legal manager’ or ‘[the employee] is a good professional and deserves promotion’ would both qualify as personal data.

The more elements related to a natural person, the greater the chance that such individual is identifiable. Hence, the greater the risk associated with the use of this data. Age alone might not be enough information to identify an individual working at the legal department of a firm. But such information can be personal data if added to other pieces such as gender, position and remuneration.

‘Sensitive’ personal data is subject to stricter regulation under the LGPD, as discussed further below. It refers to health, sex life, genetic or biometric data, racial or ethnic origin, religious conviction, political opinion, union membership or religious, philosophical or political organisation.

‘Processing’ (the LGPD uses the word ‘treatment’) means essentially any operation involving personal data, including ‘collection, production, reception, classification, use,
access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination or extraction'.15

Anonymised data is defined as data related to a subject that cannot be identified, considering the use of reasonable technical means available at the time of its treatment.16 It is not considered personal data under the LGPD, except ‘when the process of anonymisation to which they were submitted is reversed, using exclusively their own means, or when, with reasonable efforts, it can be reversed’.17

Finally, the ‘processing agents’ are defined in the LGPD as follows:18 (1) the controller is the natural person or legal entity responsible for the decisions regarding the processing of personal data; and (2) the processor (or ‘operator’) is the natural person or legal entity that carries out the processing of personal data on behalf of the controller.

Fundamental obligations and penalties

Under the LGPD, every processing (or ‘treatment’) of personal data must have a specific legal justification or basis, comply with data protection principles, respect the rights of data subjects (i.e., the individuals to whom the data relates) and follow governance rules.

One of the lawful bases for processing personal data is consent by the data subject. Consent must be free, informed and unequivocal.19 In addition to such stringent criteria, the data subject can revoke consent at any time.

Another lawful basis established in the LGPD is a contract entered into with the data subject.20 An employer that needs employees’ financial data to process payment of salaries might base the collection of such data on the employment contract. Data processed under a contract (or consent) must be available in an electronic copy and in a format that allows its subsequent use in other processing operations.21 Such obligation triggers the right to portability, as discussed below.

A third lawful basis for processing personal data worth mentioning in the present chapter is legitimate interest. Under this justification, the interest of the controller or a third party must be weighed against the fundamental rights and freedoms of the data subject.22 Nevertheless, legitimate interest cannot serve as a basis to process sensitive personal data. A data protection impact assessment is recommended, as it can be requested by the Data Protection Authority (DPA).23

In addition to relying on one of the lawful bases for processing personal data, controllers and processors must act in good faith and observe other principles established by LGPD.24 Principles like purpose, adequacy and necessity determine that the processing shall have specific purposes and be compatible with such purposes. Processing must be limited to the minimum necessary for the accomplishment of specific purposes.

15 Law No. 13,709/2018 (Article 5, X).
16 Law No. 13,709/2018 (Article 5, III).
17 Law No. 13,709/2018 (Article 12).
18 Law No. 13,709/2018 (Article 5, VI and VII).
19 Law No. 13,709/2018 (Article 7, I).
20 Law No. 13,709/2018 (Article 7, V).
21 Law No. 13,709/2018 (Article 19, Section 3º).
22 Law No. 13,709/2018 (Article 7, IX).
23 Law No. 13,709/2018 (Article 10, Section 3º).
24 Law No. 13,709/2018 (Article 6).
Free access, quality and transparency must also be observed in processing personal data. They mean that the data subject may require information about the processing free of charge and that accuracy of the data must be guaranteed.

According to the principles of security and prevention, technical and administrative measures must be adopted to protect data from unauthorised access and accidents. Measures should also be taken to prevent damage due to the processing of personal data.

The LGPD also establishes the principle of non-discrimination, which means processing may not be carried out for unlawful or abusive discriminatory purposes.

An overarching principle of the LGPD is accountability: controllers and processors must demonstrate they have adopted effective measures to comply with data protection regulation.

There are several subject rights in the LGPD that relate to such principles and obligations. The data subject has the right, for example, to obtain confirmation of processing (when and why the processing has occurred and who it has been carried out by) and to correct incomplete, (objectively and subjectively) inaccurate or outdated data.

A right that should be emphasised is the right to data portability. Upon express request of the data subject, the controller must make the data available to subsequent use by other organisations. Most likely, the right to data portability will not embrace inferences or analysis made by the controller using the data.

To comply with such obligations, controllers and operators shall formulate rules of good practice and governance that establish several aspects related to processing of personal data. Among such aspects are safety standards, educational actions, and internal mechanisms of supervision and mitigation of risks.

In the case of violation of the LGPD, controllers and operators are subject to fines of up to 2 per cent of turnover limited to 50 million reais, as well as publication of the infraction, blocking or elimination of personal data. Recently, a veto to the sanction of suspension of processing activities was overturned by Congress, so controllers and operators may also have their processing activities suspended if they fail to comply with the LGDP.

The LGPD also provides that, when calculating the fine, the DPA may consider the total turnover of a group when the turnover ‘in the area of business activity in which the violation occurred’ is not available. Such provision will likely trigger relevant discussions as to how to define ‘the area of business activity’. The experience of the Brazilian antitrust agency (CADE) with this matter should not be overlooked.

The infringement of the LGPD may lead to collective and individual actions by injured parties for damage compensation. The data subject also has the right to petition to consumer protection authorities. Controllers and processors can be held jointly liable under certain conditions of Article 42.

Issues regarding technology, media and telecommunications

The conceptual framework of the LGPD leaves room for an enforcement attentive to both the insertion of Brazil in international best practices and to specificities of the national context. The TMT industry has the potential to play a leading role in the discussion on the interpretation and regulation of the LGPD’s legal provisions.

---

25 Law No. 13,709/2018 (Article 50).
26 Law No. 13,709/2018 (Article 52).
27 Law No. 13,709/2018 (Article 52, Section 4º).
To achieve an effective and balanced enforcement, the Brazilian DPA should observe the requirement of minimum intervention, as established in Article 55-J, Section 1º of the LGPD. Enforcement should be oriented to preserve incentives to innovation and the essence of regulated sectors.

The LGPD’s transversal application to several sectors raises areas of possible conflicts. The right to petition to consumer protection authorities is an example – Article 18, Section 8º of the LGPD ensures consumers of media services, for instance, the right to petition ‘with regard to their data’ to consumer authorities. Enforcement of the law will need to establish limits and a productive dialogue in the relationship between data and consumer protection authorities.

Another example is the interface between data protection and competition law. There could be allegations of LGPD violations that supposedly represent harm to competition, such as the Facebook case in Germany. For example, one could argue that a TMT firm that obtains a large amount of data in violation of the LGPD could behave in ways that harm consumers and competitors. CADE will need to carefully assess whether there is reason to incorporate violations of the LGPD as an antitrust concern.

Moreover, concerns with privacy are not a novelty in the Brazilian legal landscape. In addition to the Federal Constitution and the Internet Bill of Rights, the LGT provides, in its Article 3, IX, that the user of telecommunication services is entitled to the respect of their privacy in the billing documents and in the use of personal data by the service provider. The duties of Anatel in observing such obligation should be harmonised with the DPA’s responsibilities on the same matter.

Specific matters relating to internet technology and communications, as well as direct marketing, will need to be defined in Brazil. The Brazilian DPA will need to define whether prior consent is necessary for using cookies and whether internet users can be deemed to have consented by using a browser that allows cookies. It will also regulate whether there is a difference between first-party cookies (used to advertise an operator’s own products or to tailor its own website) and third-party cookies (sent by an entity other than the website operator).

Another matter to be defined is the disclosure of personal data through social network services (SNS). The LGPD states that the requirement of consent is waived for general data made manifestly public by the data subject. One will need to interpret what ‘making manifestly public’ means in the context of SNS, as well as its extension to sensitive data.

The increasing use of the internet of things (IoT) will also raise issues regarding the appropriate security measures to ensure networks connected to IoT objects, as well as the need to consent to the processing of personal data in this context. The Brazilian DPA will certainly need to face such challenges.

As to direct marketing, there will be discussions about whether opt-in is required or opt-out is sufficient, considering eventual differences between means such as postal marketing, telephone marketing and marketing by electronic mail. Programmatic media and online behavioural advertising will add complexity to the analysis of the DPA.

28 Bundeskartellamt, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing (6 February 2019), B6-22/16, 2.
29 Law No. 12,965/2014.
30 Law No. 9,472/1997.
Technology, media and telecom organisations must be alert to the development of such matters in the Brazilian context. Reputational damage tends to be significant in the event they fail to comply with data protection requirements, especially to firms inserted in a digital economy highly based on trust. An image of careless data processing might be fatal to trust from consumers and employees.

IV  SPECTRUM POLICY

i  Development
Use of spectrum is conditioned to authorisations auctioned by Anatel. As seen in Section II, the most significant change regarding spectrum policy was the creation of a ‘market’ of authorisations by PLC 79.

Moreover, Anatel introduced new rules limiting ownership of spectrum bands in late 2018. Under these rules, a telecommunication company cannot control more than 35 per cent of bands below 1GHz and 30 per cent of bands between 1GHz and 3GHz. Anatel is considering similar limitations on control over bands above 3GHz.

ii  Flexible spectrum use
Anatel started considering how to regulate flexible spectrum use in 2018, but this matter has not developed since then. Related to flexible use, radio access network (RAN) sharing agreements are lawful, but subject to approval by Anatel.

iii  Broadband and next-generation services spectrum use
In previous years, the 450MHz, 700MHz, 1.9GHz, 2.1GHz and 2.5GHz bands were auctioned for use by 3G and 4G broadband technology services. In May 2019, Anatel established that the 2.3GHz and 3.5GHz bands will be used for 5G broadband technology services. The agency plans to auction these bands in the first quarter of 2020. Leftover spectrum in other bands may also be auctioned for next-generation services in the future.

iv  Spectrum auctions and fees
As seen above, Anatel plans to auction the 2.3GHz and 3.5GHz bands for 5G broadband technology services in the first quarter of 2020. Telecoms must pay a fee to acquire spectrum-use rights.

V  MEDIA

i  Regulation of media distribution generally
Pay-TV delivered via networks (cable, satellite, MMDS, etc.) is subject to several service and content obligations. Among other obligations, network operators must:

a  carry for free some channels considered of public interest;
b  carry channels programmed by independent Brazilian producers;
c  carry channels programmed by free-to-air TV broadcasters; and
d  offer a ‘basic package’ containing only channels of mandatory distribution.
Pay-TV content producers, for their part, must include content produced by Brazilian independent producers on certain channels and cap advertising at 25 per cent of programming. Similarly, free-to-air television broadcasters must include educational programmes in their channels and cap advertising at 25 per cent of programming.

Distribution of content via the internet (OTT) is often considered a ‘value added service’ and subject to no specific regulation. However, there are ongoing discussions regarding whether content in the format of TV channels delivered via the internet should be subject to the regulations applicable to pay-TV distributors (see below).

**ii Internet-delivered video content**

Over recent years, subscription to video on demand services has significantly increased while pay-TV subscriptions are shrinking. OTTs have enjoyed a near total lack of regulation in Brazil and normally pay fewer taxes than network operators. As a result, telecommunication companies providing pay-TV services have argued they face unfair competition from OTTs. Furthermore, some players argued that the lack of regulation over OTTs threatens Brazilian independent content producers given only pay-TV distributors have must-carry obligations regarding Brazilian content. Congress is considering bills to regulate distribution of content by OTTs.31

By the end of 2018, Claro (a major telecom company owned by América Móvil) filed complaints before Anatel32 against Fox (currently owned by the Disney group) and Topsports (owned by the Warner Media group) arguing that the SeAC Act applies to all distributors of linear content in the format of a channel, irrespective of the technology employed in distribution. According to Claro, as OTTs streaming linear content in the format of TV channels, Fox and Topsports should be subject to the regulation applicable to pay-TV distributors.

In July 2019, Anatel issued a provisional measure ordering Fox and Topsports to cease delivery of content in the format of TV channels via the internet until the release of a final decision on the matter. However, Anatel’s order was subsequently reversed by a federal court. Congress is considering changes to the SeAC Act to either expressly exclude or include OTTs that deliver content in the format of TV channels in the pay-TV regulation.33 In parallel, Anatel has yet to reach a final decision on the matter.

**VI THE YEAR IN REVIEW**

The main change in legislation for the TMT industry passed in 2019 was PLC 79 (see Section I.ii). Key mergers that closed in 2019 were the acquisition of Fox by Disney and the acquisition of Nextel (a mobile telephony company) by Claro.

Another highlight is the amendment of the LGPD by a Provisional Measure converted into law in July 2019. The LGPD will come into force in August 2020. As discussed above, TMT companies will be affected on nuclear dimensions by the law, both on issues common to all industries and more specific ones.

---
31 Bill No. 57/2018 and Bill No. 8,889/2018.
Several bills affecting the TMT industry are being discussed by Congress, so the landscape may see further changes soon, especially with regard to restrictions on cross-ownership and delivery of pay-TV and audiovisual content over the internet.

VII CONCLUSIONS AND OUTLOOK

With the passing into law of PLC 79, telecom operators saw an improvement in the regulatory landscape as changes introduced in the LGT are expected to reduce regulatory costs and boost investments in broadband infrastructure. Nevertheless, several hurdles remain, such as the heavy taxation of telecom services and the significant market concentration in the TMT industry.

The LGPD will come into force in August 2020. The TMT industry should not only hurry to comply with the LGPD, but also seek to play a leading role in influencing its future enforcement and regulation. Under the LGPD, every processing of personal data must have a legal ground, comply with data protection principles, respect the rights of data subjects and follow governance rules.

In the case of violation of the LGPD, controllers and operators are subject to fines of up to 2 per cent of turnover limited to 50 million reais, as well as publication of the infraction, blocking or elimination of personal data and suspension of processing activities.

Damage to reputation tends to be immeasurable in the event of TMT companies failing to comply with data protection requirements, especially for firms inserted in a digital economy highly based on trust. An image of careless data processing will be fatal to trust from consumers and employees.

Therefore, the TMT industry should be alert to issues regarding conflict of jurisdiction between the DPA and other authorities, such as consumer and antitrust authorities or Anatel. Also, TMT companies would do well in seeking to influence specific issues related to direct marketing and internet technology and communications, such as cookie policies, search engines, social network services and IoT.

Several bills affecting the TMT industry are being discussed by Congress, so the landscape may see further changes soon. It remains to be seen whether the more business-friendly approach advocated by President Bolsonaro’s Economy Minister will lead to a fresh agenda for the industry.
Chapter 4

CHINA

Jihong Chen

I OVERVIEW

In terms of matters relating to TMT, the government has always taken an affirmative position with the intention of constantly harmonising different sets of sector-specific laws and regulations with the rapid development of the TMT industry. Meanwhile, various incentive measures and preferential policies have been designed to ensure the protection and conditions for the expansion of fair competition and the development of a healthy market.

TMT regulation in China divides all telecommunications into two categories: basic telecommunications services (BTS) and value-added telecommunications services (VATS). BTS essentially refers to the provision of infrastructure facilities and basic voice and data transmissions, both domestically and internationally, while VATS refers to the provision of specialised services via the basic infrastructure facilities. China adopts a strict licensing system for the telecoms industry, and telecoms operators are required to obtain a licence to engage in either BTS or VATS. To fulfil its commitments to the World Trade Organization, China is gradually opening up its telecoms industry to foreign investment.

Among all the VATS, internet content services and e-commerce have grown at a rapid pace in recent years. Following the prosperity of the internet industry, online IP infringement, unfair competition and anti-counterfeiting and cybersecurity risks are issues that are starting to become of greater concern to telecoms operators.

II REGULATION

i The regulators

TMT is one of the broader sectors in China, touching upon a number of different fields of business. The Ministry of Industry and Information Technology (MIIT) is the primary regulatory body in charge of licensing for and administration of BTS and VATS, including internet content or service provision (ICP, ISP and SP) and internet access tariffs and charges. Due to its complex nature, the TMT sector is also governed by other regulatory authorities, including but not limited to:

a Ministry of Commerce (e-commerce policy, foreign investment in the TMT sector);
b Ministry of Culture (online gaming, internet cultural activities, online music, etc.);
c National Development and Reform Commission (IT industry planning and policy);
d State Administration for Market Regulation and its local branches (consumer rights protection, online advertising, fair competition, registration of entities);

1 Jihong Chen is an equity partner at Zhong Lun Law Firm.

© 2019 Law Business Research Ltd
China

e Ministry of Public Security (internet security);
f Office of the Central Cyberspace Affairs Commission (coordinating and supervising online content management and handling administrative approval of businesses related to online news reporting);
g National Radio and Television Administration (news, publications, TV, radio, film, import and export of films, books, music, etc.);
h State Intellectual Property Office (patent, trademark and geographical indication);
i the Office of State Commercial Cryptography Administration;
j Cyberspace Administration of China (cybersecurity); and
k National Information Security Standardisation Technical Committee (issuing standards related to cybersecurity).

ii Main sources of law

The main sources of legislation and regulations governing the TMT sector in China are as follows:
a Decision of the National People's Congress Standing Committee to Strengthen Internet Information Protection;
b the following laws:
  • Advertising Law;
  • Counterterrorism Law;
  • Copyright Law;
  • Contract Law;
  • Cyber Security Law;
  • Cryptography Law (Draft);
  • E-Commerce Law
  • Electronic Signatures Law;
  • Foreign Investment Law
  • Law of the PRC on the Protection of Consumer Rights and Interests;
  • Standardisation Law; and
  • State Security Law of China;
c the following regulations:
  • Regulations for the Management of Telecommunications;
  • Regulations for the Management of Sales of Commercial Cryptographic Products;
  • Regulations for the Management of Commercial Cryptographic;
  • Regulations for the Management of Online Publishing Services;
  • Regulations for the Management of Radio and Television;
  • Regulations for the Protection of the Right of Communication through Information Networks;
  • Regulations for the Protection and Administration of Computer Information Networks;
  • Regulations for the Protection of Computer Software;
  • Regulations for the Protection of Security of Critical Information Infrastructure (draft for comments);
  • Regulations on Multi-level Protection for Cybersecurity (Exposure Draft); and
  • Provisional Regulations for the Administration of Internet Culture;
d the following measures:
China

• Measures for the Administration of Pilot Operation of Value-added Telecommunications Business by Foreign Investors in China (Shanghai) Pilot Free Trade Zone;
• Measures for the Administration of Telecommunications Construction;
• Measures for the Administration of the Connection of Telecommunications Equipment to Networks;
• Measures for the Administration of Telecommunications Service Operating Permits;
• Measures for the Handling of Disputes Regarding Interconnections between Telecommunications Networks;
• Measures for the Administration of International Communications Gateways;
• Measures for the Administration of Internet Information Services;
• Measures for the Administration of the Transmission of Audiovisual Programmes over Information Networks such as the Internet;
• Measures for the Administration of Electronic Certification Services;
• Measures for the Administration of Internet Domain Names;
• Measures for the Administration on Use and Maintenance of Internet Information Security Management System;
• Measures for the Administration of Commercial Franchise Procedures;
• Measures for the Registration of Copyright in Computer Software;
• Measures for the Security Assessment of Export of Personal Information and Important Data (draft for comments);
• Measures for the Security Assessment for Cross-border Transfer of Personal Information (draft for comments)
• Measures for Cybersecurity Censorship (Exposure Draft);
• Interim Measures for the Administration of Internet Advertising;
• Interim Measures for the Administration of Online Car Hailing Services;
• Interim Measures for the Administration of Internet-based Goods and Service Transactions; and
• Interim Measures for Network Product and Service Security Inspection; e
the following provisions:
• Provisions for the Administration of Online Publishing Services;
• Provisions for the Administration of Mobile Internet Applications Information Service;
• Provisions for the Administration of Internet Information Search Services;
• Provisions for the Administration of the Construction of International Communications Facilities;
• Provisions for the Administration of Internet Audio and Video Programming Services;
• Provisions for the Administration of Internet News Information Services;
• Provisions for Technical Measures of Internet Security Protection; and
• Provisions on the Security Assessment of Internet-based Information Services with Attribute of Public Opinions or Capable of Social Mobilisation;
f
the following catalogues and lists:
• Catalogue of Telecommunications Services;
• Catalogue of Network (Cyber) Critical Equipment and Cybersecurity-Specific Products (Batch 1);
China

- Catalogue of Guide of Foreign Investment;
- Industry Guidelines on Encouraged Foreign Investment;
- Negative List of Access of Foreign Investment; and
- Negative List for Foreign Investment Access in Pilot Free Trade Zones;

- the following rules:
  - Rules for the Administration of Foreign-Invested Telecommunications Enterprises;
  - Rules for the Administration of the Interconnection of Public Telecommunications Network;
  - Rules for the Administration of the Establishment of Satellite Communications Networks and Installation and Use of Earth Stations;
  - Rules for the Protection of Personal Information of Telecommunication and Internet Users;
  - Rules for the Allocation of Radio Frequency Band;
  - Rules for the Registration of Real Names of Phone Users; and
  - Procedural Rules for the Resolution of Domain Name Disputes by China Internet Network Information Centre;

- the following national standards:
  - Information Security Technology – Security Capability Requirements for Big Data Services;
  - Information Security Technology – Guide of Assessment for Data Cross-Border Transfer Security (draft for comments);
  - Information Security Technology – Guide of Personal Information Protection in Public and Commercial Services Information System;
  - Information Security Technology – Baseline for Classified Protection of Cybersecurity;
  - Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity; and
  - Information Security Technology – Evaluation Requirements for Classified Protection of Cybersecurity;

- Notice of the Administration of Mobile Game Publishing Services, issued by the National Radio and Television Administration;

- Opinions on Further Opening up Value-added Telecommunication Business to Foreign Investments in the China (Shanghai) Pilot Free Trade Zone, jointly issued by MIIT and the Shanghai municipal government; and

- Circular for Removing Restriction on Foreign Shareholding in Holder of Online Data Processing and Transaction Processing in China (Shanghai) Pilot Free Trade Zone, issued by MIIT.
The main statute governing telecoms services is the Regulations for the Management of Telecommunications, supported by the Catalogue of Telecommunications Services. Foreign-invested companies may refer to the Catalogue of Guide of Foreign Investment, Industry Guidelines on Encouraged Foreign Investment, and Negative List of Access of Foreign Investment for additional restrictions and requirements imposed on acquiring telecom licences.

### iii Regulated activities

A telecommunications operator who operates basic telecommunications services or VATS (as classified in the Catalogue of Telecommunications Services) shall obtain a licence under the Measures for the Administration of Telecommunications Service Operating Permits or the Rules for the Administration of Foreign-Invested Telecommunications Enterprises.

### iv Ownership and market access restrictions

The newly revised Foreign Investment Law in 2019 and the statements of the high-profiles in recent years reveal China’s willingness to be more open to foreign investors in the TMT field, which was also one of China’s commitments to the World Trade Organization.

With certain restrictions and regulatory approval procedures, foreign-funded telecoms enterprises are able to engage in telecoms businesses not prohibited by the Negative List of Access of Foreign Investment or Negative List for Foreign Investment Access in Pilot Free Trade Zones (if applicable) provided that they abide by the provisions of the Regulations for the Management of Telecommunications and other applicable laws and regulations.

BTS and VATS are available to foreign investment by way of a Sino-foreign equity joint venture. To establish a foreign-invested telecommunications enterprise providing BTS or VATS, the major Chinese investor shall submit the required application documents for approval to MIIT.

The ultimate proportion of contribution and registered capital required for BTS business are as follows.

<table>
<thead>
<tr>
<th>Business classifications</th>
<th>Geographical areas</th>
<th>Registered capital</th>
<th>Proportion of contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>BTS business</td>
<td>Nationwide, or beyond a single province, autonomous region or municipality directly under the central government</td>
<td>Not less than 1 billion yuan</td>
<td>Foreign investors: no more than 49% (except radio paging services and the construction and operation of power grid systems)</td>
</tr>
<tr>
<td></td>
<td>Within a province, autonomous region or municipality directly under the central government</td>
<td>Not less than 100 million yuan</td>
<td></td>
</tr>
</tbody>
</table>

The major foreign investor of a foreign-invested telecommunications enterprise providing BTS shall meet the following conditions:

- **a** being qualified as a legal person or enterprise;
- **b** having obtained a licence for providing BTS from the registration country or region;
- **c** having the funds and professionals commensurate with its business operation; and
- **d** having a good performance record and experience in providing BTS.
Advantages enjoyed by the foreign investors in Shanghai Pilot Free Trade Zone (Shanghai FTZ) have become more obvious, particularly in VATS business. The chart below compares the substantive and procedural differences in foreign investors’ application for a VATS licence in Shanghai FTZ and non-free trade areas.

<table>
<thead>
<tr>
<th>Shanghai FTZ</th>
<th>Non-free trade areas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authority</strong></td>
<td>Shanghai Communications Administration (SCA)</td>
</tr>
<tr>
<td><strong>Timeline</strong></td>
<td>Ministry of Industry and Information Technology (MIIT)</td>
</tr>
<tr>
<td><strong>Requirements</strong></td>
<td></td>
</tr>
<tr>
<td>• Legally established in the FTZ.</td>
<td></td>
</tr>
<tr>
<td>• Registered capital ≥ 1 million yuan.</td>
<td></td>
</tr>
<tr>
<td>• The place of registration and service facilities of enterprises shall be located within Shanghai FTZ (for operating e-commerce business of ODPTP, the service facilities could be located outside Shanghai FTZ, but should still be located within Shanghai).</td>
<td></td>
</tr>
<tr>
<td>• The foreign investor has a record of good performance and operating experience in operating VATS business. Business description and supporting certificates should be provided.</td>
<td></td>
</tr>
<tr>
<td>• For providing service nationwide or across different provinces, registered capital ≥ 10 million yuan.</td>
<td></td>
</tr>
<tr>
<td>• For providing service within a province, registered capital ≥ 1 million yuan.</td>
<td></td>
</tr>
<tr>
<td>• The foreign investor has a record of good performance and operating experience in operating VATS business. Business description and supporting certificates should be provided.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Foreign capital ratio restrictions in certain VATS categories (Shanghai FTZ versus Nationwide VATS application in non-FTZ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>B21 (On-line Data Processing and Transaction Processing Services): foreign capital could be up to 100% for operating e-commerce business but cannot exceed 50% for operating other business.</td>
</tr>
<tr>
<td>B22 (Domestic Multi-party Communication Services): foreign capital could be up to 100%.</td>
</tr>
<tr>
<td>B25 (Information Services): foreign capital could be up to 100% for app store business but cannot exceed 50% for operating other business.</td>
</tr>
<tr>
<td>B13 (Domestic Internet Virtual Private Network Services): foreign capital cannot exceed 50%.</td>
</tr>
<tr>
<td>B21: foreign capital could be up to 100% for operating e-commerce business but cannot exceed 50% for operating other business.</td>
</tr>
<tr>
<td>B22: prohibited.</td>
</tr>
<tr>
<td>B25: foreign capital cannot exceed 50% for operating other business.</td>
</tr>
<tr>
<td>B13: prohibited.</td>
</tr>
</tbody>
</table>

### Transfers of control and assignments

An ownership change or transfer of equity of a foreign-invested telecommunications enterprise shall comply with China’s laws and regulations on investor qualifications and industrial policy requirements. First, the ownership change or transfer of equity of a foreign-invested telecommunications enterprise shall not violate the Catalogue of Guide of Foreign Investment and the Negative List of Access of Foreign Investment or Negative List for Foreign Investment Access in Pilot Free Trade Zones (if applicable). In addition, in TMT industries, MIIT and its branches and the Administrative, Industrial and Commerce authorities may review such transactions.

The enterprise shall, within 30 days of the date on which the examination and approval authority approves the change or the transfer, go through the formalities regarding that examination and approval authority. If the Chinese investor in a joint venture will obtain the entire equity, it shall, within 30 days of the date of approval by the examination and approval authority, cancel the certificate of the foreign-invested enterprise to the examination and approval authority. The enterprise shall, within 30 days of the date of change or cancellation of the foreign-invested enterprise approval certificate, apply to the registration authority for registration of change.
III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

With regard to the government institutions that were restructured in 2018, generally, internet and IP-based services are regulated by the following authorities:

a internet services and cybersecurity issues: MIIT, the Cyberspace Administration of China and the Ministry of Public Security; and

b IP-based services: the National Radio and Television Administration (news, publications, TV, radio, film, import and export of films, books, music, etc.), the Copyright Protection Centre of China (copyright registration issues) and the State Intellectual Property Office (patent, trademark and geographical indication).

ii Universal service

Under the current telecoms legal system of China, basic telecommunications operators are required to perform their corresponding obligations to make telecommunications services universally available, in accordance with relevant state regulations. MIIT may determine which telecommunications operators shall assume specific obligations in respect of the universal availability of telecommunications services by designating such operators or by inviting tenders.

The State Administration for Market Regulation and the State Council’s department in charge of pricing are responsible for formulating the procedures for the administration of compensation for the costs of making telecommunications services universally available.

In addition, telecommunications operators engaging in domestic telephone business and mobile phone business are required to provide their subscribers with free telecommunications services of a public welfare nature, such as phone numbers for reporting fire-related accidents, bandit-related incidents, medical emergencies and traffic accidents, and the availability of telephone lines shall be guaranteed.

iii Restrictions on the provision of service

Price regulation

According to the Announcement of the MIIT and the National Development and Reform Commission on Market-Regulated Prices for Telecom Services issued in 2014, telecoms service prices are regulated by the market. When setting prices, operators must fully consider:

a production and operation costs;

b supply and demand in the telecoms market;

c other factors to reasonably determine charging rates; and

d operators must publish charge plans, billing methods and other information.

On 23 August 2018, the MIIT issued a Circular on Further Regulating Activities to Market Telecommunications Tariff Schemes, stating that telecommunications business operators must prepare their own reasonable schemes for telecommunications charges. These schemes must clearly specify the operator’s:

a structure of fees;

b fee items;

c fee standards;

d charging principles;
e corresponding services;
f conditions for handling telecommunications business; and
g validity periods.

In addition, the Circular requires operators to use simple, definite, standardised and unambiguous language to present such information.

Consumers also have the right to protect their interests under the Law of the PRC on the Protection of Consumer Rights and Interests.

Requirements for manufacturers and operators

Under the network access permit system, the following requirements shall be met by telecommunications equipment manufacturers:
a obtain the relevant network access permit;
b once obtained a network access permit, promptly report such for the record to the telecommunications authorities in the various provinces, autonomous regions and municipalities, and accept the supervision and management of such departments;
c if there is any modification relating to technology and appearance, such changes shall be tested, and a new application for a new network access permit shall be submitted;
d ensure that the quality of the equipment for which they have obtained a network access permit is stable and reliable, and they may not lower the quality or performance of their products; and
e affix a sticker presenting the network access permit logo and the network access certificate stating the certificate number, applicant, name of manufacture, device name, device type and the effective date of the certificate.

The following requirements shall be met by telecommunications operators:
a obtain network access approval prior to using telecommunications equipment;
b consider that users have the right to choose the telecommunications terminal equipment to be used, and no carrier shall prevent subscribers from connecting their own telecommunications terminal equipment for which the network connection permit has been obtained;
c assist the authorities to review the certified equipment connected to their networks;
d major incidents caused by the telecommunications equipment shall be truthfully reported in a brief written report by the telecommunications operators; and
e shall not monitor and control the content, applications and services accessed by their network users under the regulations on personal information protection.

iv Privacy and data security

Regulatory and legislative policies in national interests

Under the Cyber Security Law, national security review is required for network operators who purchase network products and services that may potentially have an impact on national security. Network operators are required to provide technological support and assistance to public and state security organs in national security and criminal investigations.
**Personal information protection**

Network operators (including telecoms providers) are required by the Cyber Security Law to keep strictly confidential users’ personal information that they have collected, and establish and improve the users’ information protection system. Information Security Technology – Guide of Personal Information Security Specification (the PI Specification), the non-binding national standard, illustrates the obligations of privacy protection in detail. The PI Specification plays a key role in personal information protection and has been cited by courts and the enforcement authority. An increasing number of companies in the market also tend to refer to the PI Specification as the standard when conducting self-auditing of their personal information protection.

**Child information protection**

Under the PI Specification, personal information of persons aged 14 or under is considered as a child's personal information and is classified as sensitive personal information. To regulate the collection and processing of child information, the Cyberspace Administration of China recently published the Provisions on the Cyber Protection of Children’s Personal Information (effective as of 1 October 2019). Network operators are required to establish special rules and user agreements for the protection of children's personal information, and designate persons to take charge of the protection of children's personal information. Network operators will also need to inform the child's guardians in a noticeable and clear manner, and shall obtain the consent of the child's guardians for the collection, use, transfer or disclosure of a child's personal information.

**Network operators’ security-related obligations**

Except for the obligations of personal information protection, network operators are also required by the Cyber Security Law to fulfil the following security obligations according to the requirements of the multi-level protection scheme, to ensure that the network is free from interference, damage or unauthorised access, and prevent network data from being divulged, stolen or falsified:

- Formulate internal security management systems and operating instructions, determine the persons responsible for cybersecurity, and implement the cybersecurity protection responsibility;
- Take technological measures to prevent computer viruses, network attacks, network intrusions and other actions endangering cybersecurity;
- Take technological measures to monitor and record the network operation status and cybersecurity incidents, and preserve relevant web logs for no less than six months; and
- Take measures such as data classification, back-up and encryption of important data.

**IV  SPECTRUM POLICY**

In terms of telecommunications resources, the central government is attempting to carry out uniform planning, centralised administration and reasonable allocation, and to implement a system of use with compensation. Telecommunications resources are resources that have telecommunications functions, and are limited in amount, including, inter alia, RFs, satellite orbit locations and telecommunications network codes.

A telecommunications operator that occupies or uses telecommunications resources shall pay telecommunications resource fees. MIIT is the major government body responsible for telecommunications resource fees.
for formulating specific measures for fee collection for use of telecommunications resources. When MIIT allocates telecommunications resources, it needs to consider factors including telecommunications resource planning, usage and expected service capability. The allocation of telecommunications resources may be made either by designation or by auction. To date, no auctions have been conducted.

Without the approval of MIIT, an operator may not unilaterally use, transfer or lease out telecommunications resources or change the use of telecommunications resources. After a user of telecommunications resources obtains a telecommunications network code, the major telecommunications operators or other relevant parties shall be obligated to take the necessary technical measures to cooperate with such user of telecommunications resources to allow it to achieve the functionality of its telecommunications network code resources.

V MEDIA

i Regulation of media distribution generally

China has systematic restrictions on TV and radio content provision and transmission.

Radio or television stations shall be established by the administrative departments for radio and television under the people’s governments, and educational television stations may be established by the administrative departments for education under the people’s governments at or above the level of a city divided into districts or counties. No other entity or individual may establish radio or television stations.

An entity that intends to establish a cable television station shall obtain the preliminary consent of the competent department of radio and television of the province and apply for the approval of the National Radio and Television Administration. Upon approval, a permit to establish a cable television station shall be issued by the National Radio and Television Administration to the applying entity. An entity that intends to establish a small cable television station shall obtain the preliminary consent of the competent department of radio and television of the country, and apply for the approval of the competent department of radio and television of the province. Upon approval, a permit to establish a small cable television station shall be issued by the competent department of radio and television of the province to the applying entity.

An entity or individual that intends to set up master antenna television shall report to the department of radio and television of the district or county for its records.

An entity that intends to utilise its existing ground satellite receiving facilities or install special ground satellite receiving facilities to receive television programmes transmitted via foreign satellites shall apply in writing to the competent department at or above the provincial level. If consent is granted thereto upon examination, the applying entity shall proceed to submit the application for examination and approval to the department (or bureau) of radio and television of the province, autonomous region or municipality directly under the central government where the applying entity is located. Upon this approval, a permit to receive television programmes transmitted via foreign satellites shall be issued to the applying entity, and the case shall be reported by the examining and approving authorities to MIIT, the National Radio and Television Administration, the Ministry of Public Security and the Ministry of State Security for their records.

The watchdog also keeps a close eye on emerging platforms, such as BBS, blogs, microblogs, chat rooms, communication groups, public accounts, short videos, online streaming, information sharing and mini programmes. The Cyberspace Administration of
China and the Ministry of Public Security jointly released the Provisions on the Security Assessment of Internet-based Information Services with Attribute of Public Opinions or Capable of Social Mobilisation, clearly stating the goal of strengthening the security management of internet-based information services and the relevant new technologies and new applications and regulating internet-based information service activities, and safeguarding national security.

ii Internet-delivered video content

An entity that intends to provide internet audio and video programme-related services shall obtain a permit for audio and video programmes transmitted through an information network issued by the competent radio and television authority, or go through the formalities for registration in accordance with the provisions of these regulations.

No entity or individual that has not obtained a permit issued by the competent radio and television authority, or that has not gone through the formalities and legal steps for registration in accordance with the relevant laws and regulations, may provide internet audio and video programme-related services.

As internet access is very common in China and because of technology development, ICPs pay great attention to the protection of their contents’ copyright. ICPs may include large platforms providing audio and video content to consumers, or personal media. ICPs take technical measures to prevent copyright infringement. More and more lawsuits related to the right of communication through the information network (a subclass of copyright under the Copyright Law of China) are being filed to fight against the unauthorised use, reproduction or transmission of internet contents. The amount of compensation being awarded in these types of cases is getting higher, especially in judgments of the intellectual property courts in Beijing, Shanghai and Guangzhou that focus on the protection of copyright ownership of internet content.

VI THE YEAR IN REVIEW

i Development in e-commerce

Legislation

Coming into force on 1 January 2019, the E-commerce Law regulates business-to-business (B2B) and business-to-customer (B2C) operators in China. The E-commerce Law consists of general provisions, e-commerce operators, conclusion and performance of e-commerce contracts, settlement of e-commerce disputes, promotion of e-commerce, legal liability and supplementary provisions.

Venue

Internet courts have been established in China to hear matters including e-commerce and online transactions and generally, the entire litigation process is conducted online. Internet courts in Beijing and Guangzhou were formally established in September 2018 following the opening of China’s first internet court in Hangzhou in 2017. Internet courts may decide to complete part of the litigation process offline upon application by the litigants or if necessary for trying the case. In September 2018, the Supreme People’s Court also issued rules to regulate the litigation activities of the internet courts in China.
Industry

In October 2018, six main Chinese internet enterprises signed a convention in Beijing in which the enterprises unanimously made commitments on the integrity of e-commerce transactions (in relation to, for example, selling genuine goods, protecting consumers’ personal information and so on).

ii Multi-level Protection Scheme 2.0

Article 21 of the Cyber Security Law stipulates that China implements the cybersecurity multi-level protection scheme. The standards and accompanying administrative measures under the Multi-level Protection Scheme (MLPS) 1.0 were too outdated to catch up with the rapid development in telecommunications and information. On 13 May 2019, the Ministry of Public Security, in conjunction with other related government agencies, released the core national standards, including the Baseline for Classified Protection of Cybersecurity, Technical Requirements of Security Design for Classified Protection of Cybersecurity, and Evaluation Requirements for Classified Protection of Cybersecurity, all of which will be effective as of 1 December 2019. These core national standards, together with the Regulations on Multi-level Protection for Cybersecurity (Exposure Draft), form the MLPS 2.0.

The standards and measures under MLPS 2.0 have been adapted to embrace new technologies. MLPS 1.0 targeted traditional information systems, while MLPS 2.0 expands the subjects to network information infrastructure, big data centres, cloud computing platforms, the internet of things, industrial control systems, public service platforms, mobile internet, etc. Network operators under MLPS 2.0 are required to evaluate the security risks presented by such new technologies and applications to implement security control measures correspondingly. MLPS 2.0 also expands the regulatory enforcement measures from grading, filing and evaluation to include remote monitoring, on-site inspection, incident investigation, compliance inquiries with responsible personnel, remediation instruction, penalty notifications, emergency network cut-off, etc.

VII CONCLUSIONS AND OUTLOOK

To fulfil China’s commitments to the World Trade Organization, we believe that the VATS market will gradually be more open to foreign investors albeit foreign investment would still be restricted or prohibited in internet content services and the media (including emerging platforms).

In the age of big data, China also witnessed continuing progress to personal information protection legislations as well as tightening law enforcement in this field ever since the Cyber Security Law came into effect. A handful of accompanying rules and measures to the Cyber Security Law have been released, although more are expected to be published in the future, including the official measures regarding cross-border data transfer, which would be one of the key concerns of foreign investors dealing with data-related business.

China’s regulation of the TMT sector remains quite complex and is rapidly changing; therefore, when an entity enters into this market, it is advisable to seek legal advice from professional TMT lawyers.
I OVERVIEW

Estonia is a strong advocate of technological advancement, and the ICT sector is of major importance to the government. Estonia has become a model for free and open internet access. It is also the EU frontrunner as regards the digital provision of public services and has one of the highest shares (92 per cent) of e-government users in Europe.²

Estonia sees ICT as a key to sustained economic growth. The Ministry of Economic Affairs and Communications adopted the Digital Agenda 2020,³ which focuses on creating an environment that facilitates the use of ICT and the development of smart solutions in Estonia in general. The main goals of the Agenda are, among others:

- the completion of the next-generation broadband network, with the aim of that all residents of Estonia will have access to fast (30Mbit/s or faster) internet by 2020 and that at least 60 per cent of households will be using ultrafast (100Mbit/s or faster) internet daily;
- the continuing development of state information systems and public e-services to ensure up-to-date and citizen-friendly solutions; and
- to continue promoting Estonia as a hub for innovation and the development of the information society, and to establish a global information society think tank in Estonia.

The number of internet and mobile telephone users in Estonia has grown rapidly in the past 20 years. The availability of mobile broadband is very good while fixed broadband is less widespread, below the European average, which is mainly because of limited connectivity in sparsely populated rural areas.⁴ For this reason, a non-profit organisation, the Estonian Broadband Development Foundation (ELA SA), was founded in 2009 by the government and major Estonian communication undertakings to develop Estonia's broadband network and build and operate the EstWin high-speed base network. The project is financed mostly from public sources. In 2018, the Foundation started its 12th and last tender to procure the designing and building of approximately 400km of base network. The Foundation has set its goals to finalise the project in 2019 by bringing broadband no further than 1.5km from 98 per cent of households.⁵

---

1 Mihkel Miidla is a partner and Liisa Maria Kuuskmaa and Oliver Kuusk are legal assistants at Sorainen.
5 https://www.elasa.ee/estwin-baasvorgu-rajamine-lopusirgel/.
Separate from the base network project is the government’s last mile project. Until 2018, all local municipalities were responsible for mapping out the white areas in their jurisdiction where there is a need for developing the last mile of a high-speed internet network. This approach did not prove to be successful, and in 2018 the Ministry of Economic Affairs and Communications, along with the Estonian Technical Regulatory Authority, initiated the national last mile project, a public competition to find a suitable network builder to bring high-speed internet access to areas where there is no internet access or where the connection is of poor quality and where communications companies would not invest in the next five years (the white area). Elektrilevi (part of the state-owned energy operator) was awarded the subsidy and committed to extend broadband access to the largest possible number of households who still lack high-speed internet. Elektrilevi has initiated plans to connect 15,000 households by the end of 2019 and 200,000 households by the end on 2023.

The fast-developing ICT sector presents some challenges for policymakers, but generally the regulatory landscape in the ICT sector is in quite good shape. As previously mentioned, the ICT sector is of major importance to the state. Estonia experienced several political changes during the past year, but these are unlikely to heavily impact e-governance or other internet use. The government continues with its strategy to market Estonia as an e-state throughout the world.

II REGULATION

i The regulators

The electronic communications and media area is supervised by an independent regulatory authority, the Estonian Consumer Protection and Technical Regulatory Authority (ECTRA), which is sometimes also referred to as the Technical Surveillance Authority (previously the Technical Regulatory Authority). ECTRA supervises the fields of consumer protection, electronic communications, industrial safety and transport. In the field of communications services, the ECTRA is tasked with ensuring a sufficient and timely resource of RFs and telephone numbers for the provision of communications services and performing national surveillance of the field of communications.

Other regulatory bodies that may exercise supervision over electronic communications service (ECS) providers pursuant to their competence include (not exhaustively) the Data Protection Inspectorate, the Competition Authority and the Information System Authority. Sector-specific regulation of the competitive situation on the markets for communications services is carried out mainly by the ECTRA, while the Competition Authority has general authority (e.g., in merger proceedings).

8 Website: https://www.ttja.ee/en.
Main sources of law

ECSs are regulated by the Electronic Communications Act (ECA),\(^\text{10}\) in force from 1 January 2005 (as amended), which transposes in Estonia the EU’s regulatory framework for electronic communications. On basis of the ECA, numerous regulations of the government have been adopted to regulate certain more technical or detailed issues of the framework. Under the ECA, an ECS means a service that consists wholly or mainly in the transmission or conveyance of signals over the ECN under agreed conditions. Network services are also ECSs.\(^\text{11}\)

The ECA provides requirements for public ECNs and publicly available ECSs regarding the use of electronic contact details for direct marketing, the conduct of radiocommunications, and the management of RFs, numbering and apparatus, as well as state supervision over the compliance with these requirements and liability for the violation of these requirements. A publicly available ECS is defined as a service provided by a communications undertaking undertaking on the respective communications services market pursuant to the general procedure to all persons, and the persons need not meet any conditions differentiating them from other similar persons. A service is publicly available particularly if provision of the service is continuous and consistent and it is provided essentially under uniform conditions.\(^\text{12}\) There appear to be no definite (official) criteria available that would help to determine whether a particular service is considered to be publicly available, as there are no official guidelines or case law. However, under a conservative approach from the viewpoint of notification obligations, it does not matter whether the services are offered either on a wholesale level or on a retail level to end users to be considered as publicly available, but rather if the service is open to a particular group of (similar) customers.

The ECA is not applicable to information society services to the extent these are regulated by the Information Society Services Act (ISSA),\(^\text{13}\) which implements Directive 2000/31/EC into Estonian law. Information society services are services provided in the form of economic or professional activities at the direct request of a recipient of the services, without the parties being simultaneously present at the same location, and such services involve the processing, storage or transmission of information by electronic means intended for the digital processing and storage of data. Information society services must be entirely transmitted, conveyed and received by electronic means of communication.\(^\text{14}\)

Media services are regulated by the Media Services Act (MSA),\(^\text{15}\) in force from 16 January 2011 (as amended). The MSA provides for:

\begin{itemize}
  \item[a] the procedure and principles for the provision of audiovisual media services and radio services and the requirements for providers of media services;
  \item[b] the procedure for the issue of activity licences for the provision of television and radio services to legal persons under private law and the procedure for registration of the provision of on-demand audiovisual media services; and
  \item[c] the principles of protection of a person who has provided information to a person processing information for journalistic purposes.\(^\text{16}\)
\end{itemize}

---


\(^{11}\) Clause 2 6) of the ECA.

\(^{12}\) Clause 2 68) of the ECA.

\(^{13}\) Available in English at: https://www.riigiteataja.ee/en/eli/ee/513012015001/consolide/current.

\(^{14}\) Clause 2 1) of the ISSA.


\(^{16}\) Section 1 of the MSA.
Estonian public broadcasting is excluded from the scope of the MSA and is regulated by the Estonian Public Broadcasting Act.\(^\text{17}\)

### iii Regulated activities

Under the ECA, each person has the right to commence the provision of communications services. The provision of communications services is subject to a one-off notification obligation. A notice of economic activities for the provision of communications services must, among other required information, set out a description of the provided communications service and the geographical area of activity. Such notice must be filed via the state portal (www.eesti.ee) or via a notary.\(^\text{18}\) If publicly available communications services are provided by an entity from another EU Member State (cross-border service) on a permanent basis in Estonia, then such entity must also file the notice of economic activities to the ECTRA. The current position of the ECTRA is that foreign operators also need to establish a branch or subsidiary in Estonia.

For the provision of certain communications services, it is necessary for service providers to apply for licences. Namely, use of radio spectrum and numbering is subject to a RF authorisation and a numbering authorisation respectively. Activity licences are required for the provision of television and radio services. All licences and authorisations are subject to relevant state fees, the amount of which varies according to the type of the licence or authorisation in question. All the relevant licences and authorisations mentioned above are issued by the ECTRA.

Frequency authorisations for the use of spectrum are allocated according to the Estonian Radio Frequency Allocation Plan,\(^\text{19}\) which determines the manner, regime and purpose of using RFs. To receive an authorisation, a standard format application\(^\text{20}\) to the ECTRA must be submitted with the relevant information about the applicant (name, residence or seat, date of birth or personal identification code or registry code, contact details) and the frequency itself (which frequency is being applied for, what is its purpose, conditions of use, area of use, etc.). The ECTRA has six weeks from the receipt of a complete application to issue a licence if the use of spectrum does not need international coordination, and eight months if it does. If the use of spectrum is being allocated by way of a public competition or auction, the relevant procedural rules and deadlines are determined by the Minister of Economic Affairs and Infrastructure. The ECTRA has the right to refuse an application on certain grounds, for example if the applicant's activities may be hazardous, there is no free spectrum, the use of spectrum is not in line with the Estonian Radio Frequency Allocation Plan or national or international legislation, or if the use of spectrum is ineffective or may cause radio interference.\(^\text{21}\) The frequency authorisation establishes the conditions and requirements for the use of spectrum. Under certain conditions, the conditions may be amended. If the ECTRA has issued a frequency authorisation, the authorisation can be extended by submitting an application not later than one month before the expiry of the authorisation and by paying the relevant state fee.\(^\text{22}\)

---

17 Available in English at: https://www.riigiteataja.ee/en/eli/ee/527062014005/consolide/current
18 Sections 3–4 of the ECA.
21 Sections 11–14 of the ECA.
22 Sections 11, 15–16 of the ECA.
Upon grant of spectrum licences by way of public competition, the Minister of Economic Affairs and Infrastructure may determine a one-off authorisation charge of up to €1.597 million, a deposit for participation in the competition, or both. The one-off authorisation charge shall be determined as a fixed charge or, in the case of an auction, as a starting price. The deposit must be equal to all participants and must not exceed the one-off authorisation charge. The deposit will be returned after the winner is ascertained.\(^\text{23}\)

Authorisations for the use of numbering are allocated according to the Estonian numbering plan,\(^\text{24}\) which determines the location of numbers, short numbers, identification codes and access codes in the numbering space, the requirements for the length, use and dialling procedure of numbers, the conditions of use and the services for the provision of which they may be used. A numbering authorisation can be obtained by submitting a standard format application\(^\text{25}\) to the ECTRA, containing the information on the applicant (name, residence or seat, date of birth or personal identification code or registry code, contact details), the planned use of the number, etcetera. The ECTRA will issue a numbering authorisation within 10 working days after receipt of a complete application if there are no grounds for refusal. The numbering authorisation sets out the conditions of use of the allocated number. A numbering authorisation is issued for up to one year and can be extended by up to one year at a time. Numbering authorisations can also be granted by way of an auction on certain conditions.\(^\text{26}\)

Activity licences for television and radio services are provided on the basis of the MSA. All private broadcasters are required to have an activity licence. Estonian Public Broadcasting, which is a legal person in public law, is not required to apply for an activity licence. Different licences are issued for the provision of free access television services, conditional access television services, satellite television services and radio services. Free access television and radio service licences are issued through a public competition. All the other licences are issued on the basis of an application. For the obtaining of licences, the MSA prescribes necessary requirements on programmes, sustainability of a service and the coverage area of the service, among other conditions. A licence for free access television services is issued for up to 10 years, and the rest of the above-mentioned licences for up to five years.\(^\text{27}\)

iv Ownership and market access restrictions

Currently there are no foreign ownership restrictions in the communications sector. Under the MSA, a television or radio service provider will not be given an activity licence if it holds a dominant influence over the management of the undertaking that has been issued an activity licence for the provision of television and radio service, and the issue of the activity licence may substantially damage competition in the media services market, particularly through the creation or reinforcement of the dominant position in the market.\(^\text{28}\) Similarly, aggregate holdings of certain types of spectrum may constitute a dominant position, which would trigger the heightened attention of the ECTRA and the Estonian Competition Authority. When it comes to trading spectrum, the ECTRA has a right to refuse the transfer

\(^{23}\) Subsections 9(2)-9(24) of the ECA.
\(^{26}\) Sections 33–39 of the ECA.
\(^{27}\) Sections 32–40 of the MSA.
\(^{28}\) Clause 32 3) of the MSA.
Estonia

or grant of right to use RFs if this distorts competition, and it may, if necessary, coordinate the transfer or grant of frequencies with the Estonian Competition Authority.\textsuperscript{29} These rules apply in addition to the general merger control regime under Estonian and European competition law.

In general, Estonian law does not limit market access, except for the limitations specified above.

\section{Transfers of control and assignments}

Mergers and acquisitions are reviewed by the Estonian Competition Authority. The procedure of merger reviews is regulated by Chapter 5 (Control of Concentrations) of the Competition Act.\textsuperscript{30} Council Regulation (EC) No. 139/2004 on the control of concentrations between undertakings applies in cases of mergers with an EU dimension, but the national merger control is very similar to that of the EU. Estonia has a mandatory filing requirement for qualifying transactions. For a transaction to be qualifying, the relevant turnover thresholds must be exceeded. A merger is notifiable if the total annual turnover in Estonia of all companies concerned is more than €6 million and the total annual turnover in Estonia of each of at least two of the companies concerned is more than €2 million.\textsuperscript{31} The companies concerned include those directly involved in the merger, any other associated companies within the same control group and joint ventures. There is a two-phase merger review process, and clearance is required before closing. The length of proceedings is 30 days for a simplified procedure, and will last for four additional months when further investigation is needed. Simplified procedures may end with an approval or a decision to conduct further investigation in Phase II. The latter may conclude with a clearance, a refusal or a conditional clearance.\textsuperscript{32}

While the Competition Authority has general authority over merger proceedings, the sector-specific regulation of ECSs markets is conducted by the ECTRA. The Competition Authority used to have wider competences in the communications sector, but now only postal services have remained fully under its regulatory authority. The ECTRA and the Competition Authority are under a legal obligation to cooperate in the area of market regulation and exercise supervision in the communications sector, and, if necessary, exchange appropriate information.\textsuperscript{33} This means that when it comes to mergers in the communications sector, the Competition Authority may involve the ECTRA in the merger proceedings. In practice, merely holding a dominant position through an allocated frequency authorisation can be decisive on the outcome of transactions.

As described in subsection iv above, licence transfers may also be subject to competition law concerns. In general, RFs are transferrable or can be granted for use to another person if the Estonian Radio Frequency Allocation Plan allows it, with the RFs for broadcasting being an exception. It is thus necessary to verify the transferability or the permissibility of granting the frequency to the use of another person on a case-by-case basis, based on the Radio Frequency Allocation Plan. The transfer or grant of use must be approved by the ECTRA, who may coordinate with the Competition Authority. The ECTRA has the right to refuse the transfer or grant of the right to use RFs if it distorts competition.\textsuperscript{34}

\begin{itemize}
\item \textsuperscript{29} Subsection 17(8) of the ECA.
\item \textsuperscript{30} Available in English at: https://www.riigiteataja.ee/en/eli/ee/527122017001/consolide/current.
\item \textsuperscript{31} Section 21 of the Competition Act.
\item \textsuperscript{32} Section 27 of the Competition Act.
\item \textsuperscript{33} Subsections 40(4) and 144(1) of the ECA.
\item \textsuperscript{34} Section 17 of the ECA.
\end{itemize}
III  TELECOMMUNICATIONS AND INTERNET ACCESS

i  Internet and internet protocol regulation

IP-based services are regulated by the ISSA. ECSs and information society services are mutually exclusive; therefore, information society services are excluded from the scope of the ECA. However, state supervision over compliance with the requirements provided for in the ISSA is exercised by the ECTRA.

Contrary to the ECA, the ISSA does not contain any registration, authorisation or notification obligations for the service providers. The primary obligation of service providers is to render directly and permanently accessible to recipients of services at least the following information:

a  the name of the service provider, its registry code and the name of the corresponding register, the service provider’s address and other contact details, including the electronic mail address;

b  its registration number if, for operation in the corresponding field of activity, registration in the register of economic activities is required by law, or its activity licence number; and

c  if reference is made to the fee charged for the service, information on whether the fee includes taxes and delivery charges.

Information society service providers generally have less obligations compared to communications service providers. An information society service provider is generally not liable for the information transmitted upon mere transmission of information and provision of access to public data communications networks, upon temporary storage of information in cache memory and upon provision of information storage services. There are exceptions to this general rule.\[35\] Additionally, information society service providers are not obligated to monitor information upon the mere transmission thereof or provision of access thereto, temporary storage thereof in cache memory or storage thereof at the request of the recipient of the service; nor is the service provider obligated to actively seek facts or circumstances indicating illegal activity. However, in certain circumstances information society service providers are obliged to provide information about alleged illegal activities undertaken or information provided by recipients of their services, and to communicate to the competent authorities information enabling the identification of recipients of their service.\[36\]

ii  Universal service

Under the ECA, it is possible to designate universal service providers by way of a public competition, or public procurement if the payable charges exceed the relevant thresholds. When designating universal service providers, it must be taken into account that the end goal is to ensure provision of the service in a cost-effective manner that does not prejudice competition, at an affordable price, and in accordance with the objectives of state organisation in the electronic communications sector, which is to promote competition in the provision of ECSs. A universal service provider may be designated separately for each specified service within a specified territory.\[37\]

---

35  Sections 8–10 of the ISSA.
36  Section 11 of the ISSA.
37  Section 73 of the ECA.
The following services can be designated as universal services:

- a connection to a communications network in a fixed location enabling telephone services (which enables the making and receiving of calls, the sending and receiving of faxes and the use of data communication services at data rates sufficient to permit functional internet access, taking into account the hardware and software used by most end users);
- b public payphone services or other publicly accessible communications services enabling calls; and
- c the availability of a universal electronic public number directory and directory enquiry services.38

The USO is based on a universal service contract between the communication undertaking and the state, which sets out, inter alia, the obligations, term, charges payable by end users and the territory.39 The costs related to the performance of the USO are compensated for out of the universal service charge payable by communications undertakings whose turnover for communications services exceeds €383,500 per year. The rate of the universal service charge, established each year by the government, is 0.01 to 1 per cent of the turnover of a communications undertaking with the financing obligation in the preceding financial year. A communications undertaking with the USO is entitled to compensation for the unreasonably burdensome costs related to the performance of the obligation.40

Despite the detailed regulation of universal service providers, the competition situation in the markets for communications services is in good shape, all the services that can be designated as universal services are available on the market and no communication undertakings have currently been designated as universal service providers.

### iii Restrictions on the provision of service

**Obligation to provide access to communications networks and general terms and conditions obligations**

The EU directives that require communications undertakings to provide access to their networks have been transposed in national law by the ECA. Generally, communications undertakings are required to enter into a subscription contract with any person who submits an application to this effect. Entry into the contract may only be refused in specified cases, which include:

- a the technical impossibility in the requested area or manner to connect terminal equipment to the communications network;
- b failure by the applicant to provide information necessary for his or her identification or for communications with him or her, or the address of the location of the connection to the communications network allowing the provision of the requested communications service;
- c the provision of incorrect information upon submitting the application or upon entering into a requested subscription contract; or

38 Section 69-70 of the ECA.
39 Subsections 72(3)–72(4) of the ECA.
40 Sections 75, 81–84 of the ECA.
an applicant has a debt of collectable arrears for the provided communications services or the applicant is subject to bankruptcy proceedings.

If none of these conditions is fulfilled, the communications service provider is obliged to enter into a subscription agreement with the end user and to create a possibility for the end user to commence the use of the ECS within 10 working days after entry into a subscription contract, provided that the end user has performed the obligations assumed by the subscription contract.41

A communications service contract entered into with the end user must contain certain mandatory provisions. There is also formalised process with a one-month prior notice requirement for changes to general terms and conditions. The ECA establishes minimum information and mandatory terms that must be regulated in an ECS contract. These include, among others:

a. a description of the communications service and possibilities to use other related services;

b. charges for the services, including charges payable for maintenance, procedure for settlement of accounts as well as discounts and other price packages;

c. quality requirements set for the communications service, including service quality parameters;

d. the procedure and time limit for elimination of faults;

e. the procedure and time limit for submission of complaints and claims, and the procedure for resolution of disputes;

f. the term of the contract and conditions for cancellation and extension of the contract;

g. the measures taken by the communications undertaking to ensure security and integrity of communications networks and services; and

h. the terms and conditions of a product or communications service intended for end users with special needs.42

Some of the above contractual information (e.g., information on charges) and any standard terms used by the electronic communications undertaking must be made public on the website of the electronic communications undertaking or, in the absence thereof, in any other reasonable manner.43

Other than the mandatory provisions discussed above, the communications service provider and the end user are free to agree on contract terms.

**Net neutrality**

Regulation (EU) 2015/2120 laying down measures concerning open internet access is directly applicable in Estonia. Thus, all communications service providers in Estonia are under the obligation to treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.44 Estonia is a strong supporter of net neutrality, despite not having

---

41 Sections 93–94 of the ECA.
42 Subsection 96(1) of the ECA. The full list of mandatory terms can also be found therein.
43 Subsection 96(3) of the ECA.
44 Articles 3 and 4 of Regulation (EU) 2015/2120.
adopted any national legal acts or guidelines on net neutrality. The freedom and democracy watchdog Freedom House assesses that there are very few restrictions on internet content and communications in Estonia. There are no indications of any increase of restrictions on content or of self-censorship, and online debate is very active and open. Estonians have access to a wide range of content online, and very few resources are blocked or filtered by the government. Following court rulings on intermediary liability for third-party comments, some Estonian media outlets have modified their policies regarding anonymous commenting on their portals.45

Unsolicited phone calls, faxes, emails and texts

Estonia has implemented the e-Privacy Directive46 with the ECA. The requirements regarding marketing communications are different for legal and natural persons. Under the ECA, the use of electronic contact details of a natural person for direct marketing is allowed only with the person's prior consent (opt-in), while the use of electronic contact details of a legal person for direct marketing is allowed if, upon use of contact details, a clear and distinct opt-out opportunity is given to refuse such use of contact details free of charge and in an easy manner, and the person is allowed to exercise its opt-out right over an ECN.

Regardless of the above, if a communications service provider obtains the electronic contact details of a buyer, who is a natural or legal person, in connection with selling a product or providing a service, such contact details may still be used for direct marketing of its similar products to the buyer if the buyer is given, upon the initial collection of electronic contact details and each time when the buyer's electronic contact details are used for direct marketing, a clear and distinct opt-out opportunity free of charge and in an easy manner; and the buyer is allowed to exercise its right to refuse over an ECN.

It is important to note that the requirements described above do not apply to multiparty voice calls in real time, which have been excluded from the scope the implementation of the e-Privacy Directive in Estonia. Multiparty voice calls in real time are instead regulated in the Law of Obligations Act.47 Real-time multiparty calls may be used for communicating an offer only if the consumer has not expressly forbidden the use thereof. Thus, real time multiparty voice calls are subject to an opt-out possibility, while offers made to consumers by automated calling systems without human intervention, fax, telephone answering machine, electronic mail, SMS or other means are lawful only with the prior consent of the consumer.48

iv Privacy and data security

Cybersecurity regulations

On 9 May 2018, the Estonian parliament passed a new legislative act, the Cybersecurity Act,49 which entered into force on 23 May 2018. The Cybersecurity Act transposes into Estonian law the Security of Network and Information Systems Directive.50 The Act

48 Section 60 of the Law of Obligations Act.
provides requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities’ network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents. The Act is not applied to micro and small enterprises.51 The Act includes obligations, among others, for communications undertakings provided for in the ECA that provide cable distribution services consumed by at least 10,000 end users, and broadcasting network service providers upon providing cable distribution services or broadcasting network services. The Act also applies to Estonian Public Broadcasting and information society service providers within the meaning of the ISSA who offer online marketplaces, search engines or provide cloud computing services.52

The Cybersecurity Act requires the above-mentioned service providers to apply organisational, physical and information technological security measures for preventing and resolving cyber incidents, and preventing and mitigating any impact on the continuity of the service or the security of the system due to a cyber incident, or any possible impact on the continuity of another dependant service or the security of a system. Service providers are required, inter alia, to prepare a risk assessment and ensure its timeliness, ensure the monitoring of systems for detecting compromising actions and reduce the impact of cyber incidents. The Act also provides for an obligation to notify the Estonian Information System Authority (EISA) of cyber incidents. EISA is also responsible for the state and administrative supervision of compliance with the requirements of the Cybersecurity Act. Similarly, the ECA also includes a requirement to notify EISA immediately of all incidents endangering the security and integrity of the communications network and services that to a significant extent affect the functioning of the communications services or network, and of measures taken to eliminate such incidents.53

Under the ECA, a communications undertaking is required to take appropriate technical and organisational measures to manage the risks related to security and integrity of the communications services and network. The measures must be proportionate to the potential emergency situation, must ensure the minimum impact of incidents endangering the security and integrity of users of communications services and related networks, and must ensure continuity of the provided services.54 A communications undertaking must also guarantee the security of a communications network and prevent third persons from accessing (without legal grounds) the following data: information concerning specific details related to the use of communications services; the content and format of messages transmitted over the communications network; and information concerning the time and manner of transmission of messages.

If a specific hazard exists to a communications service or the security of the communications network, the communications undertaking must immediately inform subscribers of such hazard in a reasonable manner and, unless the hazard can be eliminated by measures taken by the undertaking, also of possible remedies and of any costs related thereto.55

51 Subsections 1(1) and 1(3) of the Cybersecurity Act.
52 Clauses 3(1)5), 3(1)10) and Subsection 4(1) of the Cybersecurity Act.
53 Subsection 87 2(2) of the ECA.
54 Subsection 87 2(1) of the ECA.
55 Section 101 of the ECA.
In the summer of 2017, the new Emergency Act\(^{56}\) entered into force, which includes a list of emergencies that justify the interruption in vital services. Vital services include, among others, phone services, mobile phone services, data transmission services, and digital identification and digital signing.\(^{57}\) A provider of a vital service is required to, among other things:

- prepare a continuity risk assessment and plan of the vital service provided thereby;
- implement measures that prevent interruptions of the vital service, including reducing the dependency on other vital services, essential contract partners, suppliers and information systems through duplicating technical systems, contracts, staff and other means important to the provision of the service, using alternative solutions, having and stocking necessary resources and other similar actions; and
- ensure the capability to guarantee the continuity and quick restoration of the service provided thereby during an emergency or another similar situation, including in the event of a technical failure or an interruption of the supply or another vital service.\(^{58}\)

**Privacy and personal data protection**

On 25 May 2018, the General Data Protection Regulation (GDPR)\(^{59}\) became applicable. This was of extreme importance in the communications sector, as the general rules set out in the GDPR are applicable in the communications sector. On 15 January 2019, the new Personal Data Protection Act (PDPA)\(^{60}\) became applicable, replacing the previous pre-GDPR act. The PDPA was followed by the Personal Data Protection Act Implementing Act,\(^{61}\) which came into force on 15 March 2019. The implementing act amends national legislation to establish legal conformity with the GDPR.

In conformity with the GDPR, the PDPA introduces specific grounds for processing of personal data. These include processing of personal data without the consent of the data subject for journalistic purposes, academic, artistic and literary expression, as well as for scientific and historical research and official statistics. More specifically, personal data may be processed and disclosed in the media for journalistic purposes without the consent of the data subject, in particular disclosed in the media, if there is public interest therefor and this is in accordance with the principles of journalism ethics. Disclosure of personal data must not cause excessive damage to the rights of any data subjects. Furthermore, some of data subjects’ rights, such as right of access, right to rectification and right to restriction of processing, inter alia, can be restricted when processing personal data for archiving in public interest.\(^{62}\) In connection with provision of information society services directly to a child, Estonia has specified that the age at which children can consent is 13 years.\(^{63}\)

In addition to the GDPR and the Personal Data Protection Act, some data protection requirements are also set out in the ECA. Under the ECA, a communications undertaking is required to maintain the confidentiality of all information that becomes known thereto in

---

57 Section 36 of the Emergency Act.
58 Subsection 38(3) of the Emergency Act.
62 Sections 4-7 of the PDPA.
63 Subsection 8(1) of the PDPA.
the process of the provision of communications services, and that concerns subscribers as well as other persons who have not entered into a contract for the provision of communications services but who use communications services with the consent of a subscriber. Above all, it must maintain the confidentiality of information concerning specific details related to the use of communications services; the content and format of messages transmitted over the communications network; information concerning the time and manner of transmission of messages.\footnote{Subsection 102(1) of the ECA.}

This information may be processed only if the undertaking notifies the subscriber, in a clear and unambiguous manner, of the purposes of processing the information and gives the subscriber an opportunity to opt out. Irrespective of whether the subscriber refuses such processing, the undertaking still has the right to collect and process such personal data without the consent of the subscriber:

a) that is necessary for the purposes of recording transactions made in the course of business and for other business-related exchange of information;
b) if the sole purpose of the processing is the provision of services over the communications network;
c) if it is necessary for the provision, upon the direct request of the subscriber, of information society services; or
d) that is necessary for billing the subscriber, including for the determination and calculation of interconnection charges.\footnote{Section 102 and 104 of the ECA.}

If the processing is done for publishing data on subscribers in number directories or through directory enquiry services, the processor must provide the subscribers with an opportunity to decide on whether and to what extent they wish such data to be published. Subscribers must also have an opportunity to verify and amend the data that concerns them, and to terminate the publication of such data.\footnote{Sections 102–107 of the ECA.}

The ECA also prescribes other requirements deriving from the e-Privacy Directive, as discussed above in subsection iii above.

\textit{Lawful interception and data retention}

Under Section 113 of the ECA, a communications undertaking must grant a surveillance agency or security authority access to the communications network for the conduct of surveillance activities or for the restriction of the right to confidentiality of messages, respectively. A communications undertaking is required to preserve the confidentiality of information related to the conduct of surveillance activities, and activities that restrict the right to inviolability of private life or the right to the confidentiality of messages. The electronic communications undertaking may recover the costs it incurs in relation to the provision of access to the communications network under the rules of Section 114 of the ECA.

Under Clause 111\textsuperscript{1}(11)\textsuperscript{5}) and Section 114\textsuperscript{1} of the ECA, a communications undertaking must provide certain retained data at the request of a court within civil matters.

\footnote{Subsection 102(1) of the ECA.}
\footnote{Section 102 and 104 of the ECA.}
\footnote{Sections 102–107 of the ECA.}
Obligations to retain data (as per the now-invalid Data Retention Directive\textsuperscript{67}) have been imposed under the ECA and have not been revoked despite the Digital Rights Ireland\textsuperscript{68} and the Tele2 Sverige\textsuperscript{69} rulings. Communications undertakings must retain for a period of one year an extensive amount of data under the ECA, and have an obligation to provide information to competent state authorities and courts.\textsuperscript{70}

**Protection of children online**

Estonia has adopted various laws that aim at protecting children online. For example, the Child Protection Act\textsuperscript{71} limits the permissibility of certain content to all children below the age of 18 years. It is prohibited to manufacture, show and disseminate to children content that promotes violence or cruelty, or contains pornographic content.\textsuperscript{72} The same is provided in the Act to Regulate Dissemination of Works which Contain Pornography or Promote Violence or Cruelty.\textsuperscript{73} This can be enforced in administrative proceedings by issuing a precept to terminate the violation and to restrict or take down the improper content. In the event of failure to comply with the precept, penalty payments can be imposed repeatedly until the precept is complied with. Parental consent cannot override the requirements set for content providers or limit their legal liability.

Note that under Estonian law, there are liability restrictions for information society service providers in the case of mere transmission, caching and storage. The latter is feasible if the service provider does not have actual knowledge of the contents of the information and, as regards claims for compensation for damage, is not aware of facts or circumstances from which the illegal activity or information is apparent. Additionally, the service provider must, upon obtaining knowledge or awareness of the facts specified above, act expeditiously to remove or to disable access to the information.\textsuperscript{74}

Sexual enticement of children below the age of 14 is criminalised and punishable under the Penal Code.\textsuperscript{75} Sexual enticement means, among others, handing over, displaying or otherwise knowingly making available pornographic works or reproductions to a person less than 14 years of age. This is punishable by a pecuniary punishment or up to three years’ imprisonment for natural persons and by a pecuniary punishment of €4,000 to €16 million for legal persons. Showing sexual abuse of a person aged less than 14 years, or engaging in sexual intercourse in the presence of such person or knowingly sexually enticing such person in any other way, are punishable by the same sanctions. Handing over, displaying or knowingly making available of works or reproductions of works promoting cruelty in another manner to a person of less than 14 years of age, or showing the killing or torturing of an animal in the presence of such person without due cause or knowingly exhibiting of cruelty to him or her in another manner, are punishable by a pecuniary punishment the amount of which is up to €3,200 in the case of legal persons.\textsuperscript{76}

\textsuperscript{67} Directive 2006/24/EC.
\textsuperscript{68} Judgement of the Court of Justice of the European Union (CJEU) of 8 April 2014 in case C-293/12.
\textsuperscript{69} Judgement of the CJEU of 21 December 2016 in joined cases C-203/15 and C-698/15.
\textsuperscript{70} Section 111\textsuperscript{1} of the ECA.
\textsuperscript{72} Section 25 of the Child Protection Act.
\textsuperscript{74} Sections 8–10 of the ISSA.
\textsuperscript{76} Sections 179–180 of the Penal Code.

© 2019 Law Business Research Ltd
The MSA also includes provisions that are aimed at protecting children. Television and radio service providers may not transmit programmes that may cause substantial physical, mental or moral detriment to minors, in particular such programmes that include pornography or that propagate violence or cruelty for the purposes of the Act to Regulate Dissemination of Works which Contain Pornography or Promote Violence or Cruelty. On-demand audiovisual media services that may cause substantial damage to the physical, mental or moral development of a minor must be made accessible by the on-demand audiovisual media service provider by means of personal identification codes or other relevant technical solutions only in a manner that is not accessible to minors under normal circumstances.77

The Advertising Act78 includes several requirements for advertising directed at persons less than 18 years of age. Advertising that targets groups that are primarily made up of children must take into account their unique physical and mental state resulting from their age. Children may not be a target group of advertising if it is prohibited to sell the advertised goods or provide the advertised services to children. Advertising that targets groups that are primarily made up of children may not:

a create the impression that the acquisition of certain goods or the use of certain services will give the child an advantage over other children or that the lack thereof will have the opposite effect;
b create feelings of inferiority in children;
c incite children to behave or act in a manner that has or may have the effect of bringing children into unsafe conditions;
d contain elements that frighten children;
e exploit the trust children place in their parents, teachers or other persons;
f include a direct or indirect appeal to children to demand the acquisition of the advertised goods or the use of the advertised services from other persons; or
g directly incite children to enter into transactions independently.79

These requirements also apply to any online advertising.

IV SPECTRUM POLICY
i Development

The Estonian spectrum policy is changing continuously. The demand for spectrum is increasing rapidly with the development of and increasing demand for new technologies and mobile communications services. Currently, the 5G mobile network is being developed. All this proves to be a challenge in conditions where frequency spectrum is a scarce resource.

To tackle this challenge, the Estonian Radio Frequency Allocation Plan is constantly changing to conform to new developments. The use of RFs in Estonia is harmonised with those of the EU, as Estonia takes account of the recommendations of the European Commission to the greatest extent possible.80 The ECA provides that the purpose of regulating the management of RFs is to ensure the purposeful, objective, transparent and proportionate
management, and the effective and efficient use, of RFs for the needs of users of RFs and for
the provision of communications services, the creation of possibilities for the development of
new technologies and fast elimination of radio interference. The Radio Frequency Allocation
Plan determines, among other things, the RF bands for the introduction of new technologies
together with restrictions on new and existing users. The ECTRA reviews the allocation plan
at least once a year and submits to the responsible minister proposals for amendments if the
development of electronic communications technology requires it.81

ii Flexible spectrum use

As discussed above, the use of spectrum requires its prior allocation by the ECTRA. Spectrum
is allocated on the basis of the Radio Frequency Allocation Plan, which determines the manner,
regime and purpose of using frequency bands. Upon granting a frequency authorisation to
a communications undertaking, the ECTRA establishes in the authorisation, among other
things, the purpose, manner, conditions and area or location of the use of spectrum, as well
as the requirements for the shared use of RFs. Therefore the authorisation may include in
its conditions the possibility to share the use of spectrum, as well as the possibility to trade
frequency or grant it for use on the basis of a contract. Accordingly, the use of spectrum is
made more flexible by way of allowing such trading and shared use of spectrum.

In addition, the ECTRA carries out spectrum auctions in previously unused frequency
ranges and rearranges the use of spectrum, if need be, as discussed further below.

iii Broadband and next-generation services spectrum use

The ECTRA is also constantly dealing with the need for new uses of mobile spectrum. For
example, in 2015 it rearranged the frequency usage of mobile operators in the 900MHz band
to enable the introduction of new technologies. In the course of the process, the frequency
blocks of each operator were rearranged so that complete frequency ranges were allocated to
each operator to create wider bandwidth and create conditions for introducing new 4G and
5G technologies.82

If the ECTRA finds that the number of available spectra is not sufficient for their
allocation, it can hold a public competition in the form of a spectrum auction. The latest
auction of mobile broadband spectrum ended in May 2017. The auction of frequencies in
the ranges of 2,540–2,570MHz, 2,660–2,690MHz and 2,575–2,615MHz ended with the
selling of three frequency division duplexes (FDD) and two time division duplexes (TDD)
that provide the right to use 100MHz-worth of spectrum in Estonia. Two operators, Elisa
Eesti AS and Telia Eesti AS, participated. FDD I and II were bought by Telia, bidding
€1,601,234 and €3,605,535 respectively. FDD III, TDD I and II were bought by Elisa,
bidding €2,608,789, €1,612,346 and €1,597,001 respectively. Accordingly, around
€11 million was earned through the auction.83

After the digital switchover occurred on 1 July 2010, the freed-up frequencies were
allocated for 4G mobile communication services. It can therefore be said that more and more
spectrum is becoming available for mobile services. More specifically, the latest and upcoming
auctions are focused on 5G technologies. During the Estonian presidency of the Council of

81 Subsection 9(2) and Clause 10(1)1) of the ECA.
the EU from July to December 2017, a Ministerial Declaration was signed to make 5G a success for Europe.\textsuperscript{84} It was agreed that 5G is the vision for a fully connected European society and a path towards the European gigabit society. The crucial step in implementing this vision is to make more spectrum available in a timely and predictable manner. To realise this goal, it is necessary to release 5G spectrum bands.\textsuperscript{85} In March 2019, the Ministry of Economic Affairs and Communications published a 5G Roadmap for Estonia, aspiring to achieve 5G coverage in larger cities and their peripheral areas by 2023 and in transport corridors by 2025.\textsuperscript{86} The plan further envisages international Connected Automated Driving corridors and more leeway for small-cell 5G networks.

\section*{iv \hspace{1em} Spectrum auctions and fees}

The ECTRA carries out auctions if it finds that the number of available spectra is not sufficient for their allocation.

Following a consultation with the stakeholders, the ECTRA decided to divide the separable bandwidth of 3,410–3,800MHz into three time division duplexes (TDD) large enough (3x130MHz) to implement the large data amounts and facilitate the future development of 5G technologies: 3,410–3,540MHz, 3,540–3,670MHz and 3,670–3,800MHz. Additionally, a fourth smaller buffer zone was left to ensure undisturbed operation of defence forces equipment.\textsuperscript{87} This frequency band is considered as the most important 5G frequency range in the European 5G Roadmap, which will allow the use of innovative technologies and devices (IoT).\textsuperscript{88} In February 2019, the ECTRA announced the auction for the 3,410–3,800MHz frequency range for the development of 5G technology with a starting price of €1,597,000 for each range. The auction was suspended in March 2019 following an appeal by Levikom, a broadband network operator, which argued that dividing the frequency into three large ranges stifles competition and provides an unfair advantage to big operators.\textsuperscript{89} In its opinion, the Estonian Competition Authority urged the Ministry to consider auctioning the spectrum in smaller 5–10MHz ranges.\textsuperscript{90}

In addition to the currently suspended 3,410–3,800MHz auction, the Ministry of Economic Affairs and Communications is planning to auction spectrum in the 700MHz frequency band in the first half of 2020. Furthermore, a public consultation for the use of 26GHz frequency band is to take place before the end of 2019 and a study for the use of spectrum in the 40.5–43.5GHz and 66–71GHz frequency range is planned for the future.\textsuperscript{91}

\begin{itemize}
\item \textsuperscript{84} https://www.eu2017.ee/sites/default/files/inline-files/Ministerial%20declaration%205G_final_1.pdf.
\item \textsuperscript{85} https://www.mkm.ee/sites/default/files/8.a_b_aoh_5g_roadmap_final.pdf.
\item \textsuperscript{86} https://www.mkm.ee/sites/default/files/eesti_5g_teekaart.pdf.
\item \textsuperscript{88} https://www.tja.ee/et/uudised/algasid-ettevalmistused-3600-mhz-sageduslubade-avaliku-konkursi-korraldamiseks.
\item \textsuperscript{89} https://news.err.ee/929416/court-cancels-5g-frequency-auction-pending-competition-complaint-decision.
\item \textsuperscript{90} https://www.konkurentsiamet.ee/public/Konkurentsiameti_seisukohit_5G_sageduslubade_suhtes.PDF.
\item \textsuperscript{91} https://www.mkm.ee/sites/default/files/eesti_5g_teekaart.pdf.
\end{itemize}
V MEDIA

i Regulation of media distribution generally
Media services are subject to the licensing obligations discussed above. In addition, there are restrictions on content that are one of the pre-requirements for obtaining licences.

For example, the MSA requires a television and radio service provider to reserve at least 5 per cent of the daily transmission time of the programme service on at least six days a week for transmitting self-produced new programmes, except on national holidays. At least 10 per cent of the monthly transmission time must be reserved for transmission of own productions, deducting the transmission time allocated for news, sporting events and games programmes as well as for advertising, teletext services and teleshopping. At least 50 per cent of the minimum capacity of own production must be shown during prime time between 7pm and 11pm. At least 51 per cent of the annual capacity of the television programme service must be reserved for transmission of audiovisual works of European origin, deducting the transmission time allocated for news, sporting events and games programmes, as well as for advertising, teleshopping and teletext services, and at least 10 per cent of such audiovisual works must have been created by producers that are independent of this television service provider. These requirements are subject to certain exceptions; for example, local channels are exempted from some of them.92

The MSA also sets out some requirements for commercial communications, TV and radio advertising, sponsorship and product placements. In addition to the MSA, these are regulated by the Advertising Act.

ii Internet-delivered video content
Besides television services, on-demand audiovisual media services are becoming increasingly popular. On-demand audiovisual media services do not require a licence, but do require a notification of economic activities to be submitted through the state portal or to a notary, as discussed above.

Most of the biggest ISPs in Estonia have started their own video distribution services. However, this does not limit the accessibility of on-demand services of other service providers. Standalone services are also freely accessible. However, generally service providers measure the use of data without taking into account that part of the data that is used for VOD. Still, it must be noted that there are examples on the market of ISPs’ own on-demand video distribution services that do not use up mobile data if streamed via the service provider’s own networks. Thus, one the strategies used to attract customers to buy video distribution services is that ISPs do not charge for the data used on streaming via mobiles on their own VOD services equally with the data used for other VOD services.

VI THE YEAR IN REVIEW
The most important changes in the legislation concerning the ICT sector in 2018 and 2019 have been regarding the GDPR, the Cyber Security Act and the auctioning of 5G spectrum frequency.

The GDPR became applicable on 25 May 2018, which required companies to adjust their data processing practices and gave people greater control over the use of their personal data.

92 Section 8 of the MSA.
On 15 January 2019, Estonia adopted the new Personal Data Protection Act (PDPA), replacing the previous pre-GDPR act. The PDPA was followed by the Personal Data Protection Act Implementing Act, which came into force on 15 March 2019 and acts to amend national legislation to establish legal conformity with the GDPR.

The Cyber Security Act entered into force on 23 May 2018. The Act provides requirements regarding the maintenance of network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents, and lays down numerous obligations for communications services and information society service providers to ensure cybersecurity.

In 2019, Estonia announced its national strategy for the development and implementation of artificial intelligence. The plan includes public-private partnership initiatives, further e-state services and sandboxes for testing and developing public sector solutions, among others.93

Significant recent transactions include the acquisition of Apollo Group by UP Invest and the acquisition of Baltic Classifieds Group by private equity firm Apax Partners.

In the summer of 2019, the Estonian Competition Authority cleared private equity firm Apax Partners’ acquisition of the 100 per cent share of the Baltic Classifieds Group from UP Invest.94 Baltic Classifieds Group operates specialised and general online classifieds portals in the Baltics. The Estonian Competition Authority also cleared the acquisition of Apollo Group by UP Invest. UP Invest holds 78 per cent of Apollo Group shares following the transaction.95 Apollo Group operates in the entertainment market, managing the Apollo book store and cinema chain.

Most of the major mobile service providers have recently come out with their own VOD services, such as Elisa’s Elisa Elamus and Telia’s TELIA TV, which includes FOX NOW, Eurosport Player and HBO. This marks a growing demand for VOD among viewers.

Telia, a major mobile and internet service provider, recently announced the launch of a new TV channel which will broadcast sports, movies and series. The channel will reach viewers in early 2020.96

With VOD and mobile internet becoming increasingly in demand, the EU also saw the growing need for the lowering of roaming charges. Eventually, on 15 June 2017 Regulation (EU) 2017/920 became applicable, which significantly lowered roaming charges in the European Union. The Regulation allows consumers to choose a subscription service that allows them to use mobile services within the EEA on the same conditions as in Estonia.

With the above developments, there is also an increasing demand for spectrum on the market. An auction for spectrum in the 3,600MHz frequency range in three 130MHz time division duplexes was announced in early 2019, but suspended shortly after a local broadband operator appealed the auction claiming it stifles competition. The Ministry of Economic Affairs and Communications is planning to auction spectrum in the 700MHz frequency band in the first half of 2020.

VII CONCLUSIONS AND OUTLOOK

Looking ahead, some of the next important developments in the communications, technology and media sector are the following.

From 1 January 2019, the Estonian Technical Regulatory Authority and the Consumer Protection Board have been joined into one single regulatory authority: the Consumer Protection and Technical Regulatory Authority (ECTRA). The new Authority resumed the obligations of the Technical Regulatory Authority and the Consumer Protection Board.97

In November 2019, all the current radio service providers’ licences will expire. The ECTRA and the Ministry of Culture carried out a competition for radio licences for the period of 2019 to 2024. The ECTRA issued a total of 28 radio service provider licences, most of which were to service providers who previously held a licence.98

The Estonian ICT sector is fast-developing and highly important to the legislators. The government’s goals include developing and implementing artificial intelligence technology, bringing ultrafast internet to more and more end users and promoting Estonia as the world’s capital of innovation regarding the communications and information society. However, there are still challenges for policymakers caused by convergence and ultra-fast developments in the sector.

Generally, Estonia follows European policies, and has successfully implemented the various pieces of EU legislation into national law. One shortcoming concerns the rules on data retention by communications service providers, which are based on an invalid directive and have not been revoked from national law.

Chapter 6

EU OVERVIEW

Marco D'Ostuni, Gianluca Faella and Manuela Becchimanzi

I OVERVIEW

The EU’s effort to build a comprehensive set of rules for the digital single market is nearing completion.

In 2019, many new pieces of legislation have been adopted or entered into force across the EU, such as the European Electronic Communications Code (EECC), the Regulation on the free flow of non-personal data, the new Audiovisual Media Service Directive (AVMSD) and the Directive on copyright.

The EECC creates a new regulatory framework for electronic communications, focusing on encouraging investments in high-capacity networks.

The new regulation on the protection of personal data in electronic communications, which is meant to apply not only to traditional telecom operators, but also to OTT service providers (such as WhatsApp, Facebook and Skype), is expected to be adopted by the end of 2019.

Moreover, in March 2019 the Commission issued its decision in the proceedings initiated against Google concerning the AdSense search advertising service, imposing a fine of €1.49 billion for abusive practices in online advertising.

II REGULATION

i The regulators

The European Commission (Commission) is the main regulatory body at the EU level. The Commission is equipped with a variety of regulatory and enforcement powers in areas related to TMT, including antitrust, privacy, online transactions, intellectual property and consolidation of the internal market for electronic communications. The Commission oversees the measures proposed by national regulatory authorities (NRAs) to address problems relating to competition in telecommunications markets.

The BEREC Regulation established the Body of European Regulators for Electronic Communications (BEREC), which became fully functional in 2011. Its role is to guarantee consistent application of the EU regulatory framework by, for example, delivering opinions

1 Marco D’Ostuni is a partner, Gianluca Faella is counsel and Manuela Becchimanzi is an associate at Cleary Gottlieb Steen & Hamilton LLP.
2 See Section III.iv.
on NRAs’ draft regulatory measures and, upon request, offering assistance to NRAs in carrying out their duties under EU law. The Commission turns to BEREC before adopting recommendations on relevant product and service markets, which guide NRAs when they define the relevant national markets. The Commission may also task BEREC with carrying out ad hoc market studies.

In September 2016, the Commission proposed an updated BEREC Regulation to transform BEREC into an agency. The Commission’s ambitious proposal envisaged turning BEREC into an agency with legally binding powers to ensure that the regulatory framework is applied consistently. However, in a draft report presented in February 2017, the appointed rapporteur stated that the status quo is functioning well and suggested that there is no need to turn BEREC into an agency. Accordingly, the initial proposal was scaled down. In the final trilogue on this matter, held on 5 June 2018, the European Parliament and the Council agreed on a compromise.

The new BEREC Regulation, which entered into force on 20 December 2018, repeals Regulation (EC) No. 1211/2009. BEREC remains a body of national regulators, with no regulatory powers. However, the new regulation establishes the Agency for Support for BEREC (BEREC Office), which has legal personality, and strengthens the role of BEREC. The latter is entrusted with ensuring the consistent implementation of the regulatory framework for electronic communications across the EU. To avoid fragmented implementation, BEREC will issue advices to the NRAs as well as draft opinions and guidelines.

ii Regulated activities

In 2002, the EU adopted a new comprehensive regulatory framework for ECNs and services, with the aim of fostering consistent regulation across the EU. In 2009, Directive 2009/140/EC, Directive 2009/136/EC and Regulation (EC) No. 1211/2009 were adopted to improve and revise the 2002 regulatory framework.

As part of the DSM strategy, in May 2015 the Commission announced a complete review of the framework for electronic communications. The consultation closed in December 2015. In the context of the 2016 annual State of the Union, the Commission presented the connectivity package, proposing to strengthen the role of BEREC and to recast four of the existing directives (the Framework, Authorisation, Access and Universal Service Directives) into a new European code.


Within the framework of the DSM strategy, new rules to modernise the EU copyright regime, including two regulations and two directives, were adopted between 2017 and 2019.12

In particular, in March 2019 and April 2019, respectively, the Parliament (in plenary) and the Council approved a new Directive on copyright in the Digital Single Market (see Section VI). The Directive was published on 15 May 2019 in the Official Journal of the European Union and Member States must transpose the new rules into national law by 7 June 2021.

Audiovisual content was previously regulated by the Television Without Frontiers Directive. With the last revision in 2007, the Directive was renamed the Audiovisual Media Services Directive (AVMS), which was then codified in 2010.13 In May 2016, the Commission tabled a proposal to reform the AVMS Directive. The new AVMS Directive was published in the Official Journal of the European Union on 28 November 2018 and Member States have 21 months to transpose it into national legislation (see Section V).

In the framework of the DSM strategy, the Commission adopted a regulation on geo-blocking and other forms of discrimination based on nationality, residence or place of establishment, which targets unjustified geographically based restrictions to cross-border trade. The new regulation against unjustified geo-blocking entered into force on 22 March 2018 and applies from 3 December 2018.14 The Regulation prohibits traders from discriminating against customers by denying them access to internet content on the basis of their location, and allows re-routing to a different version of a website only if a customer has given prior consent. It also prohibits discrimination of customers in relation to payments.

Geo-blocking measures also affect the portability of online services: users who have subscribed to certain online content (such as music, films, e-books and videogames) in their country are often denied access to the same content while travelling in another Member State. To address this issue, on 14 June 2017, the Parliament and the Council adopted the Regulation on cross-border portability of online content services, which applies from


14 See Regulation of the European Parliament and the Council (EU) 2018/302 of 23 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers’ nationality, place of residence or place of establishment within the internal market.
1 April 2018.\textsuperscript{15} The regulation ensures that subscribers to online content services in the EU have the right to access and use these services while temporarily present in another Member State (e.g., in the case of holidays, business trips or learning periods).

The Commission also has extensive investigative powers in the area of antitrust. It cooperates with national competition authorities (NCAs) to prohibit concerted practices, agreements restricting competition and unilateral anticompetitive behaviour. The Commission has exclusive jurisdiction over mergers above certain thresholds, including in the area of TMT.\textsuperscript{16}

iii Ownership and market access restrictions

In principle, EU undertakings and undertakings from non-EU states with reciprocity agreements can freely provide electronic communication services and networks. As previously established by the Authorisation Directive,\textsuperscript{17} under the EECC a prospective electronic communications provider needs an authorisation from the competent NRA (Article 12). Any limitation set by a Member State to the freedom to provide electronic communications networks and services must be duly motivated and notified to the Commission. Obtaining the authorisation involves a procedure whereby an applicant notifies the NRA of its intentions and does not have to wait for approval by the NRA. The information that may be requested in such a notification must be limited to what is necessary to identify the provider. Even though the proposed amendment of having a single notification to BEREC was not inserted in the EECC, the information that may be requested by the NRAs has been harmonised (Article 12.4).

However, number-independent interpersonal communications services, which under the new EECC fall into the category of electronic communications services (ECS), are not subject to the general authorisation regime requiring registration with the NRAs.

Finally, the use of spectrum in telecommunications is subject to a licence granted by Member States.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

On 25 November 2015, the European Parliament and the Council adopted Regulation (EU) No. 2015/2120 (Open Internet Regulation).\textsuperscript{18} The Open Internet Regulation aims, first of all, to safeguard net neutrality. Within the EU, all internet traffic will be treated equally, subject to some specific public interest exceptions (e.g., those concerning network security and child pornography). Providers of internet access services must abstain from any discrimination, restriction or interference, irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.\textsuperscript{19} Blocking, throttling, degradation

\textsuperscript{18} Regulation (EU) No. 2015/2120, Article 3.
or discrimination of internet traffic by ISPs is prohibited. IAPs can still adopt different traffic management measures without being discriminatory, but only for ‘objectively different categories of traffic’ (e.g., services like e-medicine), rather than for commercial reasons.\(^\text{20}\)

Traffic management measures that do not comply with the above requirements are allowed only under three specific exceptions: compliance with EU or national legislation that requires, for example, blocking of specific content, applications or services; protection of the integrity and security of the network; and prevention of network congestions that are temporary or occur in exceptional circumstances.

For a limited number of services, such as high-quality voice calling on mobile networks, linear (live) broadcasting IPTV services with specific quality requirements and real-time health services (e.g., remote surgery), for which an assured level of access is indispensable to deliver the service, the Regulation allows for the provision of fast lanes provided that network capacity is sufficient.\(^\text{21}\)

In addition, the Regulation provides for the end of roaming charges, which became effective from 15 June 2017 through a gradual one-year phase-out process.

On 30 April 2019, the Commission issued a report on the implementation of the Open Internet Regulation,\(^\text{22}\) concluding that the Regulation’s principles are effective in protecting end users’ rights and promoting open access to the internet.

ii Universal service

The EECC updates the EU universal service rules previously provided for by the repealed Universal Service Directive.\(^\text{23}\) Pursuant to Article 84, Member States must now also ensure the provision of affordable access to ‘adequate broadband’, in addition to voice communication services available at a fixed location. Adequate broadband is defined, taking into account BEREC reports, as the band ‘necessary for social and economic participation in society’ (i.e., the minimum quantity that is needed for services such as email, internet banking, instant messaging, calls, video calls and social media).

The EECC entrusts NRAs with monitoring the retail prices of broadband internet access service and voice communications services, in particular in relation to national prices and national consumer income. If prices prevent consumers with a low income from accessing those services, Member States may require service providers to grant special tariff options, different from normal commercial conditions.

Pursuant to Article 90, the net costs of universal service must be financed by general taxpayer funds or specific taxes levied on electronic communications networks and service providers.


\(^{21}\) The Regulation also includes a number of transparency measures for providers to ensure customer awareness of open internet access, and provides that national regulatory authorities have to monitor providers’ compliance with the minimum service quality standards. Regulation (EU) No. 2015/2120, Articles 4 and 5.


Restrictions on the provision of service

NGA Recommendation

The Commission adopted a recommendation on NGA networks on 20 September 2010.24 The NGA Recommendation seeks to provide NRAs with guidance to promote a common approach when deciding whether to impose obligations on incumbents in connection with NGA networks.

The Recommendation primarily covers remedies to be imposed on operators deemed to have significant market power. However, where it is justified on the grounds that duplication of infrastructure is economically inefficient or physically impracticable, NRAs may also impose obligations of reciprocal sharing of facilities on non-dominant undertakings, which would be appropriate to overcome bottlenecks in the civil engineering infrastructure and terminating segments.

The EECC reaffirms the obligation for operators with significant market power to grant rights to use or rights of access to civil infrastructure (such as, among others, buildings, antennae, towers, poles, ducts), when the NRAs consider that access denial would hinder competition on the market and would not be in the end user’s interest (Article 72).

Access Recommendation

After a long debate with BEREC and NRAs, the Commission published a recommendation on access remedies on 11 September 2013.25 The Access Recommendation relies on two pillars: ensuring equivalence of access and setting out a harmonised costing methodology.

As to the first pillar, the Commission suggests that equivalence of input (EoI) (i.e., the supply to competitors of the same access services enjoyed by a vertically integrated company’s downstream units) is in principle the surest way to avoid non-price discrimination.26

As to the second pillar, the Commission suggested the adoption of a common costing methodology (called bottom up – LRIC +) that, for copper-based local loop unbundling services, should have led to monthly tariffs within a defined price band.27 The Commission recommended that, once they have set tariffs within the mentioned price band, NRAs should not modify the costing methodology (and hence the tariffs) without a market-analysis procedure, and should avoid undue price fluctuations by ensuring stable access prices over at least two review periods (i.e., about six years).

26 The EoI model ensures that the incumbent’s and competitors’ downstream access products use exactly the same physical upstream inputs (e.g., same tie cables, same electronic equipment, same exchange space). Conversely, the equivalence of output model ensures that the access products offered by the incumbent to alternative operators are comparable to the products it provides to its retail division in terms of functionality and price, but they may be provided by using different systems and processes.
27 BEREC issued its Report on the Regulatory Accounting in Practice 2013, according to which data from NRAs generally confirmed the trend toward an increasingly consistent approach to regulatory accounting obligations among NRAs. The Report on the Regulatory Accounting in Practice 2018 confirms that the degree of consistent application of methodologies continues to be high among NRAs.
The EECC makes reference to the costing methodology set out in the Access Recommendation, stating that the method of cost recovery should take into account (1) the need to promote efficiency, sustainable competition and the deployment of high-capacity networks, and (2) the need to have predictable and stable wholesale prices for the benefit of operators seeking to deploy new and enhanced networks.

Monitoring and control of content

The Electronic Commerce Directive explicitly sets out that no intermediary should be obliged to engage in monitoring activities of a general nature (mere conduit rule).

The interpretation of the mere conduit rule was probed in two cases before the CJEU, which concerned the possible responsibility of Scarlet (an ISP) and Netlog (a social networking website) for exchanges of allegedly unlawful content by its users. In essence, according to the CJEU, the EU framework does not require a hosting service provider to filter all information stored by users as a preventive measure. However, the Court left open the question on the admissibility of injunctions against specifically determined copyright-infringing practices.

On 27 March 2014, the CJEU held that an ISP may be ordered to block its customers’ access to a copyright-infringing website (UPC Telekabel). In September 2016, the CJEU provided an interpretation of the mere conduit rule in a case concerning the liability of free Wi-Fi network providers for copyright infringements committed by its users (Mc Fadden). The CJEU stated that, under the mere conduit rule, the provider of a free Wi-Fi connection cannot be held responsible for the download of unlawful content by its users. However, the copyright holder can seek an injunction ordering such open Wi-Fi to be protected with a password, as this would prevent future infringements by requiring users to reveal their identity.

In August 2018, the CJEU stated that the mere conduit rule must be interpreted as meaning that the limitations of liability apply to the provider of an IP address rental service allowing the anonymous use of internet domain names, insofar as the activity of such a service provider is of a merely technical, automatic and passive nature, meaning that it has neither knowledge of, nor control over, the information transmitted or cached by its customers, and insofar as it does not play an active role in allowing those customers to optimise their online sales activity.

The proposal for the Directive on Copyright in the Digital Single Market contained a provision (in Article 13) that appeared to be more far-reaching than the mere conduit rule, as it required information society service providers to take appropriate and proportionate measures to ensure copyright protection also through effective content recognition technologies, thus introducing, to a certain extent, an obligation to monitor. However, the

28 See Paragraph 192 of the EECC.
29 Directive 2000/31/EC.
30 See Section 4, Articles 12 to 15.
31 Cases C-70/10, Scarlet Extended v. SABAM; and Case C-360/10, Sabam v. Netlog NY. For more details on these judgments, see this chapter in the seventh edition of this publication.
32 Case C–314/12 UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH. For more details on this judgment, see this chapter in the ninth edition of this publication.
33 Case C-484/14, Mt Fadden v. Sony Music.
34 Case C-521/17, Coöperatieve Vereniging SNB-REACT U.A. v. Deepak Mehta.
35 See footnote 12.
final version of the Directive on copyright in the Digital Single Market does not contain this provision, and it expressly states that no general monitoring obligation is imposed on ISPs (Article 17.8).

Another crucial aspect concerning the role of ISPs relates to the right to be forgotten. On 13 May 2014, the CJEU held that, by searching systematically for information published on the internet, indexing websites, and recording and making them available, the operator of a search engine is processing personal data within the meaning of Article 2(b) of Directive 95/46/EC (Google Spain).\(^{36}\)

The Court did not describe such processing as unlawful, but clarified that even initially lawful processing of accurate data may become incompatible with the Directive ‘where those data are no longer necessary in the light of the purposes for which they were collected or processed [. . .] in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed’.\(^{37}\)

The CJEU addressed the extent of the right to be forgotten in two judgments adopted on 24 September 2019.\(^{38}\) The cases were referred to the Court by the French Council of State and focus on two main issues: whether the right to be forgotten should be absolute - that is, automatic removal is required when the content involves sensitive personal data, such as political affiliations or a criminal record; and whether the right to be forgotten should apply globally, beyond the boundaries of Europe.

In the first case the Court concluded that the operator of a search engine is in principle required to accede to requests for de-referencing in relation to links to web pages containing sensitive personal data. It is, however, required to ascertain whether the inclusion of that link in the list of results displayed following a search on the basis of the data subject’s name is strictly necessary for protecting the freedom of information of internet users. Where the information relates to an earlier stage of the legal proceedings in which the person is involved that no longer corresponds to the current situation, the operator of a search engine is in principle required to accede to a request for de-referencing.

In the second judgment, the Court concluded that where a search engine operator grants a request for de-referencing a certain link, it is not required to de-reference it globally (i.e., on all versions of its search engine), but only on the versions of that search engine used in the EU Member States.

---

\(^{36}\) Case C-131/12, Google Spain SL, Google Inc/Agencia Española de Protección de Datos, Mario Costeja González, Paragraphs 28 and 41. For more details on these judgments, see this chapter in the seventh edition of this publication.

\(^{37}\) The Directive grants individuals the right to obtain from the controller rectification, erasure or blocking of personal data (Article 12(b)) and to object to processing on compelling legitimate grounds (Article 14). The Court affirmed that these rights can also be invoked against search engines since ‘it is the search engine operator which determines the purposes and means of that activity and [. . .] must, consequently, be regarded as the ‘controller’ in respect of that processing pursuant to Article 2(d)’ (Paragraph 33).

\(^{38}\) C-136/17, G C and Others (Déréférencement de données sensibles); Case C-507/17, Google v. Commission nationale de l’informatique et des libertés (CNIL).
On 28 September 2017, the Commission presented guidelines for online platforms to tackle illegal content\(^{39}\) aimed at improving the prevention, detection and effective removal of illegal content inciting terrorist propaganda and racist speech, and also preventing its reappearance through automatic tools.

Building upon the guidelines, on 1 March 2018 the Commission proposed a recommendation containing a set of operational measures to be taken by companies and Member States to remove illegal online content, such as the creation of fast-track procedures for trusted flaggers (i.e., individuals or entities considered by a hosting service provider to have particular expertise and responsibilities for the purposes of tackling illegal online content).\(^{40}\) In particular, terrorist content should be removed within one hour following a referral by Europol or other competent authorities.

Finally, in April 2018 the Commission adopted a communication calling upon platforms to increase their efforts to tackle online disinformation and the spread of fake news.\(^{41}\) In particular, platforms should improve the scrutiny of advertisement placements, ensure transparency about sponsored content and close fake accounts more efficiently.

On 26 September 2018, a Code of Practice was published by online platforms, leading social networks, advertisers and the advertising industry. The self-regulatory Code of Practice is the first outcome of the April 2018 Communication and aims to reduce online disinformation by, for example, implementing a better scrutiny of advertisement placements to demonetise the spreading of disinformation, or making it easier for users to discover and access trustworthy and diverse news sources.

\(\textbf{iv} \quad \textbf{Security}\)

\(\textbf{Privacy and data retention}\)

On 27 April 2016, the European Parliament and the Council adopted the General Data Protection Regulation (GDPR)\(^{42}\) together with the Police and Criminal Justice Data Protection Directive.\(^{43}\) On 25 May 2018, the GDPR entered into force. It replaced the EU Data Protection Directive\(^{44}\) and harmonised the processing of personal data by companies and public authorities across the EU.

Member States had to implement the Criminal Justice Data Protection Directive by 6 May 2018.

The Council and the Parliament made important changes to the Commission’s proposal, remarking that, inter alia:

---


\(^{44}\) Directive (EC) No. 1995/46 of 24 October 1995, OJ L281/1 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
data protection is not an absolute right and must be weighed against other fundamental rights; 45

data portability is restricted to data provided by individuals and does not apply if it adversely affects the rights and freedoms of others; 46

automated decision-making, including profiling, is permitted for fraud and tax evasion monitoring and prevention purposes, and to ensure the security and reliability of a service provided by a controller; 47 and

sanctions are to be proportionate. 48

The new rules principally advantage small and medium-sized enterprises by reducing unnecessary administrative requirements such as notification requirements for companies. The right to be forgotten has been reinforced, and a right to data portability facilitates transfer of personal data between service providers. Furthermore, the Regulation provides that market operators established outside Europe will have to apply the same rules when offering services in the EU, and it brings forward a one-stop shop for companies and users, who will only have to deal with one single supervisory authority, facilitating cross-border operations and business in the EU. The Regulation also ensures stronger protection against data breaches, as it provides that a company experiencing a breach has to report it to the relevant data protection authority within 72 hours.

In line with the Data Protection Directive previously in force, Article 45 of the GDPR provides that the transfer of personal data from the EU to a country outside the EU or EEA may take place if that third country ensures an adequate level of protection of the data. The Commission has the power to determine whether a third country ensures an adequate level of protection, taking into account the relevant domestic legislation, respect for human rights and fundamental freedoms, and the international agreements that the third country concerned has entered into.

In 2000, under the regime previously in force, the Commission adopted a decision on the adequacy of the protection provided by the safe harbour privacy principles with regard to the US (Safe Harbor Adequacy decision). 49 On 6 October 2015, the CJEU invalidated the 2000 Safe Harbor decision. 50

In February 2016, the Commission put forward a successor agreement (known as the EU–US Privacy Shield). 51 As in the case of the former Safe Harbor agreement, the Privacy Shield is intended to enable personal data of EU citizens to be transmitted to and processed in

50 Case C-362/14, Maximillian Schrems v. Data Protection Commissioner. For more details on this judgment, see this chapter in the seventh edition of this publication.
51 In the meantime, Article 26 of Data Protection Directive applies. The latter provides for some alternative grounds on which specific data transfers may take place absent an Article 25 adequacy decision. In particular, transfers may be carried out where the entity responsible for determining the purposes and means of the processing of personal data adduces appropriate safeguards, including contractual clauses binding the exporter and the importer of the data.
the United States. The final draft of the Privacy Shield, which was adopted by the Commission on 11 July 2016 by majority vote of the Member States, includes privacy principles that stipulate improved data protection requirements compared with the safe harbour with which US companies must comply if they want to be certified under the Shield. Following criticism of the first draft of the Privacy Shield, in a revised draft the Commission endeavoured to assuage, in particular, the concerns expressed recently by the Article 29 Working Party, the independent advisory body on data protection and privacy that comprises representatives from national data protection authorities in Europe.

On 12 July 2016, the Commission adopted the Privacy Shield Adequacy Decision, certifying that this measure ensures an adequate level of protection for the transfer of personal data in the US. On 16 September 2016, Digital Rights Ireland brought an action for annulment before the CJEU against the Commission's adequacy decision, challenging in particular the legality of the mass recording of personal data by US public authorities, which remains possible under the Shield. On 22 November 2017, the General Court dismissed as inadmissible the action brought by Digital Rights Ireland.

On 9 January 2018, the Commission issued a notice stating that, as of the date of the UK’s withdrawal from the European Union, the UK will be treated as a third country within the meaning of GDPR rules on the transfer of personal data. Accordingly, it will not be automatically granted the status of a safe third country.

The adoption of the GDPR also affects the ePrivacy Directive, which is lex specialis for the electronic communications sector. Given that most articles of the current ePrivacy Directive only apply to traditional telecoms companies but not to the growing number of OTT providers (that is, providers using the internet to deliver content), on 10 January 2017 the Commission presented a proposal for a ‘Regulation concerning the respect for private life and the protection of personal data in electronic communications’ (ePrivacy Regulation), aimed at replacing the ePrivacy Directive.

The proposed ePrivacy Regulation would apply not only to traditional telecom operators, but also to OTT service providers (such as Whatsapp, Facebook and Skype) that currently do not fall within the scope of the ePrivacy Directive. It would also apply to non-EU operators that provide services to users located in the EU.

The new rules place great emphasis on end users’ consent. Service providers must obtain users’ consent to process electronic communications content and metadata, such as data on the location of where a phone call was made. The Regulation would introduce more user-friendly methods to obtain such consent (e.g., appropriate settings of a browser or other application). The proposed Regulation also addresses the privacy concerns raised by tools that allow tracking of the online activities of users, such as cookies, by requiring a clear affirmative action to express consent to their use.

In April 2017, the Article 29 Working Party and the European Data Protection Supervisor released their opinion on the proposal, advocating for more effective rules, such as a general prohibition on tracking practices and privacy by default settings for software and applications.

In its Communication of 15 May 2018 the Commission called on the co-legislators to conclude negotiations by the end of 2018, but discussions are still ongoing.

**Cybersecurity**

On 6 July 2016, the Parliament and the Council approved the Network and Information Security (NIS) Directive,\(^55\) also known as the Cybersecurity Directive, which was developed within the framework of the Commission’s EU Cybersecurity Strategy.\(^56\) The Directive aims to ensure a high common level of network and information security across the EU through a set of wide-ranging measures that will generate cooperation and information-sharing mechanisms, and set minimum requirements for a broad range of public and private players.\(^57\)

In January 2018, the Commission adopted an implementing regulation laying down rules for the application of the NIS Directive.\(^58\)

On 13 September 2017, the Commission and the High Representative for Foreign Affairs and Security Policy launched the cybersecurity package, a set of measures aimed at improving the EU response to cyberattacks and crime, which includes proposals for the institution of the European Cybersecurity Agency and for a directive on the combatting of fraud and counterfeiting of non-cash means of payment.\(^59\)

On 27 June 2019, Regulation (EU) No. 2019/881 on ENISA (the European Union Agency for Network and Information Security, also known as the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (the Cybersecurity Act) entered into force.

**Free flow of data and cloud computing**

The DSM Strategy calls for a European free flow of data initiative to promote the free movement of data and encourage innovation in the EU, while protecting personal data.\(^60\)

In April 2016, the Commission launched the European Cloud Initiative,\(^61\) which includes a series of initiatives concerning the certification of cloud services to allow users to benefit from secure and high-quality services, the switching of cloud service providers and the development of a European Open Science Cloud for European researchers. The Cloud Initiative also provides for the creation of a European data infrastructure. On 16 February 2017, the European Parliament adopted by a large majority a resolution on the European Cloud Initiative.

---

This is considered a key initiative, as estimates of the cost of an incomplete DSM for cloud computing are between €31.5 billion and €63 billion per year. On the other hand, it was estimated that cloud computing can potentially contribute a total of €450 billion to the EU’s GDP between 2015 and 2020 and lead to the creation of an additional one million jobs and 300,000 companies in the EU throughout all sectors of the economy.

On 11 January 2018, the Commission published its proposal for a regulation establishing the European High Performance Computing Joint Undertaking, a legal entity that would pool European resources to develop supercomputing infrastructure for European scientific and industrial users. At the moment, the top 10 supercomputers depend on non-European technology, and this creates risks for the EU in terms of competitiveness and innovation. Located in Luxembourg, the joint undertaking started operating in November 2018 and will remain operational until the end of 2026.

On 10 January 2017, the Commission adopted a communication on building a European data economy, aimed at identifying unjustified restrictions on the free movement of data, such as data location restrictions. On 14 November 2018, the Parliament and the Council adopted Regulation (EU) No. 2018/1807 on the free flow of non-personal data in the European Union (FFD Regulation; see Section VI).

On 29 May 2019, the European Commission published new guidance to help users (in particular small and medium-sized enterprises) understand the interaction between the FFD Regulation and the GDPR Regulation. It gives practical examples on how the rules should be applied when a business is processing datasets composed of both personal and non-personal data.

**IV SPECTRUM POLICY**

The DSM strategy considers a European spectrum policy to be necessary to boost investment, as some countries were slow in allocating the 800MHz band used for mobile communications, and lagged behind in rolling out 4G technology for mobile networks as a result. On the other side, some Member States have already outpaced EU regulation (e.g., Germany started auctioning spectrum from the 700MHz band for mobiles in May 2015 and on 2 October 2018 Italy awarded the auction for the same band).

On 9 June 2015, the Commission presented the outcome of a public consultation on the September 2014 Pascal Lamy report concerning the UHF band. The report discusses how the scarce spectrum resource in the UHF broadcasting band should be used in future. The results of the consultation suggest that there is general backing for spectrum-efficient technologies for DTTV equipment.

---

63 The International Data Corporation, Uptake of Cloud in Europe: Follow-up of IDC Study on Quantitative estimates of the demand for Cloud Computing in Europe and the likely barriers to take-up, 2015.
Accordingly, on 2 February 2016 the Commission presented a proposal for a Decision of the Parliament and the Council on the use of the 470–790MHz frequency band for mobile services in the EU. 69

On 17 May 2017, the Parliament and the Council adopted such decision, 70 stating that Member States have to allow the use of the 700MHz frequency for wireless broadband ECS by 30 June 2020.

On 23 October 2017, the Commission published a study on spectrum assignment for the deployment of 5G in the EU, 71 which considers the approaches currently used across the Member States for authorising and assigning spectrum. The study suggests that longer licence durations attract larger investments and a wider network roll-out.

The EECC establishes measures aimed at improving spectrum management across the EU. This objective is targeted by giving preference to the use of radio spectrum under general rather than individual authorisations (Article 48), and by granting long-term licences to encourage investment in high-capacity networks. In fact, the EECC obliges EU Member States to ensure that radio spectrum holder rights are valid for at least 15 years with a possibility for extension (Article 49).

The EECC also establishes that Member States shall cooperate to coordinate the timing of assignment of spectrum bands for electronic communications networks and services (Article 53).

In order to facilitate market entry by new operators, the EECC implements the ‘use it or lose it principle’ with respect to withdrawal of radio spectrum licences.

V MEDIA

The new AVMS Directive entered into force in December 2018. 72 Taking into account the changes occurred in the media landscape in less than a decade and the increase of video on-demand (VOD) services, the Directive changes the definition of audiovisual media services (including for first-time video-sharing platforms) and introduces a uniform regulatory framework for TV broadcasters and VOD service providers.

It strengthens the country-of-origin principle, according to which providers only need to abide by the rules of the Member State with jurisdiction over them, by providing more clarity on which Member States’ rules apply and by aligning derogation procedures for both TV broadcasters and on-demand service providers. TV and video-sharing platforms are now required to take appropriate measures to protect minors against harmful content and to

protect people from incitement to violence or hatred and public provocation to commit terrorist offences. Video-sharing platforms will now be responsible for reacting quickly when content is reported by users as harmful.

To support the cultural diversity of the European audiovisual sector, the Directive establishes that 30 per cent of content, including in the VOD service providers’ catalogues, must be European. VOD platforms are also required to contribute to the development of European audiovisual productions, either through direct investment in content or through contributions to national funds. The level of these contributions should be proportional to VOD service providers’ revenues in the country where they are established or in the country whose audience they target mostly.

Moreover, the Directive grants more flexibility in television advertising. Instead of the current 12 minutes per hour, broadcasters can choose when to show ads throughout the day, with an overall limit of 20 per cent of broadcasting time between 6am and 6pm and the same share during prime time (from 6pm to midnight).

The new Directive also includes strict rules on advertising and product placement in children’s programmes and content available on VOD platforms. Broadcasters are required to put in place measures to effectively reduce children’s exposure to publicity on unhealthy food or beverages. Product placement and teleshopping are prohibited in children’s programmes, while EU countries can decide autonomously whether to exclude sponsorship.

The integrity of the signal is guaranteed by a new set of rules. In the case of smart TVs, service providers are not allowed to add windows with content to the screen during a programme, without first obtaining the agreement of the broadcaster.

VI  THE YEAR IN REVIEW

i  The European Electronic Communications Code

The EECC, entered into force on 20 December 2018,° led to a complete review of the framework for electronic communications.

One of the main aims of the reform is to create incentives to invest, with a lighter regulatory regime particularly for co-investment of rival operators in very high capacity networks, and to facilitate the participation of smaller operators in investment projects.

On the basis of the principle of same service, same rules (which aims at creating a level playing field for all players providing similar services), the EECC broadens the scope of regulated ECS to include over-the-top (OTT) services. The category of ECS now includes: (1) internet access services, (2) interpersonal communications services (ICS), and (3) services consisting wholly or mainly in the conveyance of signals.

The inclusion of ICS represents a significant change in EU law: ICS are services that enable interpersonal and interactive exchange of information. They are further subdivided between ‘number-dependent’ and ‘number-independent’ services. The former includes traditional voice calls, the latter refers to all types of emails, messaging services or group chats. This means that OTT services such as Whatsapp, Facebook Messenger, Skype and Voice over Internet Protocol (VoIP) services now fall under the definition of ECS.

---

According to Recital 16, ECS provided in exchange for the provision of personal data or services in which users are exposed to advertising as a condition for gaining access are services provided in exchange for remuneration and, consequently, qualify as ECS under the EECC.

Pursuant to Article 68 of the EECC, undertakings with significant market power (SMP) may be subject to regulatory obligations imposed by NRAs, such as non-discrimination, accounting separation, access to civil engineering, price control and functional separation. In order to promote co-investment in a common infrastructure, pursuant to Article 76, undertakings having SMP can offer commitments to open to co-investment the deployment of a new very high capacity network. Co-investment may take the form of co-ownership or long-term risk sharing through co-financing.

Finally, the EECC contains provisions aimed at improving consumer rights. In particular, it provides that contracts with end users cannot extend beyond 24 months and consumers must receive a summary of the contract, as an integral part of the contract itself (Article 102).

ii The new Directive on copyright

Directive (EU) No. 2019/790 establishes the new set of European copyright rules. The objective of the Directive is to provide rules to adapt certain exceptions and limitations to copyright to digital and cross-border environments. The Directive also contains measures intended to facilitate licensing practices, in particular as regards the dissemination of out-of-commerce works and the online availability of audiovisual works on video-on-demand platforms, in order to ensure wider access to content.

Two provisions of the Directive are considered particularly innovative and controversial. Article 15 introduces the right of press publishers to claim remuneration for the online use of their publications (link tax). This means that platforms such as Google, Facebook and YouTube are required to agree on a fee to be paid to publishers and content owners. Article 17 imposes on online platforms an obligation to obtain an authorisation from right holders, for instance by entering into a licensing agreement, when they give the public access to copyright protected works uploaded by their users (upload filter). If no authorisation is granted, online platforms are liable for making copyright-protected works available to the public unless they demonstrate that they have (1) made best efforts to obtain an authorisation; (2) made best efforts to ensure the unavailability of specific works for which right holders have provided the necessary information; and (3) acted promptly, upon notice from the right holders, to disable access to the notified copyright-protected work.

The Directive establishes four mandatory exceptions to copyright for the purposes of education, research, preservation of cultural heritage and inclusion of disabled people.

iii Regulation on the free flow of non-personal data

Regulation (EU) No. 2018/1807 aims to achieve a more competitive and integrated internal market for data storage and other processing services so as to unlock the potential of new digital technologies (e.g., cloud computing, big data, artificial intelligence and the IoT).
The Regulation favours the circulation of non-personal data within the EU for companies, public administrations and citizens, allowing non-personal data to be located and processed anywhere in the EU without unjustified restrictions (with the exception of data retained for purposes of public security).

The Regulation abolishes the obligations of territorial restriction of data treatment, meaning the condition requiring that the treatment of data has to be carried out in a Member State rather than in another. However, the Regulation ensures that competent authorities can access data stored or processed in another Member State for the purposes of regulatory control.

Finally, the Regulation encourages market operators to develop self-regulatory codes of conduct containing information operational requirements to facilitate the switching of service providers and the porting of data.

iv  Merger and antitrust control in telecommunication markets
As regards merger control, the Commission cleared a relevant number of mergers in the telecommunications sector between the end of 2018 and October 2019.

In October 2018, the Commission cleared unconditionally the acquisition of Com Hem by Tele2. Both operators provide telecommunications services in Sweden. Even though both companies are active in the provision of mobile telecommunications services, fixed internet access services and multiple play services, the Commission found that the transaction would raise no competition concerns because their activities are largely complementary: Com Hem’s is mainly active in fixed telecommunications and TV, while Tele2 is mainly active in mobile telecommunications. Moreover, the Commission found that the merged entity would continue to face significant competition from other players such as Telia and Telenor, both active on all retail telecommunications markets in Sweden, as well as Tre, active on the retail mobile telecommunications market.

In December 2018, the Commission approved the acquisition of United Group by BC Partners. United Group provides telecommunications and media services in South East Europe. BC Partners is a private equity firm, which controls Intelsat, a global provider of satellite communications services. The transaction gives rise to a vertical relationship between the satellite pay-TV activities of United Group in South East Europe, and the Europe-wide wholesale satellite activities of Intelsat. The Commission concluded that the proposed acquisition would raise no competition concerns because Intelsat does not have market power in the wholesale market of satellite capacity and United Group is only one of the many customers active in the market.

In July 2019, the Commission approved the acquisition of DNA, a company providing mobile and fixed communications services, broadband internet services and TV distribution services in Finland, by Telenor ASA, which provides mobile and fixed telecommunications services and TV distribution services in the Nordic region. The Commission found that there are very limited horizontal overlaps between the companies’ activities in the market for retail TV services in Finland and in the wholesale market for acquisition of TV channels. In addition, the Commission considered that a number of strong players would remain in each of the markets after the merger.

75 Case M.8842, Tele2/Com Hem Holding.
76 Case M.9152, BC Partners/ United Group.
77 Case M.9379, Telenor/DNA.
In July 2019, the Commission approved, subject to commitments, the acquisition by Vodafone of Liberty Global’s cable business providing TV, broadband and phone services in the Czech Republic, Germany, Hungary and Romania. Following its Phase I investigation, the Commission had concerns that, in Germany, the transaction: (1) would eliminate the competitive constraint exerted by the merging companies on each other in the market for the retail supply of fixed broadband services, and (2) would increase the market power of the merged entity in the market for the wholesale supply of signal for the transmission of TV channels. The Commission considered that this could impact on the broadcasters’ position, leading to quality degradation of the TV offer in Germany and hindering the broadcasters’ ability to provide innovative services, such as OTT services.

To address the Commission’s competition concerns, Vodafone committed, inter alia, to: (1) provide a remedy taker (Telefónica) with access to the merged entity’s cable network in Germany, enabling the remedy taker to replicate the competitive constraint previously exerted by Vodafone; (2) refrain from contractually restricting the possibility for broadcasters that are carried on the merged entity’s TV platform to also distribute their content via an OTT service; and (3) not to increase the fees paid by free-to-air broadcasters for the transmission of their linear TV channels via Vodafone’s cable network in Germany.

In the media sector, in May 2019 the Commission opened an in-depth investigation to assess the proposed acquisition of Bonnier Broadcasting, a TV broadcasting company active primarily in Sweden and Finland, by Telia Company AB, a telecommunication operator that provide mobile and fixed telecommunications services as well as television services, among others, in Norway and Sweden.

As a retail TV distributor, Telia Company licenses TV channels from TV broadcasters, such as Bonnier Broadcasting, to include them in its audiovisual offering. The proposed acquisition would therefore create a vertically integrated player in the audiovisual sector in Denmark, Finland, Norway, and Sweden. The Commission’s competition concerns relate to the fact that: (1) Telia Company’s competitors in TV distribution could be denied access to Bonnier Broadcasting’s TV channels that are extremely important for consumers in Sweden and Finland; (2) the merged entity could deny access to TV advertising space on its free-to-air and basic pay TV channels to Telia Company’s competitors in the markets for retail mobile telecommunication, fixed internet and TV services; and (3) the merged entity could deny access to its streaming application to customers using competing mobile and fixed internet providers. The case is currently pending.

In September 2019, the Commission cleared the acquisition of M7 Group, based in Luxembourg, by Canal +, controlled by the Bolloré Group and based in France. M7 Group is active in certain countries of the European Economic Area in the provision of retail pay television services, the broadcasting of television channels and the wholesale distribution of television channels. Canal + is active in the provision of pay-TV retail services in several countries worldwide (including France and Poland in the EEA), audiovisual content production and TV broadcasting. The Commission concluded that the proposed merger would not raise competition concerns, as there is limited overlap between the parties’ activities.

---

78 Case M.8864, Vodafone/Certain Liberty Global Assets.
79 Case M.9064, Telia Company/Bonnier Broadcasting Holding.
80 Case M.9416, Bolloré Group / M7 Group.
As to antitrust enforcement, in March 2019 the Commission concluded the proceedings initiated against Google concerning the AdSense search advertising service, imposing a fine of €1.49 billion for abusive practices in online advertising.⁸¹

The Commission found that Google had abused its dominant position in the market for the brokering of online search adverts by imposing a number of restrictive clauses in contracts with third-party websites, which prevented Google's rivals from placing their search adverts on these websites.

In particular, the Commission maintained that, starting in 2006, Google included exclusivity clauses in its contracts for the provision of online search advertising intermediation services with publishers. On the basis of such clauses, publishers were allegedly prohibited from placing any search adverts from competitors on their search results pages. As of March 2009, Google gradually started replacing the exclusivity clauses with ‘premium placement’ clauses. These allegedly required publishers to reserve the most profitable space on their search results pages for Google’s adverts. As a result, the Commission considered that Google's competitors were prevented from placing their search adverts in the most visible and clicked on parts of the websites’ search results pages. As of March 2009, Google also included clauses allegedly requiring publishers to seek written approval from Google before making changes to the way in which any rival adverts were displayed. According to the Commission, this meant that Google could control how attractive, and therefore clicked on, competing search adverts could be (‘relaxed exclusivity’ strategy).

The Commission maintained that Google’s rivals were not able to compete on the merits, either because there was a prohibition for them to appear on publishers’ websites or because Google reserved for itself the most valuable commercial spaces on those websites, while at the same time controlling how rival search adverts could appear.

In March 2019, the Commission accepted the commitments offered by Disney, NBCUniversal, Sony Pictures, Warner Bros and Sky with regard to certain clauses contained in these studios’ film licensing contracts for pay-TV with Sky UK.⁸²

US film studios typically license audiovisual content to a single pay-TV broadcaster in each Member State. The contracts signed by these studios with Sky UK allegedly contained clauses that (1) required Sky UK to block access to the studios’ films through its online pay-TV services or its satellite pay-TV services to consumers outside UK and Ireland (geo-blocking), or both, and (2) required some of the studios to ensure that broadcasters outside the UK and Ireland were prevented from making their pay-TV services available in the UK and Ireland.

According to the Commission, such clauses restrict the ability of broadcasters to accept unsolicited requests (‘passive sales’) for their pay-TV services from consumers located outside their licensed territory. The Commission had concerns that this may eliminate cross-border competition between pay-TV broadcasters and partition the EU’s Single Market along national borders.

The Commission accepted the commitments consisting in, inter alia, not introducing contractual obligations that: (1) prevent pay-TV broadcasters from engaging in cross-border passive sales to consumers located outside the licensed territory (no ‘broadcaster obligation’), and (2) require the studios to prevent other pay-TV broadcasters from engaging in passive sales to consumers located in the licensed territory (no ‘studio obligation’).

---

⁸¹ Case 40411, Google AdSense.
⁸² Case AT.40023, Cross-border access to pay-TV.
VII CONCLUSIONS AND OUTLOOK

The new EECC, which entered into force on 20 December 2018, is meant to shape the future structure of the European telecommunications sector. The reform aims, inter alia, to boost the rollout of 5G networks, given that Europe is lagging behind Asia and America in this regard, and to create a level playing field between traditional telecommunications companies and OTT providers.

Antitrust enforcement in the past year confirmed the Commission’s focus on investigating possible anticompetitive practices implemented by large companies active in high-tech markets.

Under the political guidelines for the new European Commission 2019–2024, the development of artificial intelligence remains a priority area for further action in the years to come, to be developed by prioritising investments in this field and proposing a legislation for a coordinated European approach on its human and ethical implications.

---

Chapter 7

FRANCE

Myria Saarinen and Jean-Luc Juhan

I OVERVIEW

The French regulatory framework is based on the historical distinction between telecoms and postal activities on the one hand, and radio and television activities on the other (sectors are still governed by separate legislation and by separate regulators). Amendments in the past 15 years reflect the progress and the convergence of electronic communications, media and technologies, and the liberalisation of the TMT sectors caused by the de facto competition between fixed telephony (a monopoly until 1998) and new technologies of terrestrial, satellite and internet networks. French law also mirrors the EU regulatory framework through the enactment of the three EU Telecoms Packages in 1996, 2002 and 2009, which have been transposed into French law.

The TMT sectors in France have been fully open to competition since 1 January 1998, and are characterised by the interactions of mandatory provisions originating from many sources and involving many actors (regulators, telecoms operators, and local, regional and national authorities). The TMT sectors are key to the French economy, and 2018 was once again an important year in many respects for these sectors’ business.

II REGULATION

i The regulators

There are four specialist authorities involved in the regulation of technology, media and telecommunications in France:

a ARCEP is an independent government agency that oversees the electronic communications and postal services sector. It ensures the implementation of a universal service, imposes requirements upon operators that exert a significant influence in the context of market analyses, participates in defining the regulatory framework, allocates finite resources (RFs and numbers), imposes sanctions, resolves disputes and delivers authorisations for postal activities.

b The Superior Audiovisual Council (CSA) is the regulatory authority responsible for the audiovisual sector. The CSA sets rules on broadcasting content and allocates frequencies by granting licences to radio and television operators. It also settles disputes that may arise between TV channels and their distributors, and is empowered to impose sanctions on operators in cases of breaches of specific regulations. Law

---

1 Myria Saarinen and Jean-Luc Juhan are partners at Latham & Watkins. This chapter was written with contributions from associates Lea Margono and Camille Dorval.

© 2019 Law Business Research Ltd
No. 2013-1028 of 15 November 2013 relating to the independence of the French public broadcasting service has amended the legal nature of the CSA, its composition, the status and appointment procedure of its members and their powers.

c The High Authority for the Distribution of Works and the Protection of Copyright on the Internet (HADOPI), which was established in 2009, is in charge of protecting intellectual property rights over works of art and literature on the internet. The upcoming audiovisual reform to be implemented by early 2020 under French law will bring a significant change with the merger of the CSA with the HADOPI, which will be named the Authority of Regulation of Audiovisual and Digital Communication (ARCOM).

d The Data Protection Authority (CNIL) supervises compliance with data protection regulations, and is empowered to issue sanctions that range from warnings to fines up to €20 million or 4 per cent of total global annual turnover of the group of the preceding financial year, whichever is higher.

These authorities may deliver opinions upon request by the government, Parliament or other independent administrative authorities such as the French Competition Authority (FCA), and also renders decisions and opinions that may have a structural impact on these sectors (except for HADOPI). The National Frequencies Agency is also an important agency responsible for managing frequency spectrum and planning its use (see Section IV).

The CSA and ARCEP are the two main regulators of the TMT sectors. Discussions about merging these entities at the time of the convergence or to limit the powers of ARCEP occurred regularly during the past few years, but such merger was finally given up. Instead, it was argued that the two regulators should work in closer cooperation on certain common subjects.

ii Main sources of law

The prevailing regulatory regime in France regarding electronic communications is contained primarily in the Post and Electronic Communications Code (CPCE), and regarding audiovisual communications in Law No. 86-1067 of 30 September 1986 on Freedom to Communicate, as subsequently amended.

The main piece of legislation governing the law applicable to data protection is the GDPR\(^2\) and Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (1978 Data Protection Law), as subsequently amended, which supplements or derogates to the GDPR.

Intellectual property rights are governed by the Intellectual Property Code.

iii Regulated activities

Telecoms

Telecoms activities and related authorisations and licences are regulated under the CPCE.

To become a telecoms operator, no specific licences or authorisations are required; the implementation and the operation of public networks and the supply of electronic

---

\(^2\) Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
communication services to the public is free, subject to prior notification to ARCEP (Articles L32-1 and L33-1 of the CPCE). Law No. 2015-990 of 6 August 2015 for the growth, activity and equality of economic opportunities (also known as the Macron Law) grants ARCEP the power to register on its own initiative any actor that infringed the notification obligation to declare itself to ARCEP.³

Conversely, the use of RFs requires a licence granted by ARCEP (Article L42-1 of the CPCE).

### Media

Authorisations and licensing in the media sector are regulated under Law No. 86-1067 of 30 September 1986.

Authorisations for private television and radio broadcasting on the hertz-based terrestrial frequencies are granted by the CSA following bid tenders and subject to the conclusion of an agreement with the CSA. The term of authorisations cannot exceed 10 years.⁴ Broadcasting services that are not subject to the CSAs authorisation – namely, those that are broadcast or distributed through a network that does not use frequencies allocated by the CSA (cable, satellite, ADSL, internet, telephony, etc.) – are nevertheless subject to a standard agreement or a declaration regime.⁵

### iv Ownership and market access restrictions

#### General regulation of foreign investment

Since the entry into force of Law No. 2004-669 of 9 July 2004, discrimination of non-EU operators is prohibited, and they are subject to the same rights and obligations as EU and national operators.⁶ According to Article L151-1 et seq. of the French Monetary and Financial Code, when a foreign (EU or non-EU) investment is made in a strategic sector (such as security, public defence, cryptographics or interception of correspondence),⁷ the investor must submit a formal application dossier to the French Ministry of Economy for prior authorisation. Any transaction concluded without prior authorisation is null and void, and criminal sanctions (imprisonment of up to five years⁸ and a fine amounting to up to twice the amount of the transaction) are also applicable. A Decree of 14 May 2014⁹ expanded the list of sectors in which foreign investors must seek prior authorisation from the Ministry of Economy. In particular, the Decree has added to the regulated activities referred to in Article R153-2 of the French Monetary and Financial Code activities relating to the integrity, security and continuity of the operation of networks and ECSs.

---

³ Article L33-1 I of the CPCE.
⁴ See Articles 28 to 32 of the Law of 30 September 1986, which determine the CSA’s allocation procedures.
⁵ Articles 33 to 34-5 of the Law of 30 September 1986.
⁶ Article L33-1 III of the CPCE.
⁸ Article L165-1 of the French Monetary and Financial Code.
Specific ownership restrictions applicable to the media sector

French regulations provide for media ownership restrictions to preserve media pluralism and competition. In particular, any single individual or legal entity cannot hold, directly or indirectly, more than 49 per cent of the capital or the voting rights of a company that has an authorisation to provide a national terrestrial television service where the average audience for television services (either digital or analogue) exceeds 8 per cent. In addition, any single individual or legal entity that already holds a national terrestrial television service where the average audience for this service exceeds 8 per cent may not, directly or indirectly, hold more than 33 per cent of the capital or voting rights of a company that has an authorisation to provide a local terrestrial television service.10

Regulation of the media sector is currently evolving in reaction to a number of changes in French media ownership. As a consequence, French lawmakers adopted Law No. 2016-1524 of 14 November 2016, which amends the Law of 30 September 1986.11 Its purpose is to ensure freedom, independence and pluralism in media ownership, for example by requiring media outlets to provide yearly information on their capital ownership and governing bodies,12 and reinforcing the powers of the CSA over French media governance with the creation of deontology committees.13

Regarding the radio sector, a single person cannot retain networks whose coverage exceeds 150 million inhabitants or 20 per cent of the aggregated potential audience.14 This regulation will, however, be subject to modification in the future, as it does not take into account local pluralism challenges. In this respect, a report was submitted to Parliament by the CSA in April 2014.15

Further, unless otherwise agreed in international agreements to which France is a party, a foreign national may not acquire shares in a company holding a licence for a radio or television service in France that uses RFs if this acquisition has the effect of raising (directly or indirectly) the share of capital or voting rights owned by foreign nationals to more than 20 per cent.16 Under the same circumstances, such licence cannot be granted to a company in which 20 per cent of the share capital or voting rights is owned (directly or indirectly) by foreign nationals.17 These provisions do not apply to service providers of which at least 80 per cent of the capital or voting rights are held by public radio broadcasters belonging to Council of Europe Member States, and of which at least 20 per cent is owned by one of the public companies mentioned in Article 44 of the Law of 30 September 1986.18 Specific rules restricting cross-media ownership also apply.19

---

11 Law No. 2016-1524 of 14 November 2016 strengthening media freedom, independence and pluralism.
19 Article 41-1 to 41-2-1 of the Law of 30 September 1986.
v Transfers of control and assignments

The general French merger control framework applies to the TMT sectors, without prejudice to the above-mentioned ownership restrictions and to specific provisions for the media sector. The merger control rules are enforced by the FCA.\textsuperscript{20}

Regarding the telecoms and post sectors, the FCA must provide ARCEP with any referrals regarding merger control, and ARCEP can issue a non-binding opinion.\textsuperscript{21}

Regarding companies active in the radio or TV sector involved in a Phase II merger control procedure before the FCA, a non-binding opinion from the CSA is necessary.\textsuperscript{22}

Any modification of the capital of companies authorised by the CSA to broadcast TV or radio services on a frequency is subject to the approval of the CSA.\textsuperscript{23}

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

Under the CPCE, ECSs other than voice telephony to the public may be provided freely.\textsuperscript{24}

As regards the ADSL network, and following local loop unbundling, alternative operators must be provided with direct access to the copper pair infrastructure of France Télécom-Orange, the historical operator. Therefore, as with traditional fixed telephony, DSL networks are subject to asymmetrical regulation.

As regards services, internet service providers (ISPs) can operate freely and provide services, but they must file a declaration with ARCEP before commencing operations.\textsuperscript{25} A failure to comply with this obligation constitutes a criminal offence.\textsuperscript{26}

More generally, ISPs must comply with the provisions of Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy governing e-commerce, encryption and liability of technical service providers, as subsequently amended. Law No. 2004-575 of 21 June 2004 also sets out a liability exemption regime for hosting service providers. They are not subject to a general obligation to monitor the information they transmit or store; nor are they obliged to look for facts or circumstances indicating illicit activity. Nevertheless, when the provider becomes aware that the content stored is obviously illicit, it has the obligation to remove such content or render its access impossible, otherwise it may be held liable for such content. In that respect, the question of the qualification as ‘host provider’ is still widely debated before French courts.\textsuperscript{27} The hosting provider’s neutrality or passivity criterion with

\textsuperscript{20} For recent examples of mergers in the TMT sectors, see, e.g., FCA, Decision No. 17-DCC-76 of 13 June 2017, in which the FCA ruled on the acquisition of Group News Participations by SFR Group.

\textsuperscript{21} Article L36-10 of the CPCE.

\textsuperscript{22} Article 41-4 of the Law of 30 September 1986.

\textsuperscript{23} Article 42-3 of the Law of 30 September 1986.

\textsuperscript{24} Article L32-1 of the CPCE.

\textsuperscript{25} Article L33-1 of the CPCE.

\textsuperscript{26} Article L39 of the CPCE.

\textsuperscript{27} This issue now seems resolved regarding video-sharing sites: see, for instance, the judgment of the French Supreme Court (Cass., Civ. 1ère, 17 February 2011, No. 09-67896, Joyeux Noël) in which the Supreme Court recognised a simple hosting status for Dailymotion. The Supreme Court ruled that host websites did not have to control \textit{a priori} the content they host but need to ensure that the content is not accessible once it has been reported as illegal (Cass., Civ. 1ère, 12 July 2012, No. 11-15165 and No. 11-15188, Google and Aufeminin.com). This issue is still to be debated with respect to online marketplaces such as eBay from which it follows that French courts, which are favouring a very factual analysis of the role of the services provider,
regard to the stored content is a major element in the qualification. The provider will benefit from the liability exemption regime for hosting service providers if its role is limited to a purely technical, neutral and passive service (e.g., structuring and classifying the content made available to the public to facilitate the use of its service). However, if it plays an active role providing it with knowledge or control of such content (e.g., determining or verifying the content published, broadcasted or uploaded), the provider will qualify as a website publisher. In this case, it would be fully liable for any unlawful or harmful content published, broadcast or uploaded on its website.

ii Universal service

The EU framework for universal services obligations, which defines universal services as the ‘minimum set of services of specified quality to which all end users have access, at an affordable price in the light of specific national conditions, without distorting competition’, has been implemented by Law No. 96-659 of 26 July 1996 and further strengthened by Law No. 2008-3 of 3 January 2008. Universal service is one of the three components of public service in the telecoms sector in France (the other two being the supply of mandatory services for electronic communications and general interest missions). Obligations of the operator in charge of universal service are listed in Article L35-1 of the CPCE and fall into two main categories of services:

a telephone services: connection to an affordable public telephone network enabling end users to take charge of voice communications, facsimile communications and data communications at data rates that are sufficient to allow functional internet access and free emergency calls; and

b enquiry and directory services (either in printed or electronic versions).

These services must be rendered under tariff and technical conditions that take into consideration the difficulties faced by some users, such as users with low incomes, and that do not discriminate between users on the ground of their geographical location. Following
calls for applications (one per category), the Minister in charge of electronic communications designates the operator or operators in charge of the universal service for a period of three years. France Télécom-Orange was designated as such until 2020.  

Universal service currently only covers telephone provision and not information technologies.

ARCEP determines the cost of the universal service and, when it is necessary to finance it in the event that it represents an excessive burden for the operator in charge, ARCEP also determines the amount of the other operators’ contributions to the financing of USOs through a sectoral fund. In principle, every operator contributes to the financing, with each contribution being calculated on the basis of the turnover achieved by the operators in their electronic communications activities.  

### Restrictions on the provision of service

Net neutrality is a growing policy concern in France. From the electronic communications regulator’s standpoint, which focuses on the technical and economic conditions of traffic conveyance on the internet, the key question in the debate over net neutrality is how much control internet stakeholders can rightfully exert over the traffic. This implies examining operators’ practices on their networks, as well as their relationships with some content and application providers.

The Digital Republic Law\(^\text{32}\) recently introduced the principle of net neutrality into the national legal framework and grants ARCEP with new investigatory and sanctioning powers to ensure compliance (see also Section VI.i).\(^\text{33}\) In particular, Arcep is now in charge of implementing net neutrality in accordance with Regulation No. 2015/2120 of 25 November 2015 establishing measures concerning open internet access.\(^\text{34}\) When Arcep identifies a risk of infringement by an operator, it can require said operator to comply ahead of time. The Digital Republic Law also reinforces the conditions under which the Minister in charge of electronic communications and Arcep can conduct an investigation.\(^\text{35}\)

Since the adoption of the Digital Republic Law, ARCEP has published a courtesy French translation of the guidelines for national regulatory authorities on the implementation of Regulation No. 2015/2120 of 25 November 2015, which the Body of European Regulators for Electronic Communications published on 30 August 2016.\(^\text{36}\) In June 2018, for a second year, ARCEP also published its annual report on the state of the internet in France,\(^\text{37}\) which identifies various threats that could undermine the internet’s proper functioning and neutrality, and sets out the regulator’s actions to contain these threats. This document

---

30 See Ministerial Order of 27 November 2017 designating Orange (JORF No. 0282 of 3 December 2017).
31 Article L35-3 of the CPCE.
32 Law No. 2016-1321 of 7 October 2016 for a Digital Republic.
33 Articles 40 to 47 of Digital Republic Law.
34 Article 40 of Digital Republic Law.
35 Article 43 of Digital Republic Law.
addresses issues regarding data interconnection, the transition to IPv6, the quality of fixed internet access, net neutrality and open platforms. Arcep issued in parallel a report devoted to the ways in which end user devices (mobiles and boxes) influence internet openness.

As to content, pursuant to the Law of 21 June 2004, ISPs have a purely technical role, and they do not have the general obligation to review the content they transmit or store. Nevertheless, when informed of unlawful information or activity, they must take prompt action to withdraw the relevant content, failing which their civil liability may be sought. Since 2009, HADOPI has been competent to address theft and piracy matters. It intervenes when requested to by regularly constituted bodies for professional defence that are entitled to institute legal proceedings to defend the interests entrusted to them under their statutes (e.g., SACEM), or by the public prosecutor. After several formal notices to an offender, the procedure may result in a €1,500 fine.

Finally, French e-consumers benefit from consumer law provisions and from specific regulations. In particular, they are protected against certain unsolicited communications via email if their consent has not been obtained prior to the use of their personal data. Moreover, consumers must be provided with valid means by which they may effectively request that such unsolicited communications cease. In addition, Article L223-1 of the French Consumer Code provides for the implementation of an opposition list on which any consumer can add his or her name so that advertising material may not generally be sent to him or her. With regard to phone-based advertising, the Bloctel service has been implemented since 1 June 2016 to prevent unsolicited communications to consumers registered on an opposition list. The Bloctel service had over 2 million registered users two months after its launch. All telephone operators also have the obligation to offer their users the possibility to register on an opposition list.

iv Privacy and data security
The past few years have seen increasing terrorist security threats, resulting in substantial changes in the legal framework regarding security in telecommunications.

Law No. 91-646 of 10 July 1991 concerning the secrecy of electronic communications, now codified in the Internal Security Code, provides that the Prime Minister may exceptionally authorise, for a maximum period of four months (renewable only upon a new decision), the interception of electronic communications in order to collect information relating to the defence of the nation or the safeguarding of elements that are key to France’s scientific or

---

38 IPv6 is the most recent version of the Internet Protocol, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the internet. IPv6 has been developed to deal with the issue of IPv4 address exhaustion, and is intended to replace IPv4.
41 See Article L34-5 of the CPCE.
42 See Article L34-5 of the CPCE.
43 See www.bloctel.gouv.fr.
44 See Ministerial Order of 25 February 2016 designating SA Opposetel (JORF No. 0050 of 28 February 2016).
45 The red list service ensures that contact information will not be mentioned on user lists. The orange list service ensures that contact information will not be communicated to corporate entities with the goal of advertisement. The contact information remains available on universal directories made available to the public.
economic capacity. In addition, pursuant to Law No. 2015-912 of 24 July 2015 (new Article L851-3 of the Internal Security Code) and only for the purpose of preventing terrorism, the Prime Minister may impose on providers of electronic communication services the obligation to implement an automated data-processing system for a maximum period of two months (renewable only upon a new decision) with the aim of detecting connections likely to reveal a terrorist threat. Article L851-2 of the Internal Security Code as amended by Law No. 2016-987 of 21 July 2016 provides that the administration is authorised, for prevention of terrorism, to collect real time connection data concerning individuals, beforehand identified, likely to be linked to a terrorist threat.46

Further, Law No. 2013-1168 on Military Programming (LPM) introduced a new chapter in the Internal Security Code relating to administrative access to data connection, including real-time geolocation.47 The new regime, which entered into force on 1 January 2015,48 authorises the collection of ‘information or documents’ from operators as opposed to the collection of simply ‘technical data’. In addition, access to data is exclusively administrative, namely without judicial control. Requests for implementing such measures are submitted by designated administrative agents to a ‘chosen personality’ appointed by the National Commission for the Control of Security Interceptions (CNCIS) upon the proposal of the Prime Minister. CNCIS is in charge of controlling (a posteriori) administrative agents’ requests for using geolocation measures in the course of their investigation. The Minister for Internal Security, the Defence Minister and the Finance Minister can also issue direct requests for the implementation of real-time geolocation measures to the Prime Minister who, in this case, will directly grant authorisations.

Law No. 2014-1353 of 13 November 2014, implemented by Decree No. 2015-174 of 13 February 2015, also entitles the administrative authorities to request ISPs to prevent access to websites supporting terrorist ideologies or projects.49 Additionally, laws linked to the state of emergency created extraordinary means of data search and seizure and expanded the provisions of Law No. 2014-1353.

In the context of the terrorism threat, the French legislator has amended the Criminal Proceedings Code to tackle organised crimes such as terrorism acts.50 Law No. 2016-731 of 3 June 201651 allows police officers, with the authorisation and under the control of a judge, to access, remotely and without consent, the correspondences stored in electronic

---

46 Initially, this article provided that the collection could be authorised against the individual's relatives. However, the Constitutional Council, in decision No. 2017-648 QPC of 4 August 2017, censored this provision because it infringes the balance between public security and right to privacy.

47 New Article L246-1 et seq. of the Internal Security Code introduced by Article 20 of the LPM.

48 Article 20 IV of the LPM.


50 However, the Constitutional Council established boundaries in the fight against terrorism regarding infringements of the freedom of communication. In Decision No. 2016-611 QPC of 10 February 2017, the Council considered as unconstitutional Article 421-2-5-2 of the French Criminal Code introduced by Law No. 2016-731 of 3 June 2016, which punishes any person who frequently accesses online public communication services conveying messages, images or representations that directly encourage the commission of terrorist acts or defend these acts when this service has the purpose of showing images or representations of these acts that consist of voluntary harm to life.

51 Law No. 2016-731 of 3 June 2016 reinforcing the fight against organised crime and terrorism and their funding, and improving the efficiency and the protection of guarantees of criminal proceedings.
communications available through identification. Police officers can also be authorised, by a judge and under his or her control, to use a technical disposal, such as an international mobile subscriber identity-catcher, to collect technical connection data to identify terminal equipment or users’ subscription numbers as well as data regarding the location of the terminal equipment used. This Law also extended some existing investigating powers to all organised crimes, such as the real-time collection of computer data without consent, in the context of both preliminary investigations and investigations of flagrancy.

In addition to the general rules applicable to the protection of personal data laid down in the 1978 Data Protection Law, the CPCE provides specific rules pursuant to which operators must delete or preserve the anonymity of any traffic data relating to a communication as soon as it is complete. Exceptions are provided, however, in particular for the prevention of terrorism and in the pursuit of criminal offences.

Unauthorised access to automated data-processing systems is prohibited by Articles 323-1 to 323-7 of the French Penal Code. In addition, with regard to cyberattacks, Law No. 2011-267 on Performance Guidance for the Police and Security Services (LOPPSI 2) introduced a new offence of online identity theft in Article 226-4-1 of the French Penal Code and empowers police officers, upon judicial authorisation and only for a limited period, to install software in order to observe, collect, record, save and transmit all the content displayed on a computer’s screen. This helps with the detection of infringements, the collection of evidence and the search for criminals by facilitating the creation of police files and by organising their coordination. Cybersecurity threats are dealt by the National Agency for the Security of Information Systems (ANSSI), a branch of the Secretariat-General for Defence and National Security created in 2009.

In terms of personal data protection, obligations were reinforced with the entry into application of the GDPR. The CNIL published in 2018 a new guide on the security of personal data, recalling basic precautions to be implemented systematically and providing risk management methodologies. Moreover, LOPPSI 2 increases the instances where authorities may set up, transfer and record images on public roads, premises or facilities open to the public in order to protect the rights and freedom of individuals, and recognises that the CNIL has jurisdiction over the control of video protection systems.

With regard to the detection of cyberattacks, Law No. 2018-607 of 13 July 2018 created Article L33-14 of the CPCE that involves operators in the detection of cyberattacks. Pursuant to this article, electronic communications operators are entitled to use technical

55 See Articles L34-1 and D98-5 of the CPCE.
57 See Article 32 of the GDPR.
markers such as IP addresses to detect or prevent any potential threat that may affect the security of information systems of their subscribers. In this case, operators shall inform the ANSSI without delay.

With regard to the protection of children online, Article 45 of the 1978 Data Protection Law requires that clear information be provided to minors, using terms that are adapted to their age. Adequate vigilance and warning systems shall also be implemented (e.g., awareness messages, age gates with reliable controls, possibility of parental supervision, etc.). Regarding consent, specific rules apply in France. The age of a child’s consent in relation to the offer of information society services is 15 years old (whereas it is, by default, 16 years old under Article 8 of the GDPR). Children under 15 years old may only give their consent after being duly authorised to do so by the holder of parental rights. The lawfulness of the processing activity, therefore, requires a double consent: that of the minor as well as that of the holder of parental rights.62

The implementation of the Network and Information Security Directive

With regard to cybersecurity, the Network and Information Security Directive (NISD)63 has been implemented into French law by Law No. 2018-133 of 26 February 2018 and Decree No. 2018-384 of 23 May 2018. This framework imposes an obligation in terms of security of network and information systems on two categories of entities: (1) the operators of essential services (OESs) and (2) digital service providers (DSPs).

The categories of services considered as essential services are listed in the appendix of Decree No. 2018-384 (e.g., payment services, insurance, services involving preventive medicine, diagnosis and healthcare, selling of electricity and gas). The Prime Minister can designate operators as an OES if they provide at least one of the services listed.64 The operator is notified of the Prime Minister’s intent to designate it as an OES and can formulate observations.65 The first designations are expected in November 2018.

DSPs are providers of cloud, online marketplace and search engine services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.66 Nevertheless, the French implementing law excludes from its scope certain types of entities already subject to information system security regulations, such as operators for their activities related to the operation of ECNs or the provision of ECSs and providers of trust services for electronic transactions subject to Article 19 of Regulation 910/2014 dated 23 July 2014.67

Both OESs and DSPs shall appoint a representative in charge of the contact with the ANSSI.68 For DSPs, this representative acts in the name of the provider for compliance with

---

62 Article 45 of the 1978 Data Protection Law.
its obligations set forth of the NSID framework. DSPs shall keep an updated list of all networks and information systems necessary for the provision of their services within the European Union.

As regards security measures that should be implemented, OESs shall comply with security measures defined by the Prime Minister in a specific regulation (which has not been adopted to date). DSPs shall ensure, based on the state of art, a level of security for all networks and information systems necessary for the provision of their services within the European Union appropriate to the existing risks. DSPs shall refer to Article 2 of the Commission Implementing Regulation of 30 January 2018 for the security measures that should be implemented. Documents attesting to this implementation should be made available to the ANSSI in case of control.

Both OESs and DSPs shall report to the ANSSI, without delay, after becoming aware of any incident affecting networks and information systems that has or is likely to have a significant impact on the continuity of services.

Non-compliance with the obligations set forth in the NSID framework may be sanctioned with criminal fines ranging from €100,000 to €125,000 for OESs and from €75,000 to €100,000 for DSPs.

IV SPECTRUM POLICY

i Development
The management of the entire French RF spectrum is entrusted to a state agency, the National Frequencies Agency. It apportions the available radio spectrum, the allocation of which is administered by governmental administrations (e.g., those of civil aviation, defence, space, the interior) and independent authorities (ARCEP and the CSA) (see Section II).

ii Flexible spectrum use
The trend towards greater flexibility in spectrum use is facilitated in France by the ability of operators to trade frequency licences, as introduced by Law No. 2004-669 of 9 July 2004. The general terms of spectrum licence trading are defined by Decree No. 2006-1016 of 11 August 2006, and the list of frequency bands the licences of which could be traded are laid down by a Ministerial Order of 11 August 2006. A frequency database that provides information regarding the terms for spectrum trading in the different frequency brands open in the secondary market is publicly accessible. A spectrum licence holder may transfer all of its rights and obligations to a third party for the entire remainder of the licence (full transfer).
or only a portion of its rights and obligations contained in the licence (e.g., geographical region or frequencies). The transfer of frequency licences is subject either to the prior approval of ARCEP or to notification to ARCEP, which may refuse the assignment under certain circumstances. Another option available for operators is spectrum leasing, whereby the licence holder makes frequencies fully or partially available for a third party to operate. Unlike in a sale, the original licence holder remains entirely responsible for complying with the obligations attached to the frequency licence. All frequency-leasing operations require the prior approval of ARCEP.

iii Broadband and next-generation mobile spectrum use

Spectrum in the 800MHz and 2.6GHz bands was allocated for the deployment of the ultra-high-speed 4G mobile network: in that respect, licences for the 2.6GHz frequency were awarded to Bouygues Telecom, Free Mobile, Orange France and SFR in September 2011, and in December 2011, licences for the 800MHz were awarded to the same operators except Free Mobile, which has instead been granted roaming rights in priority roll-out areas. New spectrum in the 700 and 800MHz bands was transferred in December 2015 to promote better network capacities in areas with low population density, but the transfer will only be made effective from October 2017 to June 2019. The French government launched a call for applications, to be sent before 2 October 2018, in order to reassign the 900MHz, 1,800MHz and 2.1GHz bands, whose authorisations will expire between 2021 and 2024. As a result of an agreement reached between ARCEP, the French government and operators on 14 January 2018, the reassignment procedure will take into account operators’ stated commitments to improve voice and data coverage in all territories, making regional development targets a priority.

On 16 June 2017, ARCEP had authorised Bouygues Telecom and SFR to deploy 4G networks in the 2.1GHz band, historically used by French mobile operators’ 3G networks, to improve 4G speeds.

Additionally, under ARCEP supervision, 5G deployment is being prepared, with network coverage estimated to begin in 2020. The European Union’s public–private partnership between the European Commission and telecom industries, the 5G-PPP, which was launched on 1 July 2015, provides a framework for national 5G development. On 30 September 2015, ARCEP gave Orange authorisation to conduct initial tests for 5G in the city of Belfort until the end of 2016. The authorisation delivered to Orange tests three formerly unused spectrum ranges, namely the 3,600–3,800MHz, 10,500–10,625MHz and 17,300–17,425MHz frequencies. ARCEP recently published a synopsis of the responses to its public consultation on ‘New frequencies for superfast access in the regions, for businesses, 5G and innovation’ launched on 6 January 2017. Following this consultation, ARCEP

---

79 Article R20-44-9-2 of the CPCE.
80 ibid.
81 ARCEP, Decision No. 2011-1080 of 22 September 2011.
82 ARCEP, Decision No. 2011-1510 of 22 December 2011.
83 See ARCEP press release of 2 August 2018.
84 ARCEP, Decisions No. 2017-0734 (Bouygues Telecom) and No. 2017-0735 (SFR) of 13 June 2017.
85 See ARCEP press release of 30 September 2015.
86 See ARCEP press release of 22 June 2017.
now seeks to prepare 5G deployment in the 26GHz and 1.5GHz bands. On 16 July 2018, the French government officially launched its 5G roadmap. Three main goals have been announced: (1) launching of several 5G pilot programmes in various regions; (2) allocation of new 5G frequencies and ensuring a commercial rollout in at least one major city by 2020; and (3) provision of 5G coverage for main transport routes by 2025. Additionally, four main working areas have been identified: (1) free-up and attribute RFs for the 5G network; (2) foster the development of new industrial uses; (3) accompany the deployment of 5G infrastructures; and (4) ensure transparency and dialogue on 5G deployments and the exposure of the public.

On 15 July 2019, ARCEP launched a public consultation in connection with its draft procedure for awarding licences to use frequencies in the 3,490–3,800MHz band. The contributions to this public consultation will enable ARCEP to finalise the procedure and the terms of allocation. The aim is to allocate frequencies in the autumn of 2019.

iv Spectrum auctions and fees

Spectrum auctions in the case of scarce resources

Pursuant to Article L42-2 of the CPCE, when scarce resources such as RF are at stake, ARCEP may decide to limit the number of licences, either through a call for applications or by auction. The government sets the terms and conditions governing these licensing selection procedures, and until now such proceedings have always been in the form of calls for applications.

Fees

Pursuant to Articles R20-31 to R20-44 of the CPCE, licensed operators contribute to the financing of the universal services.

V MEDIA

Media are, in particular, subject to certain content requirements and restrictions.

i Content requirements

At least 60 per cent of the audiovisual works and films broadcast by licensed television broadcasters must have been produced in the EU, and 40 per cent must have been produced originally in French.

Private radio broadcasters must, in principle, dedicate at least 40 per cent of their musical programmes to French music.  

---

87 See ARCEP press release of 30 July 2018.
89 See ARCEP Draft Decision of 15 July 2019 proposing the procedure for awarding the 3,490–3,800MHz band in Metropolitan France.
90 Articles 7 and 13 of Decree No. 90-66 of 17 January 1990.
In addition, pursuant to Law No. 2014-873 of 4 August 2014 for genuine equality between women and men, audiovisual programmes have the duty to ensure fair representation of both women and men. Furthermore, audiovisual programmes and radio broadcasters must combat sexism by broadcasting specific programmes in this respect.92

Law No. 2018-1202 of 22 December 201893 with regard to ‘fake news’ suggests several measures to limit the impact of false information on the public election process. For instance, Article 11 of the Law provides that certain operators of online platforms – in the context of public elections – should implement measures to combat the broadcasting of false information likely to trouble public order or alter polls’ reliability. They should implement easily accessible and visible systems that will allow users to report such false information, including when they are financed by third parties.

Advertising
Advertising is particularly regulated in television broadcasting.94 In particular, advertising must not disrupt the integrity of a film or programme, and there must be at least 20 minutes between two advertising slots. Films may not be interrupted by advertising that lasts more than six minutes.

Rules governing advertisements are stricter on public channels. In particular, since 2009, advertising is banned on public service broadcasting channels from 8pm to 6am. This prohibition does not, however, concern general-interest messages, generic advertising (for the consumption of fruits, dairy products, etc.) or sponsorships, which may continue to be broadcast.

In addition, some products are prohibited from being advertised, such as alcoholic beverages above a certain level of alcohol or tobacco products.

A new decree, Decree No. 2017-159 dated 9 February 2017, extended the media owners’ transparency requirements in order to protect advertisers of digital advertisement. According to Article 2 of the Decree, the media owners have to provide advertisers with the date and place of diffusion of the advertisements; the global price of the advertising campaign; and the unitary price charged for each advertising space.

VI THE YEAR IN REVIEW

i The ‘blockchain’ legal framework
On 9 December 2017, the French government published Ordinance No. 2017-1674 relating to the use of the blockchain technology for the record of the issuance and assignment of certain securities.

Pursuant to Article L211-3 of the French Monetary and Financial Code, securities must be recorded in an account (compte-titres) kept by the issuer of the titles or an intermediary. As of 1 July 2018, blockchain technology should be accepted as a parallel form of records for all transactions involving securities that are not listed, provided that the issuer of the securities formally accepts the use of such technology.

93 Law No. 2018-1202 of 22 December 2018 regarding the fight against the manipulation of information.
The Decree of 24 December 2018 sets out the conditions applicable to this mechanism. The distributed ledgers used to register securities are required to comply with the four following technical conditions: (1) they must be ‘conceived and implemented’ in a manner that preserves the integrity of the information recorded; (2) they must allow ‘directly or indirectly’ the identification of the owners of the securities: it must be possible to determine the nature and quantity of the securities held through the distributed ledger; (3) they must set out a business continuity plan including an external data recording system; and (4) the owners of the securities registered on the distributed ledger must be able to access statements of transactions.

After the adoption of a specific tax regime for crypto-assets (flat tax and exemption of crypto-to-crypto transactions) in the Budget Act for 2019 and the clarification of the accounting treatment of crypto-assets and initial coin offerings (ICOs) by the French Accounting Rules Authority (ANC), another significant milestone has been reached with the entry into force of the Law Pacte in 24 May 2019, which establishes a framework for fundraising via the issuance of virtual tokens (ICOs) and digital assets services providers.

### ii The overhaul of the data protection law

A new data protection law was enacted on 20 June 2018 to adapt 1978 Data Protection Law to the GDPR and Directive (EU) 2016/680. Since then, the 1978 Data Protection Law was redrafted by Ordinance No. 2018-1125 dated 12 December 2018 for better readability and to ensure the coherence of the French legislation with EU legislation on data protection. It entered into force on 1 June 2019, together with a new implementing Decree No. 2019-536 dated 29 May 2019.

### iii The first GDPR sanctions

On 21 January 2019 the CNIL imposed a €50 million fine on Google LLC for breach of its transparency and information obligations and lack of legal basis for the processing of targeted advertising.

This €50 million fine is the first fine imposed by the CNIL under the GDPR and seems intended to be exemplary. It is the highest ever imposed by the CNIL. The CNIL stated that a €50 million fine was appropriate on the grounds that (1) the breached GDPR obligations were fundamental and central provisions of the GDPR (Articles 6, 12 and 13); (2) a significant number of data subjects was concerned; (3) the alleged infringements were continuous (and continuing) breaches of the GDPR; and (4) the significance of targeted advertising revenues to Google’s economic model.

---

96 See Ruling of the ANC of 10 December 2018 modifying the Ruling of 5 June 2014.
99 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
100 CNIL Decision No. SAN - 2019-001 of 21 January 2019 imposing a pecuniary sanction against GOOGLE LLC.
On 28 May 2019, 13 June 2019 and 18 July 2019, the CNIL imposed three other fines under the GDPR regime, mainly for failure of the infringers to implement technical and organisational measures to ensure security and confidentiality of personal data (article 32 of the GDPR).  

iv The CNIL’s new guidance on cookies

On 4 July 2019, the CNIL published new guidance on cookies providing general requirements for obtaining valid consent to the placement of cookies and other tracking devices.  

According to the guidance, organisations shall not place cookies or process personal data obtained through them unless users have previously positively accepted the placement in a free, specific, informed and unambiguous manner, in line with the definition and conditions of Articles 4(11) and 7 of the GDPR. As a result, the guidance repeals the CNIL’s 2013 guidance, pursuant to which users who continued browsing a website after being informed of cookie placement were deemed to have given consent.  

The guidance also details conditions under which certain audience management cookies may be exempted from the opt-in consent requirement.  

The CNIL announced that the guidance will be followed by supplemental guidance, which will specify the practical arrangements for obtaining valid consent, including by industry sectors.

v The implementation of Article 15 of the Copyright Directive under French law

The Copyright Directive 2019/790 came into force on 7 June 2019. The Directive is part of a wider strategy to reform the laws relating to digital marketing, e-commerce and telecommunications, to bring the EU into the digital age and achieve greater harmonisation of the laws governing these areas. Member States have until 7 June 2021 to transpose the Directive into national law.

France recently became the first Member State to transpose Article 15 of the Copyright Directive by the Law of 24 July 2019, creating a neighbouring right to the benefit of press publishers and news agencies for the online reproduction and representation of their publications by an online communication service provider. The Law will enter into force as from 24 October 2019 but will not apply to press publications published for the first time before the entry into force of the Copyright Directive on 6 June 2019.

It introduces new provisions under the French Intellectual Property by implementing an obligation to obtain an authorisation from publishers of online news services or news agencies before any reproduction or communication to the public of all or part of their press

---


102 CNIL decision No. 2019-093 of 4 July 2019 adopting guidelines on the application of Article 82 of the amended law dated 6 January 1978 to the reading or writing operations in a user’s terminal (in particular cookies and other tracking devices) (corrigendum).


104 Law No. 2019-775 of 24 July 2019
publications in a digital form by an online communication service provider. These rights will expire two years after the press publication is published, a term calculated from 1 January of the year following the date on which that press publication is published.

Press publishers and news agencies shall be granted compensation by online communication service providers using all or part of a press publication based on the exploitation revenues of any kind, direct or indirect, of the said communication service provider and if not possible on a flat-rate basis. Furthermore, the Law went beyond the provision of the Directive by specifying that such compensation shall take into account quantitative and qualitative elements such as ‘human, material and financial investments made by publishers and news agencies’, as well as ‘the contribution of press publications to political and general information and the importance of the use of press publications by an online communication service to the public’.

Finally, the Law has duly included the exceptions to such neighbouring right that relate to: hypertext links, the use of isolated words and the use of ‘very short extracts’ of a press publication and outlines that the use of isolated words or very short extracts may not impact the effectiveness of the new neighbouring right and that this effectiveness is ‘notably affected when the use of very short extracts replaces the press publication itself or exempts the reader from referring to it’.
I OVERVIEW


Within this rapidly evolving landscape, the Italian Communications Authority (AGCOM) has adopted many new regulatory measures in 2019.

With regard to telecommunications, AGCOM:

a completed the coordinated analysis of the markets for fixed-location access services (Resolution No. 348/19/CON), which defines the regulatory obligations imposed on TIM (as the operator holding significant market power in these markets in Italy, excluding the municipality of Milan) for the supply of wholesale access services on its optical fibre and copper networks. The Resolution takes into account the project for the voluntary separation of the fixed access network notified by TIM on 27 March 2018;

b defined the technical characteristics and the denominations of the different types of infrastructure used for the provision of phone services, television networks and electronic communications to end users (Resolution No. 292/18/CONS); and

c completed the analysis concerning mobile network voice call termination services and notified 12 operators who provide these services on their mobile network as holders of significant market power (Resolution No. 599/18/CONS).

In the audiovisual and media sectors, with Resolution 355/19/CONS AGCOM suspended the terms of the procedure aimed at identifying the relevant markets and any positions of dominance in the audiovisual media services sector until completion of the re-farming of the 700MHz band (1 July 2022), currently used for DTTV broadcasting.

Finally, in 2019 the Council of State concluded a long-running litigation concerning the 28-day invoicing system for landline and mobile telecommunication services adopted by the main Italian operators.

---

1 Marco D’Ostuni is a partner, Marco Zotta is a senior attorney and Manuela Becchimanzi is an associate at Cleary Gottlieb Steen & Hamilton LLP.
II REGULATION

i The regulators

Two main authorities are entrusted with regulating the IT, media and telecoms sectors in Italy:

a AGCOM, established by Law No. 249/1997, is an independent administrative body empowered to regulate and supervise electronic communications, broadcasting and publishing in Italy. In 2012, Law Decree No. 201/2011 extended AGCOM’s powers to postal services. AGCOM’s activity follows two main directions: preserving fair competition among market operators by preventing the creation of monopolies; and protecting consumers by ensuring minimum standards of quality, pluralism and the provision of universal services; and

b the Ministry of Economic Development, through its Department of Communications. In coordination with AGCOM, the Ministry manages the radio spectrum by approving the national frequency allocation plan and by issuing the related tender procedures. Upon request by operators, it also grants authorisations for the provision of networks and ECSs, as well as for the provision of television and radio contents.

ii Main sources of law

The main sources of law in the TMT sector are:

a Legislative Decree No. 259/2003 (the Code), which implemented the comprehensive regulatory framework for ECNs and services adopted in 2002 at the EU level, including the Framework, Authorisation, Access and Universal Service Directives. In 2009, Directive 2009/140/EC, Directive 2009/136/EC and Regulation (EC) No. 1211/2009 were adopted to improve and update the 2002 regulatory framework, and the Code was amended accordingly. The Code sets out the rules governing both public and private telecommunications services, including the provision of internet-based services;

b Law No. 249/1997, which established AGCOM and set out its regulatory powers; and

c Legislative Decree No. 177/2005 (the Consolidated Text on Radio and Audiovisual Media Services), which contains the regulatory framework concerning radio and television broadcasting.


On 18 December 2018, Directive (EU) 2018/1808 concerning the provision of audiovisual media services (the Audiovisual Media Services Directive) entered into force. Member States have until 19 September 2020 to transpose it. Italy has not yet adopted the measures necessary to transpose the Directive. The main points of the Directive include, in particular, the strengthening of the country of origin principle, the definition of video sharing

---

2 Directive 2002/21/EC.
3 Directive 2002/20/EC.
4 Directive 2002/19/EC.
5 Directive 2002/22/EC.
platforms, the strengthening of child protection measures (such as more stringent prohibitions for certain types of advertising), measures against the dissemination of violent content and content instigating terrorism or racial hatred, and the introduction of a 30 per cent minimum quota for European works for on-demand audiovisual media services and the obligation to give such works prominence.

iii Regulated activities
Italian telecommunications law provides for a general authorisation regime set out in the Code. Pursuant to Article 25, Section 3 of the Code, any provider of networks or ECSs is required to obtain an authorisation from the Ministry of Economic Development. To this end, the provider must file a declaration of its intention to commence the provision of electronic communication networks or services.

Article 1 of the Code defines the notion of ECSs as those services, normally provided for remuneration, which consist wholly or mainly in the transmission of signals on ECNs (by cable, optical fibre, satellite and any other electromagnetic means).

The provider can start to operate as soon as it has filed the declaration. However, no later than 60 days from the filing, the Ministry of Economic Development must verify that the conditions and requirements are met and grant the authorisation or, where appropriate, impose a ban on the activity. The authorisation is granted for a maximum 20-year period, is renewable and can be transferred to third parties.

The authorisation grants the provider the right to negotiate interconnection with pre-existing network providers and telecommunication services operators. It also entails the right to use RFs.6

The provision of media services is also subject to an authorisation regime, as set out in the Consolidated Text on Radio and Audiovisual Media Services.

iv Ownership and market access restrictions
Italian law generally makes no distinction between Italians and foreign nationals concerning investment and ownership in the telecommunications sector. However, Article 25, Section 1 of the Code provides that restrictions on the general authorisation regime provided by law can be applied by the Ministry of Economic Development to non-EU or non-EEA citizens and enterprises.

Moreover, the Ministry of Economic Development can issue an authorisation to non-EU companies only if Italian entities would have a reciprocal right to enter the market in their country.

Access to the telecommunications sector is also affected by the general rules set out in Law Decree No. 21/2012, as implemented by Presidential Decree No. 85/2014, concerning the regulation of strategic operations in the communications sector, such as the installation of infrastructure and the provision of broadband services.

These rules give the government special powers when facing operations that could constitute a threat to national security and defence, namely, the possibility to:

- impose additional requirements related to supply safety, data security and technology transfers;

---

6 See Articles 26 and 27 of Legislative Decree No. 259/2003.
b impose a veto on the merger or demerger of a company, on its transfer or the transfer of its registered office abroad, as well as on the dissolution of a company; and

c prohibit the purchase of shares by entities other than the government, Italian public bodies or entities controlled by them in the event that the purchase of shares would result in the purchaser holding a share of capital able to compromise the interests of defence and national security.

v Transfers of control and assignments

In the telecommunications sector, both AGCOM and the Italian Competition Authority (AGCM) enforce merger control rules. Pursuant to Article 1.6(c)(11) of Law No. 249/1997, AGCM must obtain a non-binding opinion from AGCOM on proposed decisions concerning communication operators.

Italian law also provides ownership restrictions to ensure external pluralism and competition in the media sector. Pursuant to Article 43 of the Consolidated Text on Radio and Audiovisual Media Services, AGCOM exercises its control to prevent the creation of dominant positions and ensure that the anti-concentration limits provided by law are respected by companies operating in the integrated communications system (ICS).7

To this end, undertakings operating in the ICS are required to notify a proposed merger to AGCOM, which can veto the merger if it would result in the creation of a dominant position capable of harming pluralism. Any merger concluded without prior clearance by AGCOM is null and void.

As stated in AGCOM’s Procedural Regulation adopted under Article 43 of the Consolidated Text on Radio and Audiovisual Media Services, AGCOM’s investigations on dominant positions are articulated in two subsequent stages: market identification and analysis.8 In January 2019, AGCOM adopted Resolution No. 9/19/CONS concerning the analysis of the economic size of the ICS for 2017.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

Given the variety of internet-based services (e.g., email, mailing lists, social networks and web search engines), all attempts to provide a comprehensive internet regulation have been unsuccessful.

---

7 Pursuant to Article 2(g) of Law No. 112/2004, the ICS is ‘the economic sector that includes the following activities: newspapers and periodicals; electronic publishing including the internet; radio and television; cinema; external advertising; product and service announcements and sponsorship’.

8 See Articles 5, 6 and 7 of the Procedural Regulation adopted by AGCOM with Resolution No. 368/14/CONS. In the first phase, AGCOM issues a draft resolution identifying the relevant markets, which is submitted to public consultation for 30 days. On the basis of the consultation outcome, AGCOM issues a final resolution that indicates the market that will be subject to analysis in order to assess the existence of dominant positions or positions that could otherwise harm pluralism. In the second phase, after having acquired the necessary information, AGCOM issues a new draft resolution, which it also submits to public consultation, concerning the analysis of the relevant market. If, based on the analysis, AGCOM finds a dominant position, it must adopt measures aimed at removing it.
However, sector-specific regulation exists, for example, with regard to online piracy. The digitisation of communications has exponentially increased the ability to reproduce and distribute works online without the consent of the copyright owner. Pursuant to Article 182 bis and 182 ter of Law No. 633/1941 (Copyright Law), as amended by Law No. 248/2000, both AGCOM and SIAE, the Italian association of authors and publishers, are competent to prevent and detect online copyright violations.

In exercising its powers, through Resolution No. 680/13/CONS, AGCOM adopted the Regulation on the protection of copyright on ECNs, the first measure ever adopted in Italy to fight online piracy. The Regulation aims to protect online copyright through two complementary actions: support for the development of a legal offer of digital works, and fighting against piracy through effective, proportionate and dissuasive enforcement procedures. The Regulation is only addressed to intermediary service providers and not to end users. The Regulation ensures the provided protection only at the initiative of the copyright owner. If the owner has already filed a claim on the same matter before the judicial authority, AGCOM has to dismiss the matter.

To stop copyright breaches, AGCOM may adopt different measures. If the works that infringe copyright are on a server that is situated in Italy, AGCOM can order the hosting service provider to remove the works or to disable access to them. If the server is located abroad, AGCOM orders the mere conduit service provider to disable access to the copyright-infringing website. Moreover, AGCOM can enable redirection to a web page whose content will be determined by AGCOM itself. All the measures taken by AGCOM may be appealed before the administrative judge.

Legislative Decree No. 3541/2017 entrusted AGCOM with the tasks of monitoring the adoption by collective management organisations of appropriate governance and financial standards in relation to rights holders and users, and the granting of multi-territorial licences for copyright on musical works for online use in order to promote their cross-border dissemination. Through Resolution No. 396/17/CONS AGCOM has adopted the regulation implementing the decree.

Finally, Law No. 167/2017 introduced new provisions in the field of copyright by entrusting AGCOM with the power of adopting precautionary measures for the protection of copyright, as well as measures preventing the reiteration of copyright breaches that have already occurred.

AGCOM implemented Law No. 167/2017 by adopting Resolution No. 490/18/CONS, which significantly amends the Regulation on the protection of copyright on ECNs.

ii Universal service

The Universal Service Directive has been implemented in Italy by Articles 53–57 of the Code. These provisions state that all users on the national territory, regardless of their geographical location, shall be entitled to certain ECSs to be provided at a predetermined quality level.

Article 58 of the Code establishes that AGCOM may designate one or more undertakings as having a USO; AGCOM carries out an objective, transparent and non-discriminatory designation procedure, whereby no undertaking is a priori excluded from being designated; and until the designation, which to date has not been made by AGCOM, TIM Mobile SPA (TIM) is designated by law as having a USO.

The universal service in the telecommunications field currently includes the following services:
a the provision of access at a fixed location to the public communications network, which allows users to make and receive calls, communicate by fax, send data and have functional access to the internet; 
b the supply of telephone directory services; 
c the provision of public pay telephones, which also allows for free access to emergency numbers; and 
d the supply of special conditions and options of service for disabled users.

In economic terms, the cornerstone of the universal service principle is the accessibility and flexibility of rates (i.e., the obligation to provide service even to unprofitable customers).

Although the concept of universal service has been extended over time to include a reference to functional internet access, it still does not include broadband services. However, through Resolution No. 113/16/CONS, AGCOM launched a preliminary investigation concerning the possibility to qualify the provision of broadband in the terms of the universal service. The results of the public consultation were summarised in June 2017 in Resolution No. 253/217.

AGCOM concluded that the EU requirements for the inclusion of broadband internet within the USO are met with reference to the 2Mbps internet connection speed, considering that such connection speed is used at a national level by at least half of all households and at least 80 per cent of all households having a broadband connection.

By Resolution No. 258/18/CONS, AGCOM defined the economic conditions for the supply of universal services to low-income users.

iii Restrictions on the provision of service

Network neutrality

Although there is no law in Italy that specifically regulates network neutrality, the latter has become a growing concern in AGCOM’s agenda. Network neutrality is the principle according to which there should be no discrimination in the treatment of internet data based on the content, device, application, origin and destination of the content. In 2011, AGCOM launched a public consultation entirely focused on net neutrality, the results of which were summarised in Resolution No. 714/11/CONS.

Network neutrality is challenged by the spread of forms of traffic management, which implies the treatment of bytes transmitted over communications networks.

The respect of the net neutrality guarantees provided by European Regulation No. 2015/2120 is monitored by AGCOM. Regulation No. 348/18/CONS establishes the right of end users to use terminal equipment of their choice and to enter into agreements with ISPs that do not limit the exercise of this right (the ‘free modem’ right). ISPs cannot refuse to connect to the network the terminal equipment chosen by the user, nor can they impose additional charges or unjustified delays on end users.

9 For example, according to this principle, a service provider cannot reserve priority to its own audiovisual content over that released by its competitors or via YouTube.

10 The results of the consultation showed a widespread consensus on, inter alia, the following issues: the idea that applying forms of traffic management does not constitute per se a market failure or a reduction in the opportunities available to the end user; and the fact that pricing (for example, choosing between flat-rate pricing and usage-based pricing) considerably affects the use of internet-based services. The results are available at www.agcom.it/le-risultanze-delle-consultazioni-gennaio-2012-.
With Resolution No. 68/18/CONS, AGCOM issued a warning against Vodafone for imposing a fee to access the internet from a mobile network in tethering mode, considering that this entails a restriction to the user’s freedom to choose the device from which to access the internet.

Additionally, the monitoring and supervisory activities carried out by AGCOM also concentrated on traffic management measures, as well as on the supply of ‘specialised services’.\(^{11}\) With regard to zero-rating offers (i.e., those offers where an ISP applies a zero price to the data traffic associated with a particular application or class of applications (and the data does not count towards any data cap in place on the internet access service)), AGCOM supervisory power focused on inducing providers to alter their contractual conditions, removing elements of potential incompatibility with EU Regulation No. 2015/2120.\(^{12}\)

Finally, AGCOM is aware of the possibility that EU network neutrality regulations may hinder the deployment of 5G, given that 5G services will rely on a core feature called ‘network slicing’, which allows a network operator to provide dedicated virtual networks with functionality tailored to different services or customers over a common network infrastructure.\(^{13}\) However, under Regulation No. 2015/2120 the principle of net neutrality does not prohibit an ISP from adopting reasonable traffic management measures. Such measures are considered to be reasonable as long as they are not discriminatory, they are proportionate and they are not based on commercial reasons, rather on technical requirements that pertain to specific traffic categories. AGCOM seems to suggest that network neutrality’s influence on the deployment of 5G will likely be determined by how the possibility to adopt reasonable traffic management measures will be interpreted, in an effort to accommodate network slicing and other new business models needed to support the deployment of 5G, yet without compromising the principle of network neutrality.\(^{14}\)

**Liability of ISPs**

As regards the liability of ISPs, pursuant to Article 17 of Legislative Decree No. 70/2003, ISPs are not subject to a general monitoring obligation with regard to content uploaded by their users that ISPs transmit or store; nor are they subject to a general obligation to actively seek facts or circumstances indicating illegal activity. However, when informed of any unlawful conduct or information provided by recipients of their service, they must promptly inform the competent judicial or administrative authority. In addition, upon request by the authorities, they must promptly prohibit access to illegal content. Failure to comply with this requirement may result in their civil liability.

\(^{11}\) AGCOM, Annual report, 2019, p. 77.

\(^{12}\) ibid.

\(^{13}\) See Italian Chamber of Deputies, IX Committee, Hearing of AGCOM Secretary General, Filippo Arena, on the fact-finding investigation concerning ‘New telecommunications technologies with particular regard to the transition to 5G and the management of big data’. Rome, 18 September 2019.

\(^{14}\) ibid.
Measures against unsolicited phone calls, faxes, emails and texts

Presidential Decree No. 178/2010 established a Public Objections Register. The Ministry of Economic Development – Department of Communications has entrusted the management of the Register to the Ugo Bordoni Foundation (FUB). Anyone, whether a natural or legal person, whose telephone number is listed in public telephone directories can subscribe free of charge to the Register to stop receiving unsolicited sales and marketing calls.

If, notwithstanding the subscription to the Register, an interested person still receives unsolicited calls, he or she can seek the intervention of the Authority for the Protection of Personal Data or a judicial authority.

Article 130 of Legislative Decree No. 196/2003 protects consumers against unsolicited advertising through email, fax or SMS (such as spam) by requiring their prior consent to the use of personal data for commercial purposes.

On 4 February 2018, Law No. 5/2018 (the Telemarketing Law) entered into force, introducing new provisions on the functioning of the Public Objections Register. The main feature of the reform is the possibility to be included in the Register also when using mobile numbers and landlines not registered in telephone directories.

iv Security

Homeland security

Law No. 43/2015 converted into law the Anti-Terrorism Decree. It contains urgent measures for the fight against international terrorism. To protect national security, the Law introduces measures to counter proselytising activities organised through the use of the internet. The use of IT tools is considered an aggravating circumstance for crimes related to terrorism or incitement to terrorism committed through IT tools. The Law also provides that the Italian Postal and Communications Police must constantly update a blacklist of websites that are being used for terrorist purposes in order to facilitate police investigation.

Self-expression

With regard to the limitations to self-expression on the internet, there is no criminal provision that specifically targets online defamation. Article 595 of the Italian Criminal Code contains the general provision on defamation. However, it does not refer to defamation committed through the use of the internet, not even as an aggravating circumstance.

Data protection, privacy and the right to be forgotten

The protection of personal data in electronic communications in Italy is regulated by GDPR, which entered into force on 25 May 2018, and the Privacy Code, as amended by Legislative Decree No. 101/2018.

The GDPR has significantly changed the current Italian – and broader European – data protection framework. As a general rule, any operator in charge of collecting and processing personal data can do so only after obtaining the written consent of the person to whom the

---

15 Law Decree No. 7/2015.
16 Nonetheless, Italian courts often condemn online defamation under this provision.
18 Legislative Decree No. 196/2003.
19 Article 23 of the Privacy Code.
data relates or when one of the conditions set forth in Article 6 of the GDPR occurs (for example, when processing personal data is necessary to comply with a legal obligation of the controller; or to protect the vital interests of the data subject). To this end, the operator has to provide the user with any relevant information concerning the purpose of the data collection, including the rights of the user to access such data and to demand its modification or deletion.

Pursuant to Article 32 of the GDPR, network operators are subject to a general obligation of custody to reduce the risk of destruction, loss or unauthorised access to personal data.

Traffic data, meaning data processed for the purpose of conveying a communication on an ECN, must be deleted by the network operator as soon as the communication is complete. However, the operator is allowed to store it for a longer period of time – but in any case not longer than six months – if this is necessary for invoicing purposes. Moreover, the operator must store traffic data for up to 24 months for the prosecution of criminal offences.

Pursuant to Article 126 of the Privacy Code, location data can only be processed when it is made anonymous (or with the prior consent of users, revocable at any time) and to the extent and for the duration necessary for the provision of the service requested.

Failure to comply with these requirements may result in the application of both administrative fines and criminal sanctions. The operator processing the data has to inform AGCOM, the Italian Privacy Authority and the data subject about any risk of breach of network security, or about any breach of personal data that has occurred.

Privacy concerns also underlie the right to be forgotten, which is the right for individuals to have information about themselves deleted from the internet so that they cannot be found through search engines.

At the national level, one of the most prominent judgments in this field was rendered by the Court of Cassation in Google v. Vivi Down, concerning the broadcasting on Google Video of a video showing some boys humiliating a fellow student suffering from Down’s syndrome, and also insulting the Vivi Down association. Google’s managers faced criminal charges for failing to prevent online defamation and for having unlawfully processed personal data concerning the health condition of the boy. However, in the end, they were acquitted of all charges.

The Court of Cassation specified the characteristics of the right to be forgotten in a case concerning the breach of such right by both the director and the publisher of an online newspaper due to the prolonged permanence online of an article on a criminal issue that had involved the plaintiffs in the past and was still pending. The Court specifically identified the

20 Article 123 Section 1 of the Privacy Code. The exact moment of completion of the transmission of a communication depends on the type of ECS provided. For example, for a telephone call, the transmission will be completed when one of the users ends the connection. For an email, it will be when the recipient collects the message from the server of his or her service provider.

21 See Articles 162 and 167 of the Privacy Code.

22 This principle has been affirmed by the European Court of Justice in Case C-131/12, Google Spain SL, Google Inc v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzales, 13 May 2014.

23 Court of Cassation, judgment No. 5107/14 of 17 December 2013.

24 Court of Cassation, judgment No. 13161 of 24 June 2016.
unlawful processing of personal data in the maintenance of a direct and easy access to that article through the search engine, and not in the original methods of publication or in its archiving.

The Court of Cassation identified some balancing criteria aimed at settling the conflict between the right of an individual to be forgotten and the opposing right for the media to report news. The Court established certain conditions that legitimate a compression of the right to be forgotten, such as:

- the contribution made by the news to a debate in the public interest;
- reasons of justice, police matters, protection of rights and scientific, educational or cultural freedom;
- the status of the public person of the subject involved;
- the truthfulness, actuality and continence of the news; and
- the granting of the right of reply before the spreading of the news.

In a very recent case, the Court of Cassation further specified these balancing criteria by stating that, when facing a conflict between the right to be forgotten and the opposing right for the media to report news, the judge has to assess the public, concrete and current interest at the mentioning of the identifying elements of the people involved. This mention can be considered legitimate only if it refers to people who are in that moment subject to public interest, both for their notoriety or for their public role; otherwise, the right of such individuals to privacy with respect to past and hurtful events that have no trace in the collective memory has to prevail.

Following the judgment in Google Spain, Google has adopted a template to request the removal of search results deemed to be inappropriate, offensive or harmful to privacy. Alongside this measure, pursuant to Article 17 of the GDPR, data subjects have a right to obtain from the controller erasure of their personal data, inter alia, where the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, the data subject withdraws consent on which the processing is based or the personal data has been unlawfully processed.

According to Article 140 bis of the Privacy Code, these rights can be enforced before the Italian Privacy Authority or, alternatively, before the judicial authority.

**Interception of electronic communications**

Law No. 43/2015 modified Article 226 of the implementing provisions to the Code of Criminal Procedure. When it is necessary to acquire information concerning the prevention of crimes having, inter alia, terrorist purposes, committed through the use of electronic devices, the public prosecutor may authorise the interception of communications for a maximum of 40 days. The prosecutor can also authorise the storage of traffic data for up to 24 months and the acquisition of all useful information from telecommunications operators.

---

26 Court of Cassation, judgment No. 19681 of 22 July 2019.
Protection of children

Pursuant to Article 34 of the Consolidated Text on Radio and Audiovisual Media Services, as amended by Legislative Decree No. 120/2012, it is, in principle, prohibited to broadcast programmes that, taking into account the time of the broadcast, could seriously harm the physical, psychological and moral development of children, especially if the programmes contain violent or pornographic scenes.

Nevertheless, such programmes can be broadcast upon the request of broadcasting companies provided that they include a parental control system. In particular, they must be marked with an audio and visual signal at the beginning of and during the broadcast.

Legislative Decree No. 203/2017 has entrusted AGCOM with the task of classifying (from the perspective of children's protection) video games and audiovisual works to be spread online. Through Resolution 186/18/CONS, AGCOM issued a public consultation on this topic. By Resolution No. 74/19/CONS, AGCOM adopted the related regulation. In 2003, representatives of ISPs adopted the Italian Self-Regulation Internet and Underage Code, which contains specific provisions to target online child pornography. In June 2017, the Parliament adopted Law No. 71/2017, the first specific law in Italy targeting cyberbullying, which introduces measures to prevent the cyberbullying phenomenon, especially by emphasising the role of schools. Moreover, a victim of cyberbullying or her or his parents can demand a website operator to remove or obscure any personal data from the internet. If the operator does not comply with the request within 48 hours, the victim can lodge a complaint before the Italian Privacy Authority.

Cybersecurity

Cybersecurity is a growing policy concern in Italy. The threats in cyberspace can take different forms such as cybercrime, cyberespionage and cyberterrorism. In 2013, the government strengthened the protection of Italian cyberspace by creating a three-layer structure. The first layer is embodied in the Inter-ministerial Committee for the Security of the Republic, which is in charge of elaborating general strategies for national security. On the middle layer, the Decree establishes the creation of a permanent body in charge of connecting all administrations and regulatory bodies involved in the pursuit of strategic cybersecurity objectives. Finally, the Inter-ministerial Centre for Situation Assessment and Strategic Planning coordinates the recovery of systems functionality after an attack.

The National Anti-Crime Computer Centre for Critical Infrastructure Protection is a branch of the Italian Police in charge of surveillance of the cybersecurity of infrastructure in sensitive areas, such as defence, telecommunications and energy.

---

27 Law No. 71/2017.
28 See Articles 2 and 4 of Law No. 71/2017.
29 The structure was created by the Decree of the President of the Council of Ministers 24 January 2013, Directive laying down the guidelines for cybernetic protection. Article 2 Section 1 of the Decree defines cybersecurity as 'the condition under which cyberspace is protected by adopting appropriate measures of physical, logical and procedural security to face events, either voluntary or accidental, consisting of the undue acquisition and transfer of data, in its modification or unlawful destruction or in the damage, destruction or impairment of the smooth operation of networks and information systems or their components'.

© 2019 Law Business Research Ltd
In June 2016, within the framework of the National Conference on Cyber Warfare held in Rome, the creation of the first European Centre for Advanced Cybersecurity, based in Italy, was announced.

In 2017, the government adopted the national plan for cybersecurity based on 11 points that cover all aspects of individual, state, industrial and military security.

The legal landscape in this sector has also been impacted by the Directive EU/2016/1148 on Security of Network and Information Systems (the NIS Directive), implemented by Legislative Decree No. 65/2018. The NIS Directive is the first EU-wide legislation on cybersecurity and introduces significant fines based on a percentage of global turnover, similar to the regime imposed for antitrust violations. It also identifies the authorities responsible for implementing the measures required by the directive for economic sectors that are considered to be strategic.

IV SPECTRUM POLICY

i Development

Radio spectrum is an essential resource for telecommunications networks. It is the basis for wireless communications, but it is also key in areas such as broadcasting, transport, defence, environmental protection and energy. Due to the increasingly urgent demand for this scarce resource, spectrum policy has become crucial at both European and national level.

The management of the Italian RF spectrum is entrusted to the Ministry of Economic Development and AGCOM. The Ministry elaborates the national frequency allocation plan, which divides radio spectrum into frequency bands and assigns each band to services and users.

On this basis, AGCOM adopts the national frequency assignment plan, which determines the location of radio stations and the frequencies assigned to each of them. The final allocation of frequencies and the granting of the related rights of use is made by the Ministry of Economic Development following a call for applications by network operators. Both the allocation and the assignment of RFs has to be based on objective, transparent, non-discriminatory and proportionate criteria.30

Implementing Decision (EU) No. 899/2017, the Budget Law for 2018 entrusted AGCOM with the definition of procedures to reassign the 700MHz frequency, currently used for DTTV broadcasting, to mobile broadband wireless services for the development of 5G (re-farming), and the adoption of a new frequency assignment plan for frequencies to be allocated to DTTV, to provide a new framework for the DTTV service.

In 2017, the Ministry of Economic Developments launched a selection for the realisation of 5G trials in five big and medium-sized cities for a duration of four years, namely Milan, Prato, L’Aquila, Bari and Matera. The requirements for the trials are (1) efficient use of the 3.7–3.8GHz band; (2) adoption of technical solutions within those offered by 5G (including network slicing); and (3) implementation of at least one of the three use cases defined by the International Telecommunication Union (i.e., eMBB, m-MTC, and URLLC). The trials have been awarded to three groups of companies: (1) Vodafone, in technical partnership with industry and the Public Administration; (2) WindTre and Open Fiber; and (3) TIM, Fastweb and Huawei Italy.

30 Article 14 Section 1 of the Code.
Through Resolution 290/18/CONS, AGCOM adopted the new frequency assignment plan for frequencies to be allocated to DTTV. The plan indicates 15 new digital terrestrial networks: 10 national networks in the UHF band, four local networks in the UHF band and a regional network in the III VHF band.

The Budget Law for 2019 eliminated the restriction that required one-third of the available frequencies to be assigned for the dissemination of information of local interest. The previous frequency assignment plan was therefore updated with AGCOM Resolution No. 39/19/CONS.

ii  Flexible spectrum use
Following the European trend, the Italian regulatory framework concerning spectrum use has become more flexible. The intention is to promote spectrum sharing, not necessarily limited to a particular frequency band, as a spectrum management tool.

In July 2015, the Ministry of Economic Development, together with FUB, started an experiment on the 2.3GHz band, comprising the full sharing of spectrum by licensed and unlicensed operators.

On the basis of the results of this experiment, through Resolution No. 121/16/CONS AGCOM launched a public consultation concerning the licensed shared access to radio spectrum. The consultation concerned the extent to which a public or private frequency owner should share the portion of the spectrum that is not being used with one or more licensees on a voluntary or mandatory basis, without the risk of interferences that could impair the normal operation of its systems. The outcome of the public consultation, summarised in a document published on AGCOM’s website in November 2016, showed that the participants considered the licensed shared access approach to be particularly convenient with regards to spectrum portions that cannot be quickly diverted from the use to which they are assigned or that cannot be easily released by current incumbents.

On this basis, AGCOM is currently evaluating innovative forms of spectrum sharing, such as the collective use of (unlicensed) bands under licensed assisted access.

Pursuant to Article 14 ter of the Code, owners of allocated frequencies can trade them or allow other entities to use them through a lease. The owner has to notify both the Ministry of Economic Development and AGCOM of the intention to trade such frequencies. The authorities can impose a ban on the intended transfer of frequencies if the rights to use them were obtained free of charge.

iii  Broadband and next-generation mobile spectrum use
Following the Radio Spectrum Policy Programme elaborated at the EU level, AGCOM aims to boost the development of broadband services in Italy through efficient assignment of frequencies.

---

31 See COM (2012) 478 Final, 3 September 2012, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Promoting the shared use of radio spectrum resources in the internal market’.

32 Decision No. 243/2012/EU. As regards the 5G pioneer bands (700MHz, 3,400–3,800MHz and 26GHz bands), EU legislation has laid down a number of deadlines to facilitate the roll-out of 5G, subject to certain exceptions for justified reasons, namely: (1) Member States are required to allow the use of the 700MHz band for terrestrial wireless broadband communications services by 30 June 2020 and (2) the European Electronic Communications Code requires Member States, by 31 December 2020, to reorganise
Considering the increasing market demand for wireless broadband services, AGCOM has defined the rules for the assignment of the 3,600–3,800MHz band in Resolution No. 659/15/CONS. The Resolution establishes coverage obligations to meet the demand for high-speed connectivity services to implement the national strategy for ultra-broadband.

Following the European Commission’s call to make the 700MHz frequency available to mobile broadband to implement 4G and 5G technology across Europe, Law No. 205/2017 (Budget Law for 2018) regulates the process that will lead, in the four-year period running from 2018 to 2022, to the assignation of the 700MHz frequency to wireless broadband services.

Through Resolution 231/18/CONS, AGCOM established the procedures for the allocation and the rules for the use of the 5G frequencies; on this basis, in July 2018 the Ministry of Economic Development launched a national auction for the allocation of 5G frequencies. The list of companies admitted to the auction procedure was published on 6 August 2018. On 10 September 2018, the companies presented their initial economic offers; the auction was awarded on 2 October 2018, with offers amounting to €6.55 billion.

Vodafone and Telecom have been awarded the generic batch of the 700MHz band, in addition to the reserved portion already awarded to Iliad as a new entrant in the market.

Italy is, therefore, the first European country to have assigned all the pioneering bands for the development of 5G, anticipating the terms set by the European Code of electronic communications.

Resolution No. 129/19/CONS AGCOM defined the criteria for the conversion of the rights to use frequencies for the digital terrestrial services into rights of use of transmission capacity.

In September 2018, the Chamber of Deputies launched an inquiry concerning new telecommunications technologies, with particular regard to the transition to 5G and the management of big data. The aim of the survey is to analyse the potential offered by new technologies, which can lead to significant improvements, for example, in the field of transport safety or for the functioning of smart cities, focusing on the risks connected to the more rapid circulation of data.

iv Spectrum auctions and fees

The design of the selection procedure for assigning the spectrum can have an impact on competition, particularly how the market structure will look after the assignment. As the uses of the radio spectrum have increased, the application of spectrum by the regulator has developed from a centralised subsystem, where its use was determined by the regulator, to a market-based approach where users compete for spectrum. The Italian regulatory authorities believe that competitive procedures, namely auctions, are the most appropriate means to assign RFs to interested network operators. The merits of auctions are their transparency and capacity to attract foreign capital, and the fact that they allow the legislator to set a certain threshold of financial gain.

and allow the use of sufficiently large blocks of the 3,400–3,800MHz band and to allow the use of at least 1GHz of the 26GHz band, subject to demand and to any significant constraints on migration of existing users or band clearance.

33 These companies are Iliad Italia SpA, Telecom, Fastweb SpA, Vodafone, Wind 3 SpA, Linkem SpA and Open Fiber SpA. Only Iliad Italia SpA, as a new entry in the market, expressed interest in participating in the procedure for the batch of the 700MHz band.
Auctions are generally structured as an open procedure with a simultaneous multiple round-ascending mechanism. A large number of licences are simultaneously placed for sale and potential buyers call prices up during each round.

Only one operator for each group of companies is allowed to participate to avoid any risk of collusion and anticompetitive hoarding of frequencies. Participation in the auction must also be secured by an appropriate security deposit. Auction procedures have been used in Italy to assign the right of use for the 3.5GHz, 800MHz, 1,800MHz, 2,000MHz, 2,600MHz and 1,452–1,492MHz bands and, more recently, for the 5G frequencies (694–790MHz, 3,600–3,800MHz and 26.5–27.5GHz).

As for 5G, AGCOM’s auction regulation promoted the efficient use of spectrum by means of innovative auction tools, such as ‘use it or lease it’ clauses (aimed at incentivising an efficient exploitation of spectral resources, these clauses provide that operators without frequencies in specific bands can use the frequencies in those bands that are not used by the licensees in a number of Italian municipalities included in a ‘free list’), as well as ‘club use’ clauses (according to which each licensee can use all the awarded spectrum in areas where frequencies are not used by other licensees. To this end, each licence holder has pre-emptive rights on its assigned lot).

Moreover, the auction format included some special rules for new entrants, such as reserved spectrum, more lenient minimum coverage obligations and a right to national roaming (i.e., under specific circumstances, incumbent mobile operators that win spectrum in the 700MHz band must offer national roaming to new entrants on fair, non-discriminatory and transparent conditions). Additionally, to ensure competition between operators, a cap on the amount of spectrum that each operator can win was introduced.

AGCOM’s regulation also fostered the access and the development of new players in the value chain, including infrastructure-only operators and service providers, who can collaborate with mobile networks operators to offer innovative 5G services. In particular, the obligation according to which each licensee must provide wholesale access to other players for the development of 5G services is aimed at fostering non-telcos (verticals) and their service providers to develop innovative business cases and at ensuring the widest level of 5G coverage and access for all users on the national territory (including also the deep digital divide areas), in line with the objectives of the Italian and the European framework.

V MEDIA

i Regulation of media distribution generally
The Consolidated Text on Radio and Audiovisual Media Services sets out the rules governing the Italian broadcasting system. This regulatory framework includes different provisions for network operators and content providers.

---

34 Article 2(1)(c) of the Consolidated Text on Radio and Audiovisual Media Services defines a network operator as ‘the holder of the right to install, provide and operate an electronic communications network via digital, cable or satellite on terrestrial frequencies and the right to provide installations for the transmission, multiplexing, distribution and dissemination of frequency resources that allow the transmission of programmes to users’.

35 Article 2(1)(d) of the Consolidated Text on Radio and Audiovisual Media Services defines content providers as ‘the person who has the editorial responsibility for the preparation of television or radio programmes and related data-programmes to be broadcast, even with conditional access, on terrestrial
Network operators must obtain a 12-year authorisation granted by the Ministry of Economic Development. However, the authorisation does not entail the automatic allocation of RFs and the right to use them, which has to be obtained separately.

The provision of television and radio content is also subject to a 12-year authorisation granted by the Ministry of Economic Development. Television content providers are additionally required to fulfil the obligations established by AGCOM in Resolution 435/01/CONS.36

Private broadcasters have to comply with a number of limitations and obligations established by law to protect end users. They are required to organise programming based on issuer classification. Therefore, the nature of the authorisation determines the related obligations depending on whether the broadcaster has a commercial, social, information or teleshopping purpose. To this end, ICPs authorised to provide content at the national or local level are required to, inter alia, broadcast news and radio news daily, allow access to their programmes to all political actors on an equal basis and broadcast certain events considered by AGCOM as having a major importance for society, on a free-to-air basis.37

More stringent obligations are imposed on RAI SpA, the concessionaire of the public broadcasting service, which has to be provided throughout the whole national territory (i.e., servicing not only lucrative urban areas, but also rural areas).38 The new service contract between RAI and the Ministry of Economic Development was approved in December 2017 and covers the years 2018 to 2022, replacing the previous one (2010 to 2012). The new service contract focuses on information, the obligations regarding the access to the RAI offer by people with disabilities, and the obligations on broadcast advertising (in this regard, it prohibits advertisements in any form on thematic channels dedicated to children and advertisements on gambling). On the merits of the obligations regarding information, the new service contract requires, among other things, that RAI must activate ‘tools aimed at combating the spread of fake news’, calling for (1) the establishment of an internal permanent commission; (2) the development of specific educational and didactic content; and (3) the implementation of promotional initiatives regarding the risks deriving from the spread of fake news.

In general, concerning the regulatory interventions on the prohibition of gambling advertisements, Law Decree No. 87/2018, converted into law by Decree No. 96/2018 (the Dignity Decree), provided for a general prohibition of any form of promotional communication concerning gambling. Law No. 208/2015 attributed to AGCOM supervisory and sanctioning powers concerning gambling advertising (a competence that was previously exercised by the Customs and Monopolies Agency and by the Italian Competition Authority for the aspects connected to unfair commercial practices). With Resolution No.

---

36 For example, pursuant to Article 6 of the Regulation content providers are required to store the complete recording of television programmes for a period of three months following broadcasting. Pursuant to Article 10, they must also reserve at least 20 minutes per week for advertising European works.
37 See Article 7 of the Consolidated Text on Radio and Audiovisual Media Services and AGCOM Resolution No. 131/12/CONS.
38 See Article 45 of the Consolidated Text on Radio and Audiovisual Media Services.
579/18/CONS, AGCOM published a questionnaire aimed at acquiring useful elements for the purpose of preparing guidelines on this topic. The guidelines were approved with Resolution No. 132/19/CONS.

When it comes to the regulatory measures to fight hate speech, AGCOM, over the past few years, recorded a growing recourse to expressions of discrimination against categories or groups of people, due, for example, to their particular socio-economic status, their ethnicity, their sexual orientation or their religious beliefs. With Resolution No. 403/18/CONS, AGCOM therefore kick-started the procedure for the adoption of a regulation specifically addressing non-discrimination and the contrast to hate speech. The regulation scheme was submitted to public consultation with Resolution No. 25/19/CONS.

In 2017, AGCOM adopted Resolution No. 41/17/CONS, which identifies the relevant markets in the audiovisual media services sector pursuant to Article 43(2) of the Consolidated Text on Radio and Audiovisual Media Services. The previous procedure concluded by AGCOM in the field of ICS dates back to 2010 (Resolution No. 555/10/CONS). The aim of the resolution is to identify, in a subsequent phase, any positions of dominance or positions likely to harm pluralism in the identified markets.

The Resolution identifies three relevant markets in the audiovisual media services sector: national free-to-air audiovisual media services; local free-to-air audiovisual media services; and national audiovisual media services for payment.

However, AGCOM has specified that the second phase will not take the local free audiovisual media services market into consideration because, following the entry into force of Law No. 9/14, this specific sector has undergone several changes owing to the need to reorganise the terrestrial frequencies.

As regards online distribution of audiovisual content, the Resolution also includes providers of audiovisual online services for payment, such as Netflix. This is because they are considered to be similar to the traditional pay-TV providers, as both services are based on users’ subscriptions and offer premium content. On the contrary, the provision of free audiovisual content through websites, social networks such as Facebook or Twitter and search engines such as Google, is deemed to fall outside the market definition of audiovisual media services, because the providers of free online content appear to be competing not with the traditional free-to-air broadcasters, but with the other internet operators.

Considering that the re-farming of the 700MHz band is intended to significantly change the structure of the digital terrestrial broadcasting, with significant repercussions on the offer of audiovisual media services to end users, with Resolution 355/19/CONS AGCOM suspended the terms of the procedure aimed at identifying the relevant markets and any positions of dominance in the audiovisual media services sector until completion of the re-farming of the 700MHz band.

ii Internet-delivered video content
The transition from traditional forms of media distribution and consumption towards digital converged media platforms continues to disrupt and change the commercial foundations of the entertainment and media industry. In Italy, as high-speed broadband connections become more widespread, internet video distribution continues to grow. According to the 15th Report on Communication by Censis–UCSI in 2018, the different forms of TV over internet (such as WebTV, smart TV and IPTV) have a 30.1 per cent audience (+3.3 per cent).
All of the most important TV channels have developed on-demand services that allow users to watch TV programmes online after the original broadcast. In addition to this, many operators have started to provide IPTV services. IPTV allows users to access television broadcasting networks (both in live-streaming and on-demand mode) via an internet broadband connection by using a set-top box (and not via a PC, tablet or smartphone, which can be used for WebTV).39

Although there is no comprehensive law governing the delivery of video content over the internet, by Resolution No. 606/10/CONS and Resolution No. 607/10/CONS, AGCOM has adopted two regulatory measures concerning the provision of audiovisual and radio media services on other electronic media (WebTV, IPTV and mobile TV) and the provision of on-demand audiovisual media services, respectively.

VI THE YEAR IN REVIEW

i Relevant regulatory measures

TIM’s separation of the fixed access network and Resolution No. 348/19/CONS

Pursuant to Article 50 ter of the Electronic Communications Code, on 27 March 2018 TIM notified to AGCOM its project for the voluntary separation of the fixed access network, which will lead to the creation of a separate legal entity (NetCo), 100 per cent controlled by TIM. NetCO will have its own assets (access network infrastructures, electronic equipment, IT systems and personnel) to supply and maintain the network access, both in copper and in fibre, including the equipment necessary for the supply of VULA and bitstream services. The separation should ensure the equal treatment of all operators, because NetCo will act as an ‘one-stop shop’ access point for all wholesale services both for other authorised operators and TIM’s commercial division.

The voluntary legal separation project notified by TIM was submitted to public consultation. Currently, AGCOM is completing the regulatory evaluation of the project. In the meantime, on 18 July 2019, AGCOM adopted Resolution No. 348/19/CON concerning the coordinated analysis of the markets for access services provided at a fixed location. It replaces Resolution No. 623/15/CONS.

With Resolution No. 348/19/CONS, AGCOM:

a identifies the municipality of Milan as a relevant market distinct from the rest of Italy both for the local access services market (market 3a) and for the wholesale access services market for consumer products (market 3b), due to the significant presence of electronic communication infrastructures alternative to those of TIM (open fibre) and to the level of competition registered for the access services to the wholesale fixed network;
b considering the level of competition registered in markets 3a and 3b in the municipality of Milan, it revokes the regulatory obligations imposed on TIM by Resolution No. 623/15/CONS;
c it confirms that TIM holds significant market power in markets 3a and 3b in the Rest of Italy and proposes the confirmation of TIM’s regulatory obligations concerning access, transparency, non-discrimination, accounting separation, price control and cost accounting;

---

39 In 2015, the most widespread WebTV, Netflix, made its debut on the Italian market.
d introduces some regulatory changes in relation to the municipalities considered most competitive; and
e with regard to the price control obligation imposed on TIM, it defines the cost-oriented access prices for the period 2018–2021.

Resolution No. 292/18/CONS
With Resolution No. 292/18/CONS, AGCOM defined the technical characteristics and the related denominations for the different types of infrastructure used for the provision of phone services, television networks and electronic communications to end users. It imposes on electronic communication operators some transparency obligations in advertising and describing the offers, as well as contract writing requirements.

Given the positive outcome of the monitoring carried out on the implementation of the provisions of Resolution No. 292/18/CONS, with resolution No. 35/19/CONS, AGCOM definitively approved the use of the coloured symbols ‘F’, ‘FR’, ‘R’ in all communications to the public, in order to identify in a simple manner the various types of access to the internet, depending on the type of connection between the station and the user site.

Resolution No. 599/18/CONS
Through Resolution No. 481/17/CONS, AGCOM submitted to public consultation the new market analysis concerning mobile network voice termination services. With Resolution No. 599/18/CONS, AGCOM concluded the analysis and notified 12 operators who provided voice call termination services on their mobile network as holders of significant market power. The Resolution also establishes symmetrical tariffs for termination services for all notified operators. Moreover, for the first time AGCOM has imposed the obligation to control the prices for the supply of interconnection kits. The obligation to control prices is confirmed only for calls originated within the European Economic Area.

ii Relevant litigation
The 28-day invoicing issue
Starting from 2015, all the operators informed their customers that the billing and renewal of services provided would be carried out on a four-weekly basis (every 28 days) and not on a monthly basis.

By Resolution No. 121/17/CONS, AGCOM established that the billing period for landline telecommunication services shall be no less than one month and the billing period for mobile telecommunication services shall be no less than 28 days, giving telecommunication operators 90 days to comply with the new provisions. Subsequently, Law No. 172/2017 confirmed Resolution No. 121/17/CONS.

Nonetheless, some operators maintained the 28-day invoicing system. By Resolution No. 269/18/CONS, AGCOM adopted specific measures against TIM, Wind Tre, Vodafone and Fastweb establishing the right of users to the reimbursement (by 30 December 2018) of the eroded days in the period between 23 June 2017 and the day of return to billing on a monthly basis, which took place between February and April 2018. The reimbursement has to be granted through the postponement of the invoicing date for a number of days equal to those illegitimately eroded. At the same time, operators are given the possibility to propose alternative compensation solutions to customers.
The operators appealed Resolution No. 269/18/CONS before the Administrative Court of Lazio (Rome), seeking the suspension of the measures therein adopted. On 21 November 2018, the Administrative Court rejected the appeal, reiterating the obligation imposed by AGCOM to reimburse customers by the end of 2018.

TIM, Wind Tre, Vodafone and Fastweb appealed the judgment before the Council of State. On 12 July 2019, the Council of State rejected the appeals, confirming the right of customers to the automatic reimbursement of the days illegitimately eroded through the 28-day billing system.

The same invoicing practices by telecom operators has been subject to the assessment of the Italian Antitrust Authority (IAA). On 7 February 2018, the IAA initiated proceedings against TIM, Fastweb, Vodafone, Wind Tre and Asstel for allegedly coordinating to preserve an increase of the tariffs charged to end users.

According to the IAA, the alleged coordination between the parties led to the adoption of almost identical implementation methods of the provision of Law No. 172/2017. Within the proceedings initiated to assess the alleged coordination between the operators, on 21 March 2018, the IAA initiated a sub-proceeding to adopt interim measures. It imposed on the operators the duty to suspend, pending the proceeding, the coordination concerning the repricing of the tariffs communicated to their customers, and it required each operator to define the terms of its offers independently from its competitors. The Interim Measure was confirmed on 11 April 2018.

This is the first interim measure adopted by the IAA in the context of anticompetitive agreement proceedings. The main case is still pending.

**Council of State – Judgments 5928/5929 and 5929/2019**

With Judgments No. 5928/2018 and 5929/2018 the Council of State defined the long-running dispute concerning the radio and television frequencies allocation in Italy. In 2007, the European Commission highlighted the incompatibility with EU Law of the Italian framework for (1) the allocation and management of radio and television frequencies and (2) the transition from analog television broadcasting to digital television. Given the need to assign the new frequencies, Italy adopted a regulatory framework aimed at allowing the entry into the market of new operators, which consisted in the launch of a beauty contest with a part of the frequencies reserved to new entrants. By Law of 26 April 2012 the beauty contest was suspended and replaced with a public selection procedure. Being an onerous procedure, it prevented the participation of smaller companies such as Europa Way, and it excluded operators who already owned three multiplexes (including Persidera, which had been awarded the beauty contest). The matter was referred to the European Court of Justice, which, in its judgment of 26 July 2017, acknowledged the incompatibility of the suspension of the beauty contest with European law, which prescribes that the regulation of the television market has to be dealt with by an independent administrative authority.

By Judgment No. 5929/2018 the Council of State partially accepted the appeal, re-attributing to AGCOM the power to choose autonomously whether to continue the interrupted beauty contest or to retain the criteria and the conditions of the onerous tender, ensuring in the meantime the provisioning of the audiovisual service.

---

40 Judgments Nos. 11303, 11304, 11305 and 11306 of 21 November 2018.
41 Judgment No. 4913 of 12 July 2019.
42 Case I820.
With Judgment No. 5928/2018 the Council of State acknowledged that the frequency conversion system was not compliant with the principles of non-discrimination, transparency, free competition and proportionality, especially considering that Rai and Mediaset already illegally offered some digital networks in violation of the anti-concentrative limits provided by Italian law and thereby held a competitive advantage. However, considering the ongoing re-farming of the 700MHz band and the 5G tender, the Council of State decided not to cancel the frequency allocation plan in force.

iii IAA intervention regarding the TMT sector

**Case A514 – Alleged abusive conducts of Telecom Italia in the ultra-broadband sector**

On 28 June 2017, the IAA initiated a proceeding against Telecom Italia for a possible abuse of dominant position. The investigation concerns an alleged abuse committed by Telecom in the markets for (1) wholesale broadband and ultra-broadband access services and (2) retail broadband and ultra-broadband fixed telecommunications services. The IAA accuses Telecom of having carried out a complex abusive strategy, composed of several conducts.

In the first place, according to the IAA, Telecom Italia attempted to impede or slow down the carrying out of tenders issued by Infratel Italia SpA (‘Infratel’, an in-house company of the Ministry of Infrastructure and Economic Development) for the deployment of ultra-broadband infrastructures in the ‘white areas’, in order to preserve its monopoly in these market failure areas. Telecom Italia is deemed to have done so by announcing its intention to invest in white areas after the tender process started. It, therefore, changed the investment plan presented during the public consultation phase carried out by Infratel, aimed at defining the areas that would not be interested in any private investment in ultra-broadband infrastructure in the near future (therefore called white areas).

Second, Telecom Italia allegedly planned a litigation strategy to slow down the awarding of the tenders (sham litigation), therefore impeding the entrance of new operators in the ultra-broadband market.

Third, Telecom Italia is deemed to have implemented anticompetitive practices with regard to the commercial offers for wholesale and retail ultra-broadband services, marketing promotions containing conditions capable of locking in the customers, and setting wholesale prices that could not be replicated by other competitors.

On 17 May 2019, the IAA sent the statement of objections to Telecom Italia, confirming the accusations detailed above. A final decision is expected between the end of 2019 and early 2020.

iv Mergers in the media sector

**SKY’s acquisition of R2**

On 28 November 2018, Sky Italia Srl (SKY) notified the acquisition of control over R2 Srl (R2). Owned by Mediaset Premium SpA (MP), R2 provides technical and administrative platform services for broadcasting by means of digital terrestrial television (DTT).

On 7 March 2019, the IAA opened an in-depth investigation into the transaction, alleging that SKY’s acquisition of sole control over R2 was part of a set of arrangements between SKY and MP – concluded on 30 March 2018 – that had ‘technical-functional’ and ‘economic-contractual’ links with the transaction. According to the IAA, the transaction was capable of lessening competition in the market for retail pay-TV services, in which SKY and MP were the main players, by providing an incentive for MP to exit the market, and had the
same effects as an acquisition of the whole of MP by SKY. The market for retail pay-TV services includes, in the IAA’s view, broadcasting through satellite (direct-to-home (DTH)), DTT and the internet. The IAA considered that the transaction could potentially hinder competition also in the markets for: (1) wholesale access services to DTT technical platforms; (2) the wholesale licensing of broadcasting rights; and (3) the wholesale supply of pay-TV channels.

Since the parties were not subject to a standstill obligation pursuant to Article 16 of Law 287/90, they completed the transaction after notification, and SKY acquired sole control over R2 before the IAA completed its assessment.

However, the transaction included a condition subsequent to allow SKY to return R2 to MP if the IAA adopted a prohibition or a conditional decision on the merger. Following notification of the statement of objections by the IAA, SKY withdrew the notification and R2 was demerged back into MP. As a result of the return of R2 to MP, R2’s platform was opened to third-party access.

Despite the notification’s withdrawal and the return of R2 to MP, the IAA took the view that the demerger only partially restored the situation to the status quo ante and did not remove the anticompetitive effects that the notified transaction had generated in the meantime.

On 20 May 2019, the IAA issued a decision clearing the notified transaction, albeit imposing the following remedies on SKY for a period of three years as of notification of the decision:

a an obligation not to conclude new contracts for the acquisition of broadcasting rights and linear pay-TV channels edited by third parties on an exclusive basis for the internet platform in Italy;

b an obligation to grant third parties access on a fair, reasonable, non-discriminatory and cost-oriented basis to any new proprietary DTT platform that SKY may set up, to the extent that the platform in question is ‘compatible with the R2 assets’ that SKY modified during the time in which it exercised control over the R2 platform;

c an obligation on SKY not to use information and assets belonging to R2 and already acquired for SKY’s pay-TV offers;

d an obligation to designate, within two months of the decision, a trustee to verify SKY’s compliance with the remedies; and

e an obligation to draw up and submit to the ICA, within three months of the decision and each year thereafter, reports setting out the actions taken by SKY to comply with the remedies.

Terzo Fondo F2i/Persidera

On 4 September 2019, the IAA launched an investigation on the acquisition of control of Persidera SpA (Persidera), a network operator active in the digital terrestrial broadcasting market (DTT) by Terzo Fondo per le Infrastrutture, set up and managed by F2i SGR SpA (F2i).

The merger involves the demerger of Persidera and of its subsidiary TIMB2 Srl in two newly established companies: NetCo, which will hold the business unit of radio and television broadcasting infrastructures on terrestrial frequencies, and MuxCo, which will hold purely intangible assets (ownership of the right of use) and some network assets, also managing commercial relationships with audiovisual media service providers.

NetCo will be acquired by EI Towers SpA (EI Towers), while MuxCo will be acquired by F2i SGR.
The merger involves the television industry, with specific reference to digital terrestrial broadcasting. The IAA believes that the acquisition of Persidera by F2i, by virtue of the control of EI Towers by the same F2i, could determine the establishment of a dominant position of the new company with (1) horizontal effects, since Persidera and EI Towers are direct competitors in the supply of ‘full service’ services to network operators for the management of frequencies and (2) vertical effects, by foreclosing inputs for network operators that are not vertically integrated and customers for companies competing with EI Towers. Moreover, due to the stake held by Mediaset in EI Towers, the IAA must ascertain whether there is a risk of coordination between Persidera, active in digital broadcasting, and Mediaset, active in the same market through its subsidiary Elettronica Industriale.

**Sky and Dazn’s commercial agreement**

On 31 August 2019, Sky Italia and Dazn announced the signing of a commercial agreement which, in addition to different offers to access streaming content, also includes the opening of the satellite channel DAZN1. From 20 September 2019 onwards, SKY subscribers with HD decoders that will activate the SKY-DAZN offer will have access to the DAZN1 channel, which will allow them to watch three Serie A TIM matches, two BKT Series matches for each round and a selection of international matches of football and other sports.

**VII CONCLUSIONS AND OUTLOOK**

The rapid development of technologies constantly opens up new scenarios in the IT, media and telecommunications markets. At the moment, the focus on the implementation at the national level by 2020 of the new EU Electronic Communications Code, which establishes a shift in the telecommunications sector, is introducing industrial policy objectives and expanding the role of the regulatory authorities.

The review of the telecommunications framework focuses in particular on measures that provide incentives for investment in high-speed broadband network. Particularly essential are the developments linked to the 5G frequency bands, which allow the transmission of significantly higher amounts of data in a very short time, also favouring the launch of the internet of things, opening the path to the convergence of fixed, mobile and broadcasting services.
I OVERVIEW

The media and telecommunications environment in Japan has continued its rapid development throughout 2018 and 2019. While the country has already achieved a broadband penetration rate of 100 per cent, numerous measures have been (and continue to be) implemented to prepare the nation’s telecommunications networks and regulatory regimes for hosting the 2020 Olympic Games in Tokyo. To accommodate the increased number of foreign visitors that will attend the Olympic Games, both the government and private mobile service providers have focused their efforts on the expansion of free Wi-Fi accessibility. Concurrently with this increase in free Wi-Fi availability, long-standing restrictions on the use of foreign mobile devices in Japan have been liberalised, with the result that overseas visitors may temporarily bring and use their personal devices without registration.

The government, the three main mobile services providers and, more recently, Rakuten Mobile have announced their intent to offer next-generation 5G cellular data services by 2020. In furtherance of this goal, NTT DOCOMO, KDDI, Softbank and Rakuten Mobile were each allocated 5G spectrum by Japan’s Ministry of Internal Affairs and Communication (MIC) in April 2019. These four mobile services providers have each announced plans to invest significant sums toward the proliferation of 5G access. We expect Japan to make significant developments to its telecommunications networks in the months leading up to the Olympic Games, and to continue developing its infrastructure thereafter.

The government is also increasingly prioritising the expansion of market access and competition within the Japanese telecommunications industry, with the ultimate goal of reducing mobile device charges for Japanese consumers. Recent regulations and policy guidelines issued by the MIC have led to a significant increase in the number of active MVNOs, which has also resulted in a number of major Japanese companies entering the MVNO sector. The increase in MVNO service availability has served to both further increase pressure on Japanese regulators to facilitate fair competition within the telecommunications industry, as well as incentivise the major telecommunications companies to reduce prices.

The MIC and other government authorities have taken steps to eliminate, or rigorously regulate, various business practices considered by many to be anticompetitive, such as SIM card locking and automatically renewing two-year service contracts. The MIC and other governmental agencies remain committed to improving high-quality telecommunications
network access and reducing associated costs for consumers, and we foresee significant regulatory reforms on the horizon to accomplish these goals.

Recently, the Intellectual Property Strategy Headquarters of the Cabinet Office (IPSHQ) expressed significant concern about the growing number of websites promoting and enabling the piracy of media content in Japan, which the IPSHQ views as harmful to its ‘Cool Japan’ policy. In 2018, the IPSHQ announced its intent to adopt more concrete regulations during 2019 designed to block access to piracy websites. The IPSHQ’s proposal was vigorously debated among politicians, scholars and industry insiders, and eventually the IPSHQ decided during its final meeting in October 2018 not to schedule further discussions on the topic. Reports speculate that the IPSHQ may discontinue entirely its discussions on regulations to block access to piracy websites.

II REGULATION
i The regulators
The MIC’s broad authority to regulate in the telecommunications and broadcasting spaces is derived from a series of statutes, which are the ultimate source of law in these sectors in Japan. The core statutes conferring this authority include:

- the Wire Telecommunications Act, which governs facilities for wired signal transmission, such as wired telephony, wired broadband networks and cable television;
- the Radio Act, which governs facilities for wireless signal transmission, such as mobile phones, terrestrial and satellite television broadcast infrastructures and high-powered Wi-Fi networks;
- the Telecommunications Business Act, which regulates telecommunications and media businesses; and
- the Broadcast Act, which regulates the content that telecommunications and media businesses carry or provide.

The Broadcast Act and the Radio Act were amended in November 2010 to provide a more streamlined regime for the review and granting of broadcast licences, which included the separation of broadcasting licences from transmission licences, previously a single licence, in order to make the process of receiving a licence easier for applicants.

Prior to this amendment, general broadcasting licences, cable radio broadcasting licences, CATV broadcasting licences and licences to broadcast content through third-party facilities were granted by the MIC under different statutes using different procedures that had developed over time as the underlying technologies were developed and implemented. The statutory licensing provisions for these activities were consolidated into the amended versions of the Broadcast Act and Radio Act, under which broadcasting activities have been divided into two major licensing categories: main broadcasting, consisting of both terrestrial broadcasting and broadcasting through broadcasting and communication satellites located over 110 east longitude; and regular broadcasting, covering broadcasting through all other satellites, CATV and IPTV.

Prior to the amendment, terrestrial broadcasting licences were granted only to broadcasters that both provided their own broadcast content and operated the wireless transmission facilities used for its distribution. Under the amended Broadcast Act and Radio Act, broadcasters are able to distribute their programming through third-party terrestrial
wireless transmission facilities, just as they already were permitted to distribute their programming through third-party satellites and third-party cable television providers.

These reforms have lessened the regulatory burdens on telecommunications and broadcasting companies to provide flexibility as to the management of those companies and to open up competition by decoupling the ownership of broadcasting facilities from the production of broadcasting content.

**ii Regulated activities**

The MIC exercises its statutorily conferred regulatory power in numerous ways. For one, it has the authority to grant broadcasting licences (for facilities such as television and radio stations that produce or broadcast media content), wireless transmission licences (for mobile phones and facilities such as mobile phone base stations and satellites) and telecommunication business licences (for traditional wired communications as well as mobile phone providers and ISPs), and monitors the businesses conducted with such licences.

The MIC is also charged with allocating radio spectrum to licence holders, and has adopted detailed regulations to monitor and establish technical standards applicable to spectrum users and their licensed facilities and businesses. The process through which the MIC exercises this decision-making authority is often criticised as opaque and arbitrary. For example, the allocation of radio spectrum frequencies to private sector service providers is based on the overall judgement of the MIC, and not on any clear set of factors, leaving applicants unsure as to what elements are being considered and opening the MIC to accusations of favouritism or political manipulation. Spectrum policy in Japan is further discussed in Section IV.

The Broadcasting Act requires licensed broadcasters to stay politically neutral and report the ‘truth’. In February 2016, the Minister of the MIC stated during a legislative session that a broadcaster would violate the Broadcasting Act if it repeatedly broadcasted lengthy content supporting a particular political view without reporting on other political views. The Minister further indicated that, in the event of such a violation, the MIC could issue an order to suspend such broadcaster’s business. This statement was criticised for potential chilling effects on freedom of speech.

**iii Ownership and market access restrictions**

*Restrictions on foreign investment*

Foreign ownership and management of broadcasting licence holders, wireless transmission licence holders and Nippon Telegraph and Telephone Corporation (NTT), a semi-privatised national telecommunications service provider, is restricted by statute.

As discussed in Section II.i, the Broadcast Act and the Radio Act, each amended in 2010, now divide broadcasting activities into two categories: main broadcasting and regular broadcasting. Under the amended Broadcast Act, no foreign national, foreign entity or Japanese entity that has either a non-Japanese director or 20 per cent or more of its voting shares directly owned by one or more foreign nationals or entities may hold or receive a licence for main broadcasting. Further, the indirect foreign ownership of 20 per cent or more of a licence holder’s voting shares through a domestic subsidiary or affiliate is not permitted for terrestrial (non-satellite) main broadcasting licences. If foreign nationals or entities acquire 20 per cent or more of the voting shares of a main broadcasting licence holder, the licence will be cancelled. To avoid the unintended cancellation of its licence, a main broadcasting licence holder whose shares are traded on a stock exchange is permitted by statute to refuse
to recognise any transfer of its shares that would cause it to violate the foreign ownership restrictions. By contrast, foreign investment in regular broadcasting licence holders is not restricted. As a result, several foreign-owned broadcasters now broadcast into Japan through cable television and third-party satellites.

**Restrictions on cross-ownership**

Ownership of multiple broadcast outlets is restricted by the Broadcast Act and related regulations. This restriction on the concentration of ownership is intended to support press freedom and the diversity of speech in broadcasting. The restriction includes limits on the simultaneous ownership of shares in, and control over board seats of, multiple main broadcasting licence holders, as well as aggregate upper limits on the use of satellite transponder capacity for owners of multiple main broadcasting licence holders. However, in response to worsening business conditions for radio broadcasters, the MIC amended its regulations in 2011 to relax restrictions on the cross-ownership of radio broadcasting licence holders, now allowing simultaneous control of up to four licences. Cross-ownership of newspapers and broadcasters is not restricted in Japan. Newspaper companies often hold large ownership stakes in broadcast companies: in fact, each major private television broadcast network in Japan is affiliated with a major newspaper.

**iv Transfers of control and assignments**

In addition to foreign ownership and management, and cross-ownership limits, MIC approval is required for mergers and acquisitions that result in a new entity holding a main broadcasting or wireless transmission licence. Therefore, a statutory merger pursuant to which a licence holder will not be the surviving company, or the divestiture of a business conducted under such licence, each generally require MIC approval. The MIC’s review process focuses on the proposed transferee rather than the transferred broadcasting or wireless business, and primarily involves a determination as to whether that transferee would have been eligible to independently qualify as a new licensee if it had submitted a full application. According to the MIC, it generally endeavours to finish the licence transfer review process within one month, which is significantly shorter than in the case of licence renewals or new applications.

Further, the Telecommunications Business Act was amended in May 2015 to require the major telecommunications companies to renew their respective telecommunications business registrations when they engage in mergers or share acquisitions. This amendment, which came into effect in 2016, allows the MIC to review the potential anticompetitive effects of any proposed merger or share acquisition on business operations and fair trade. Anticompetitive concerns are particularly important in the Japanese telecommunications industry, which was monopolised by three major private telecommunication companies – NTT DOCOMO, KDDI and SoftBank – until Rakuten Mobile entered the market in October 2019.

---

2 These renewal requirements apply to any fixed line provider with greater than 50 per cent market share and any mobile provider with greater than 10 per cent market share.

3 NTT DOCOMO is publicly traded, but NTT Corporation holds approximately 64.10 per cent of its outstanding shares. NTT Corporation is 36.11 per cent owned by the Japanese Ministry of Finance as of 31 March 2019.
In addition, pursuant to Japan’s Foreign Exchange and Foreign Trade Act, certain acquisitions of shares in broadcasting licence, wireless transmission licence and telecommunication business licence holders by non-Japanese parties are subject to prior filing and waiting periods. When there are no national security concerns present, this is ordinarily a pro forma requirement.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

The MIC regulates internet and IP-based services (such as high-speed internet and VoIP), along with wired telephony and mobile phones, under the Telecommunications Business Act. The Act and the regulations thereunder emphasise protection of the secrecy of communications and the reliable and non-discriminatory provision of telecommunications services.

The Act not only regulates service providers that operate their own network facilities, but also service providers that facilitate telecommunications between users but do not operate their own network facilities (such as dedicated hosting services on which clients can operate an email server). Internet-based services that are not designed to facilitate telecommunication, such as internet banking and internet-based newsletter and media subscriptions, are not deemed to be telecommunications services and therefore are not regulated under the Act. However, personal matching services, SNS providers and other businesses not traditionally considered ‘telecommunications’ services may nonetheless be regulated under the Act, necessitating a filing with the MIC before commencing business.

ii Universal service

Under the Telecommunications Business Act and the NTT Act, the NTT group is required to provide wired telephony services (analogue or IP over optical fibre), pay phone services and emergency call services to all areas of Japan. NTT East and NTT West provide services to depopulated areas, and a telecommunications trade association comprised of each of the major telecommunications companies in Japan, then reimburses NTT East and NTT West for any cost deficits incurred by the NTT group’s provision of the service. National law requires each telecommunication service provider connecting its network with that of NTT East or NTT West to pay a small fee (approximately ¥2 to ¥8, varying from year to year) per landline and mobile phone number (customer), which costs are typically passed along to individual users in connection with their monthly telephone service bills.

There is no similar law requiring universal broadband service. However, as of 2015, the broadband infrastructure (3.5G, satellite internet, 3.9G, DSL, optics fibre/FTTH, etc.) penetration rate in Japan had already reached 100 per cent, and super-broadband infrastructure (optics fibre/FTTH, 3.9G and other infrastructure with data transmission

---

4 Regulated transactions include an acquisition of 10 per cent or more of the shares of a licence holder whose shares are traded on a stock exchange or over-the-counter market; and an acquisition from a Japanese party of any shares in a licence holder whose shares are not traded on a stock exchange or over-the-counter market.

5 NTT East and NTT West are subsidiaries of NTT (Nippon Telegraph and Telephone Corporation), which is itself 36.11 per cent government-owned. NTT was initially a single consolidated conglomerate that conducted all of the activities now conducted by the individual NTT group companies. In 1999, the NTT conglomerate was forced to split into multiple smaller companies for antitrust purposes.
speed over 30Mb per second, including DSL, FWA, satellite, BWA, etc.) penetration rate had similarly reached 99.98 per cent.

**Rakuten Mobile: a new MNO service provider**

Rakuten K.K., a major e-commerce platform, has long had the largest market share of all MVNOs in Japan. Its recently established subsidiary, Rakuten Mobile, was approved to become Japan’s fourth MNO in April 2018. Rakuten Mobile was allocated 1.7GHz 40MHz bandwidth in April 2019, and shortly thereafter announced the launch of its MNO services. To consolidate its service offerings, Rakuten K.K. also assigned its MVNO business to Rakuten Mobile in April 2019.

Rakuten Mobile had planned to commercially launch its MNO services in October 2019, but encountered delays that prevented it from meeting this timing. A ‘free supporter programme’ was launched by Rakuten Mobile on 1 October, which will continue until March 2020. Under the programme, 5,000 users in urban areas (including Tokyo’s 23 wards, Osaka, Kobe and Nagoya) are able to use voice, data and short message services without cost in exchange for participating in quality testing and customer surveys. According to media sources, Rakuten Mobile recently reported to the MIC that services have not yet been rolled out to 20 per cent of the planned ‘free supporter programme’ participants.

**Public Wi-Fi access**

According to a 2017 survey of foreign visitors conducted by the Japan Tourism Agency, the lack of free public Wi-Fi in Japan was ranked the third most inconvenient aspect of their visit to Japan.

The MIC has been planning and implementing improvements to public Wi-Fi services in an effort to increase the number of foreign visitors to Japan. In particular, the MIC has been managing the implementation of the SAQ2 JAPAN Project since June 2014. The goals of the SAQ2 JAPAN Project include:

- increasing the number of free Wi-Fi hotspots and improving the accessibility of these hotspots to the public;
- facilitating the availability and installation of Japanese SIM cards for foreign mobile phone users in Japan;
- reducing international roaming fees applicable to foreign mobile phone users in Japan; and
- implementing multi-language interpretation systems (i.e., translation applications).

In November 2013, an NTT group affiliate began providing a smartphone application called Japan Connected-free Wi-Fi, which allows users to connect to approximately 170,000 public Wi-Fi access points across Japan, including those at airports, train stations, convenience stores and tourist spots, with a one-time new user registration. The smartphone application is available in 16 languages, including English, French, German, Spanish, Italian, Chinese, Korean, Thai and Bahasa Indonesia. This NTT group affiliate also continues to install additional Wi-Fi access points.

---

6 This application was prepared primarily for foreign visitors’ use, but Japanese residents are also able to use the application.

7 SAQ is an acronym for selectable, accessible and quality.

8 As of October 2019.
In preparation for hosting the 2020 Olympic Games in Tokyo, in February 2016 the MIC issued a policy statement encouraging the adoption of a simplified and unified authentication protocol with the goal of increasing foreign visitors’ access to free public Wi-Fi services. In furtherance of this goal, the MIC is conducting field tests to prove the workability of a unified authentication protocol using smartphone applications and is disseminating this protocol to local municipalities to aid in the revitalisation of local economies through increased tourism. On behalf of the MIC, Gateway App Japan, a non-profit organisation, publishes a smartphone application called the Omotenashi app9 with the cooperation of KDDI and SoftBank, the primary competitors of the NTT group. It has yet to be decided whether the two smartphone applications (Japan Connected-free Wi-Fi and the Omotenashi app) will be consolidated or made compatible. Recently, a handful of private companies, such as Accenture and SoftBank, have launched first-party applications enabling foreign visitors to access thousands of Wi-Fi access points across Japan. With users’ consent, some of these private companies gather anonymised data from the use of their applications, including data user attributes and location history, which they then analyse and sell to third parties as reports.

Tokyo Metro, a railway company owned by the Japanese national and local Tokyo governments that operates many of the subway lines in Tokyo, provides public Wi-Fi access points at nearly all stations. In 2017, Tokyo Metro announced that it would equip all of the subway trains it operates with Wi-Fi by 2020. Both Japan Connected-free Wi-Fi and Travel Japan Wi-Fi will be available on these trains.

In January 2019, the government began imposing a ¥1,000 departure tax, informally known as the ‘international tourist tax’, on all foreign visitors to improve Japan’s tourism infrastructure, including through the proliferation and enhancement of public Wi-Fi.

Separately from the above improvements to free Wi-Fi services, major Japanese mobile phone service providers have established an emergency disaster service set identifier (SSID): 00000JAPAN. This SSID enables each Wi-Fi user to use all Japanese mobile service providers’ Wi-Fi networks during natural disasters regardless of the provider to which they are subscribed.10 This SSID was made available for the first time during a two-week period following an earthquake in the Kumamoto area in April 2016. More recently, this SSID was activated following flood disasters in the Hiroshima and Osaka areas in July 2018 and September 2018, respectively, as well as following a large earthquake in Hokkaido in September 2018. During the 2018 Hokkaido earthquake, however, the Wi-Fi access points were rendered unusable due to widespread electrical outages. In light of growing security and privacy concerns, the MIC recently warned that communications sent through this SSID are intentionally unencrypted to prioritise accessibility, and therefore subject to interception by third parties.

Use of foreign mobile devices

As a general rule, it is prohibited to use mobile devices in Japan that do not meet Japanese radio wave emission standards, and with respect to which the manufacturer has not obtained authentication from the government. Therefore, until relatively recently, many foreign visitors’ use of their personal mobile devices in Japan was technically illegal, although there are no known cases of any foreign visitor being charged with Radio Act violations.

9 Omotenashi means hospitality.
10 Normally, users can only use the Wi-Fi network of the service provider to which they are currently subscribed.
for personal mobile device use. In August 2016, an amendment to the Radio Act took effect, permitting foreign visitors to Japan to use their personal mobile devices (even if not authenticated in Japan) for up to 90 days, so long as the devices have either been certified by the Federal Communications Commission in the United States or received CE certification in the European Economic Area using standards equivalent to those imposed upon Japanese technology. This Radio Act amendment was implemented to encourage foreign tourists to visit Japan in anticipation of the Olympic Games in 2020. While there had previously been concerns that devices not authenticated in Japan could adversely affect the radio use environment, the MIC eventually concluded that the likelihood of any adverse effect was minimal. In addition to government-imposed restrictions, private companies in Japan have in certain cases voluntarily adopted policies prohibiting the sale of certain foreign mobile devices. In May 2019, for example, NTT DOCOMO, KDDI and Softbank voluntarily ceased distribution of mobile devices manufactured by Huawai after sanctions were imposed upon it by the United States. These carriers eventually resumed sales of Huawei devices after the US government announced it was extending the pre-‘ban’ grace period.

Proliferation of the IoT

To address the rapid increase in the number of IoT devices, which could exhaust the number of available mobile phone numbers, the MIC in January 2017 amended its regulations on the assignment of phone numbers to assign the designation ‘020’ to M2M data connection devices, keeping them separated from standard mobile numbers designated with ‘090’, ‘080’ and ‘070’. It is expected that M2M data connections conducted through mobile networks will initially be used primarily for telemeters (e.g., remote management of water and gas meters, vending machines and elevators) and telematics (e.g., GPS and other information services equipped in vehicles) and will eventually cover connected cars and other IoT devices. NTT DOCOMO, KDDI and several MVNOs commercially launched M2M data connection services in October 2017.

New regulations have recently been adopted to address IoT devices’ vulnerability to cybercrime (see the ‘Cybercrime’ section below).

IP network

In November 2015, NTT announced a plan to switch from the use of fixed-line PSTN to IP telephony. According to NTT’s updated implementation plan, NTT will commence work on the switch to IP telephony in January 2024 with planned completion in January 2025. As the existing PSTN is a fundamental telecommunications infrastructure, the MIC is paying close attention to what kind of IP telephony will emerge as well as the process through which NTT will transition away from PSTN. In light of the importance of PSTN to the existing infrastructure, in February 2016 the MIC asked the Telecommunication Council to identify potential issues that could arise from the switch to IP telephony. To mitigate certain concerns identified by the Council (such as consumers’ ability to retain existing telephone numbers), the MIC presented a proposed amendment to the Telecommunications Business Act to the Diet in March 2018, which was subsequently enacted in May 2018. Under the proposed amendment, each telecommunication company must obtain the MIC’s approval of its plans regarding the use of telephone numbers, and must thereafter comply with the approved plans. Additionally, when telecommunication companies cease to provide services during the shift to IP telephony, those companies must file notice of such cessation with the MIC so that the MIC may make a public announcement of the terminating services to customers.
Restrictions on the provision of service

The telecommunications industry in Japan has traditionally been dominated by NTT East and NTT West and by three major private telecommunication companies: NTT DOCOMO, KDDI and SoftBank. A fourth major service provider, Rakuten Mobile, was granted an MNO business licence in April 2018. While Rakuten Mobile initially planned to begin providing services in October 2019, its commercial MNO services were delayed. Because existing providers can become dominant to the exclusion of new entrants once their network or technology standard has been adopted by a critical mass of users, the MIC and the Japan Fair Trade Commission (JFTC) have jointly adopted guidelines to regulate anticompetitive practices by service providers with high market shares. For example, the guidelines state that the JFTC could take corrective action, such as issuing a cease and desist order, if a telecommunications service provider with a high market share, such as a mobile phone carrier, were to contractually restrict its customers from switching to another service provider or to charge an excessive cancellation fee for doing so.

Pricing restrictions

Under the Telecommunications Business Act, prices charged to end users by NTT East and NTT West for wired telephony and payphone services are subject to caps to be determined by the MIC. These caps are intended to prevent these companies from abusing their near-monopoly over these fundamental services and to encourage them to improve efficiency. Prices to be charged by NTT East and NTT West for optical data services, and prices to be charged by KDDI, NTT DOCOMO and SoftBank for mobile services, must all be submitted to the MIC for review before implementation. If the MIC finds a pricing scheme inappropriate, either because it is anticompetitive or otherwise significantly unreasonable, the MIC may require the carrier to change its pricing scheme. Otherwise, prices charged to end users and the other terms of service are not regulated. This may change, however, as Prime Minister Shinzo Abe and other government officials have recently started applying pressure on the major telecommunications companies to reduce prices for mobile phone services.

As a general rule, all telecommunication business licence holders must provide access to any other carrier that seeks to interconnect with their network. However, the prices charged for, and the methods of, interconnection have been areas of both public controversy and regulatory scrutiny. Telecommunications companies have pressed for greater access to NTT’s infrastructure, including its optical fibre network. NTT only provided access to its fibre optic network on a bulk basis until 1 February 2015, after which NTT East and NTT West respectively began to offer single-line fibre optic wholesale to other carriers, including to non-traditional telecommunication companies such as Sohgo Security Services (ALSOK) and Tsutaya, a rental video company. These fibre optic wholesale programmes are designed to facilitate fibre optic use by reducing fees for fibre optic services at the end user level. As of December 2017, approximately 690 operators had commenced use of these fibre optic wholesale services.

Prior to the commencement of NTT’s fibre optic wholesale programme, there were competition-related concerns stemming from the confidential nature of NTT East’s and NTT West’s contracts with the secondary retailers to whom they provided fibre optic wholesale services. At the time, other major telecom service providers, such as KDDI and Softbank, expressed concerns that NTT East and NTT West were providing their fibre optic wholesale services to NTT group companies at lower prices than to unaffiliated companies, which in turn enabled NTT group companies to provide fibre optic services to end users at lower
prices. In response to these concerns, the MIC issued guidelines relating to the provision of fibre optic wholesale that prohibit the disparate treatment of select service providers and also provide the MIC with potential enforcement mechanisms. A survey conducted by the MIC showed that NTT DOCOMO and NTT Communications (a data communication company within the NTT group) obtained approximately 60 per cent of the fibre optic wholesale service market by offering large fee discounts on their respective mobile services to end users. Given the prominence of this market share, and due to their relationship to NTT East and NTT West, other fibre optic service providers have argued that the discounted fees charged by NTT DOCOMO and NTT Communications are anticompetitive in nature. To address these concerns, the MIC decided in May 2016 to launch investigations into NTT DOCOMO’s business practices. In its investigation report, which was issued in August 2018, the MIC concluded that the discounted fees charged by NTT DOCOMO and NTT Communications did not constitute anticompetitive practices. However, the MIC did determine during its investigation that NTT DOCOMO’s online description of the terms and conditions applicable to its pricing discount was misleading to customers. NTT DOCOMO voluntarily modified this description, but in June 2018 the MIC nonetheless issued an administrative direction to NTT DOCOMO to prevent future occurrences of misleading marketing.

**MVNOs**

Along with the introduction of fibre optic wholesale services, the availability of mobile line wholesale services (MVNOs) in Japan has also begun to expand. While MVNOs have existed in Japan since 2001, until recently the number of service providers and subscribers had been few in number. In 2007, the MIC’s guidelines regarding MVNOs were amended to clarify the relative rights and obligations between MVNOs and MNOs, and a formalised dispute settlement procedure was established. After this amendment, the number of MVNO service providers using MNOs’ mobile lines or WiMAX lines significantly increased. In 2014, the guidelines for the operation of Type II designated telecommunication facilities were amended, which included a change in the calculations for mobile line wholesale pricing. These calculation changes have reduced mobile line wholesale prices to the benefit of MVNOs. More recently, in 2017 the guidelines regarding MVNOs were amended twice to, among other things, clarify that the MIC is authorised to issue business improvement orders to MNOs who discriminate against MVNOs with respect to providing access to its network.11

The aforementioned guideline amendments have spawned a recent increase in MVNO activity. In FY 2013, only 22 MVNOs provided data communication services or voice communication services in Japan. However, as of March 2019 the number of active MVNOs has increased to 1,003. Correspondingly, there were 20.94 million MVNO subscribers by March 2019, up from 7.17 million in December 2013. However, despite this recent increase in MVNO activity, MVNO service subscribers still only constituted 11.6 per cent of all mobile service subscribers as of March 2019.

---

11 The MIC, as part of its regulatory enforcement powers, has the authority to issue business improvement orders to telecommunications companies to the extent it deems their activities to significantly disrupt the sound development of telecommunications services.
Anticompetitive business practices

One of the reasons MVNO penetration remains low stems from MNOs’ common practice of permitting subscribers to purchase new mobile devices on monthly instalment plans – often simultaneously offering discounts on monthly subscription fees equal to or greater than the amount of such monthly instalment payments. MNOs advertise that this instalment and discount programme renders subscribers’ new devices ‘effectively free’. In contrast, the vast majority of MVNOs do not have the financial resources to permit subscribers to pay for new mobile devices in instalments. Instead, MVNO subscribers seeking a new mobile device must often pay its entire purchase price upfront. This resource disparity has made it difficult for MVNOs to compete with MNOs for new subscribers.

Recognising the high barriers to entry created by these ‘effectively free’ mobile device programmes, in March 2016 the MIC issued guidelines compelling MNOs to decrease the size of their mobile device discounts so that subscribers are required to make reasonable payments toward their new devices. The intended result of these guidelines is to bolster competition and, eventually, reduce mobile service subscription fees. In October 2016, the MIC issued official warnings to NTT DOCOMO, KDDI and SoftBank for attempting to subvert the March 2016 amended guidelines by distributing coupons to subscribers and potential subscribers in lieu of discounts.

The MIC has also made efforts to address the issues of SIM locking and mandatory two-year service contracts with automatic contract renewal, in each case to facilitate competition between MNOs and MVNOs and reduce consumers’ mobile expenses.

Since the MIC’s initial adoption of guidelines in 2010, it has encouraged mobile service providers to provide SIM unlock options for customers’ mobile devices, as it believes that the practice of SIM locking prevents consumers from freely choosing mobile service carriers and causes competition stagnation. Following an August 2018 amendment to the guidelines, mobile service providers will be required to honour SIM unlock requests for all mobile devices effective as of 1 September 2019, including devices purchased on second-hand markets, other than mobile devices for which the purchase price is being paid in instalments (in which case, SIM unlock requests must still be honoured starting 100 days after the purchase).

Until recently, there had been little progress toward the abolishment of automatically renewing two-year service contracts. For years MNOs frequently required customers enjoying the benefits of their ‘effectively free’ mobile device programmes to enter into two-year contracts under which customers were required to pay approximately ¥10,000 for early termination, plus an accelerated payment of the purchase price of a smartphone that would otherwise be paid by instalments during the two-year term. The two-year contract system, in conjunction with the effectively free mobile device practice, has long been identified as reducing customers’ freedom of choice in mobile service carriers. Though the MIC issued guidelines on numerous occasions over the years to address these contracting practices, which it viewed as raising anticompetitive concerns, the guidelines were largely ineffective at addressing the fundamental issue of automatically renewing two-year contracts.

However, the Japanese government finally took the next step in May 2019 by legislatively imposing restrictions on the use of automatically renewing two-year contracts through an amendment to the Telecommunication Business Act – a significantly more affirmative step than its prior non-binding guidelines. As a general principle, the newly amended Telecommunication Business Act prohibits the use of any contract provisions that would restrict consumers’ ability to terminate their mobile service contracts if the restrictions rise to a level that would be deemed to have anticompetitive effects. Given the generality, the
MIC has been delegated the task of adopting specific regulations to carry out this mandate. The MIC has drafted proposed regulations to clarify the types of anticompetitive behaviour that are prohibited under the amended Telecommunication Business Act, which have been reviewed by the Information & Communication Council and are in the process of being revised. The latest draft of the MIC’s proposed regulations lists, among others, the following as examples of prohibited provisions in consumers’ mobile service contracts:

\[ a \] any termination penalty (regardless of amount) in conjunction with a contract term longer than two years;

\[ b \] regardless of contract length, any early termination penalty in excess of ¥1,000; and

\[ c \] automatic renewal clauses coupled with an early termination fee, regardless of the initial contract term, unless the following conditions are met:

- the contract must be terminable without a fee during a minimum three-month window – extending from one month prior to expiry of the original contract term through the first two months of the renewal period;
- consumers must be given the choice, upon execution of the original contract, not to have any termination penalty apply to renewal periods;
- consumers must be given the choice, at the time of automatic renewal, not to have any termination penalty apply to that renewal period; and
- the service provider cannot change pricing or terms to incentivise customers to consent to a longer termination penalty period.

The MIC has also recently begun analysing the state of competition between MVNOs. In particular, the MIC has expressed concerns that MNOs might favour affiliated MVNOs and, in turn, discriminate against unaffiliated MVNOs by providing them slower data traffic speeds. The MIC did not mention any MNOs by name, but many commentators believe that the MIC was referring specifically to KDDI (with respect to UQ Communications, an MVNO that is 32 per cent-owned by KDDI) and SoftBank (with respect to Y!Mobile, a low-cost mobile service affiliated with SoftBank). In October 2018, the MIC established new regulations prohibiting MNOs from discriminating between MVNOs with respect to data traffic speeds.

Similar to the primary mobile service providers described above, the MIC has also recently expressed concerns that the market shares of UQ Communications and Wireless City Planning (WCP) could permit them to stifle competition by rejecting competitor MVNOs’ requests to connect to their telecommunication facilities. In response, the MIC designated UQ Communications and WCP as ‘Type II designated telecommunication’ companies effective as of December 2019. This designation requires UQ Communications and WCP to each file with the MIC its respective terms and conditions regarding competitor MVNOs’ access to its telecommunication facilities.

In light of increasing customer complaints, effective as of October 2018, the amended enforcement regulations of the Telecommunication Business Act added MVNO voice communication services to the list of services for which customers have an eight-day ‘cooling-off period’ after signing a new service contract, during which the agreement can be terminated without penalty.
Unsolicited communications
Separate regulations exist in Japan restricting unsolicited texts and emails and unsolicited phone calls. With respect to unsolicited texts and emails, the Act on Regulation of Transmission of Specified Electronic Mail prohibits:

a. the transmission of emails using false sender information as a means of advertisement for the sender's own or another person's sales activities;

b. the transmission of emails to persons who have not opted in to receive such specified emails; and

c. even where the recipient has opted in to receive emails from the sender, the transmission of an unreasonably large number of emails for the purpose of corroborating or promoting the sender's own or another person's sales activities.

Violators of these prohibitions on unsolicited texts and emails may face penalties of up to one year's imprisonment or a fine of up to ¥1 million. Regulations pertaining to unsolicited phone calls are handled at the local prefectural level. Accordingly, each local prefectural government has established a local ordinance prohibiting the making of unsolicited phone calls. For example, in July 2018 the Metropolitan Government of Tokyo increased penalties under an anti-nuisance ordinance prohibiting continued unsolicited phone calls, facsimiles, emails, and SNS messages, with offenders now being penalised with up to one year's imprisonment or a fine of up to ¥1 million.

iv Security
Protection of personal information
In keeping with Japan's constitutional protection of freedom of speech and secrecy of communication, the Telecommunications Business Act prohibits ISPs from censoring or infringing on the privacy of communications passing through their networks.

As a general matter, the Law Concerning the Protection of Personal Information (the Privacy Act) protects personal information or data that can be used to identify specific living persons. Under the Privacy Act, the entities handling such information are required to publish a 'purpose of utilisation' regarding its use. Personal information incorporated into a database must be kept accurately, and necessary and proper measures to maintain its security must be instituted. Any person whose personal data is kept in a database for more than six months has a right to request access to the data, and add to, modify or delete it. In August 2015, the Privacy Act was amended to strengthen the protection of personal information, including through expanded protection of sensitive personal information, restrictions on the transfer of personal information outside Japan and the establishment of protocols for the use of anonymised data to facilitate big data analysis.

Further, the MIC has issued Privacy Act guidelines that are specific to telecommunications businesses. As these guidelines are structured to reflect the requirements under both the Privacy Act, which generally applies to all businesses handling personal information, and the Telecommunications Business Act, which provides protections relating to the secrecy of communication (a constitutional right), they are considered even more stringent and robust than the Ministry of Economy, Trade and Industry guidelines, which solely reflect Privacy Act regulations. Under the MIC's Privacy Act guidelines, information related to persons making or receiving communications, such as their usage history, identity and user location, may only be disclosed to third parties in very limited circumstances, such as pursuant to a search warrant. In addition, the MIC's Privacy Act guidelines were amended on 2 November 2011,
allowing telecommunications business providers to provide a user’s locational information to third parties only if they have the user’s consent, a search warrant or other valid justification; and to obtain a user’s locational information pursuant to law enforcement agencies’ requests only if a warrant is issued. The MIC’s Privacy Act guidelines also require telecommunications businesses to establish internal regulations regarding the length of time they may retain communication log records, and to delete this information after the expiry of such period. In June 2015, the MIC amended the guidelines again to set out a suggested length of time during which communication log records may be retained (six months to a year, depending on the business reasons for retaining such information).

In response to amendments to the Privacy Act, the MIC, in April 2017, amended the guidelines to, among other things, require telecommunications business operators to publish privacy policies regarding their collection and use of private information and, in particular, the collection of information through smartphone applications. Telecommunications business operators are particularly likely to transfer personal data across borders, which is subject to certain restrictions under the Privacy Act when a business operator processing personal data in Japan transfers the data to third parties located in foreign countries. Even foreign businesses (not directly processing personal data in Japan) should pay attention to the extraterritoriality of Japan’s data privacy rules, which is triggered when the foreign business collects personal data from a data subject located in Japan when supplying goods or rendering services to him or her. In an effort to facilitate the international exchange of information, in July 2018 the Personal Information Protection Committee and the Commissioner for Justice, Consumers and Gender Equality of the European Commission mutually recognised each other’s personal data protection regimes as equivalent. Beginning in January 2019, the restrictions on the cross-border transfer of personal data between Japan and the EU have been exempted.

**Treatment of infringing content**

ISPs are not currently required to proactively delete content that infringes upon the intellectual property rights or privacy of others. However, the Internet Provider Liability Limitation Act, enacted in 2001, provides a safe harbour for ISPs that delete such content. Under this safe harbour, no ISP may be held liable for the deletion of content on its network if the ISP reasonably believes that the content infringes the intellectual property rights or privacy of others, or if a third party alleges infringement and the content sender does not respond to the ISP’s inquiry within seven days. The Internet Provider Liability Limitation Act further shields ISPs from tortious liability for failing to delete infringing content. In reliance on this statutory defence to liability, ISPs generally do not take steps to monitor the content passing through their networks. The Act does, however, authorise persons whose rights are infringed by content delivered over the internet to demand information regarding the sender of the content from ISPs so that legal action may be taken against the sender. However, as a practical matter, it is often not possible to identify the original sender of such infringing content where content passes through multiple networks. In recent years, the government has paid close attention to piracy issues affecting Japanese businesses, in particular those piracy activities that target the types of media relevant to its Cool Japan policy (e.g., manga and animation).

In April 2018, the IPSHQ took what many viewed to be an aggressive step by issuing a policy called Urgent Countermeasures against Piracy Sites directed at piracy issues. Under this policy, the IPSHQ declared that it is appropriate for private ISPs to voluntarily block access to three major piracy websites: Manga-mura, Anitube and Miomio. The policy does
not legally oblige ISPs to block access to these sites, but the IPSHQ nonetheless expects ISPs to voluntarily comply. Notably, there has been strong backlash against the policy from the Japan Internet Providers Association, which has argued that blocking access to these sites violates laws protecting the secrecy of communications. According to the IPSHQ, the policy is simply a temporary measure intended to bridge the gap until the government passes more permanent legislation concerning piracy websites. The IPSHQ established a council of experts for the purpose of drafting such legislation, and initially targeted the issuance of an interim report in September 2018. However, there has been strong disagreement among the council’s members concerning the legitimacy of blocking access to online content, which led to a failure to meet the intended report timing. The final meeting of the council in October 2018 ended without a subsequent meeting being scheduled. According to reports, the council may discontinue further discussions. We anticipate that concrete legislation on this matter will remain the subject of significant debate.

Protection of minors
A statute for the protection of minors from harmful internet content, known as the Youth Internet Environment Act, became effective in April 2009. The statute directs government bodies to improve internet safety for juveniles (under the age of 18) by encouraging ISPs to use technologies that limit juvenile access to harmful content. The statute targets content glorifying crime or suicide, obscene sexual content, and other depictions of extreme violence or cruelty. The statute further exhorts parents to monitor their children’s internet use, and to limit access to inappropriate content by using filtering software and other measures.

The statute requires mobile network service providers to filter internet content for customers that are juveniles, except where a parent has expressly requested that filtering not be used. Under the Act, commencing in April 2010, manufacturers of devices with internet connectivity (other than mobile phones) became required to pre-install filtering software or otherwise facilitate the use of third-party filtering software or services. Initially, the Act did not impose any filtering-related requirement on mobile phone use outside the mobile network (e.g., on Wi-Fi) partly because only 1.5 per cent of juveniles owned smartphones in 2010. However, as of 2017, 63.2 per cent of juveniles owned smartphones, and only 44 per cent of those juvenile smartphone users utilised filtering software. This means that a large population of juveniles could have been exposed, or at least had access, to inappropriate content in an unfiltered manner. In June 2017, the Act was amended to include smartphones within the scope of mobile network service providers’ obligations to filter internet content and manufacturers’ obligations to pre-install filtering software. The amended Act also requires mobile network service providers (i.e., MNOs and MVNOs) to confirm whether each new subscriber is a juvenile, and if so, to explain filtering to such juvenile and activate filtering. The amended Act became effective in February 2018.

Cybercrime
In Japan, cybercrime has long been an area of public concern. In recent years, law enforcement has focused its efforts on combating cybercrime related to computer hacking through the unauthorised use of IDs and passwords, and other attacks on security holes; the distribution of computer viruses, and the input of data and unauthorised commands that can cause damage to computers and data; and other types of crimes facilitated through the internet, such as drug trafficking, prostitution, fraudulent internet auctions and child pornography.
Combating the distribution of child pornography has been an area of particular scrutiny and public interest. The Act on Punishment of Activities Relating to Child Prostitution and Child Pornography and the Protection of Children, originally passed in 1999, prohibits the distribution of child pornography. This Act was amended in 2004 to outlaw the uploading and distribution of child pornography over the internet, and was further amended in 2014 to criminalise the simple possession of pornographic images featuring minors and to require ISPs to block such pornographic material.

To combat increasing cybersecurity threats, the Basic Act on Cybersecurity was enacted in November 2014. The Act prescribes the concept of cybersecurity and defines the roles and responsibilities of the government. In January 2015, the Cybersecurity Strategic Headquarters (Headquarters) and National Center of Incident Readiness and Strategy for Cybersecurity were established to facilitate programme planning, policy formulation and overall coordination for cross-cutting cybersecurity measures. In July 2017, the Headquarters issued a policy statement on cybersecurity focusing on 2020 and beyond, which lists the actions the government intends on taking, including the formation of a cybersecurity incident response team for the 2020 Olympic Games.

With respect to government authorities’ ability to monitor the content of telecommunications, law enforcement authorities were previously only permitted to utilise wiretapping during criminal investigations of organised crime for murder, drug-related crimes, arms possession or stowaway smuggling by obtaining a wiretap warrant pursuant to the Act for Wiretapping for Criminal Investigation (Wiretapping Law). However, in April 2016, the Wiretapping Law was amended to permit wiretapping to be used in criminal investigations underlying a broader scope of organised crimes, including those involving the use of explosive materials, kidnapping, fraud, theft and child pornography.

The MIC has expressed particular concerns that IoT devices are vulnerable to malware that could render them ‘zombies’ subject to manipulation by a cyber-attacker. The MIC has stressed that, to implement countermeasures against cyberattacks, it is essential to have specific information relating to the servers used for cyberattacks and infected networks. However, it was difficult for telecommunications business operators to share such information with one another in light of legal obligations to protect the secrecy of communications under the Telecommunications Business Act. In May 2018, the Telecommunications Business Act was amended with the goal of establishing a legal framework to permit the sharing of information among telecommunications business operators for cybersecurity purposes. Under the amended Telecommunications Business Act, a third-party organisation designated by the MIC will act as a hub through which the relevant information will be shared among telecommunications business operators without violating the secrecy of communications. In January 2019, the MIC designated ICT-ISAC Japan, a cybersecurity research organisation, to act as the third-party for these purposes. In addition, the Act on National Institute of Information and Communications Technology (NICT) has been amended to authorise the NICT to assess networks and identify those lacking appropriate password configurations. The NICT will identify the specific networks and convey the particular network-specific information to telecommunications business operators via a designated third-party organisation so that they can warn network owners of any password configuration deficiencies. The NICT began operating in February 2019 under the project name ‘NOTICE’ (i.e., the National Operation Towards IoT Clean Environment). Following these cybersecurity developments, the Telecommunication Business Act was correspondingly amended in April 2019 to add new data security requirements to the technological specification requirement for IoT terminal equipment.
IV SPECTRUM POLICY

i Development

The need for access to the radio spectrum has steadily increased with the proliferation of new technologies utilising wireless data transmission. The number of licensed wireless stations and devices increased from 3.8 million in 1985 (a majority of which were attributable to amateur radio stations and handheld two-way radios) to 251 million as of March 2019 (99 per cent of which were attributable to mobile devices).

The MIC holds broad discretion to determine how the radio spectrum is allocated in Japan and describes its decision-making process as open and collaborative – including consultations with the public, scholars and industry experts. However, the MIC’s decision-making has been criticised by some as arbitrary and opaque. This has led to some calls for the implementation of spectrum auctions as a fairer method of allocation. Despite such criticism, the MIC has yet to establish a system that provides transparency over spectrum policy and spectrum allocation decisions. While there was some movement toward implementing a spectrum auction system, a bill that would have implemented such system was submitted to the legislature in March 2012, the bill lost momentum following a December 2012 change in the controlling political party in Japan, and the bill has since been rejected.

Many critics point to the MIC’s issuance, in December 2014, of 3.5GHz 120MHz bandwidth spectrum licences to each of NTT DOCOMO, KDDI and SoftBank as prime examples of its discretionary authority when allocating spectrum. This was the first spectrum allocation since the MIC amended its policy restricting submissions of multiple licence applications from companies that operate their spectrum as a group. Prior to the amendment, companies that held more than one-third of the voting rights of another company were restricted from submitting licence applications together with such affiliate companies. However, to reduce multiple applications by de facto group companies and facilitate greater entry into the spectrum market, the MIC expanded this restriction on multiple licence applications by group companies to take into consideration additional factors in determining what companies constitute a group, including their non-voting capital structures, decision-making authority and the business relationships between companies. Due to this amended restriction, YMobile, a company in which SoftBank held an ownership stake but that had not previously been considered a SoftBank group company, was now considered a member of SoftBank’s group and unable to submit a spectrum allocation application, which resulted in applications being accepted from NTT DOCOMO, KDDI and SoftBank only.

As the MIC planned to allocate 40MHz of the 120MHz available to each of the three applicants, it was always clear that each would receive an equal allocation. However, there was some competition in the individual allocations across the available 120MHz in which the MIC exercised discretion. The 120MHz bank is divided into high, medium and low components. While NTT DOCOMO’s first choice was the low component, both KDDI and SoftBank preferred the high component. The MIC determined that it would grant SoftBank the high component because KDDI failed to specify in its application when they would be able to start operation of speeds of more than 1Gbit/second.

In November 2017, the MIC announced the allocation of 1.7GHz 80MHz bandwidth and 3.4GHz 80MHz bandwidth. Each of NTT DOCOMO, KDDI and SoftBank applied for allocation of 60–120MHz bandwidth. In addition, this time Rakuten Mobile, a major online shopping platform that has the largest MVNO market share, applied to become the fourth MNO. Pursuant to the MIC’s policy in favour of new entrants, Rakuten Mobile
obtained 1.7GHz 40MHz bandwidth and announced the launch of its MNO services. Each of NTT DOCOMO, KDDI and SoftBank also obtained 40MHz bandwidth.

In May 2019, the Radio Act was amended to expedite the implementation of 5G services. Meanwhile, the MIC completed the first round of 5G spectrum allocation, which was awarded to NTT DOCOMO, KDDI, Softbank and Rakuten Mobile in 2019 on the condition that 5G services shall be rolled out on a nationwide basis. For the purpose of expediting 5G spreading, the MIC also started granting subsidies to corporations for the installation of optical fibre.

ii  Flexible spectrum use

Originally, the Radio Act required the MIC to grant bandwidth licences that specified the specific purpose for which the bandwidth could be used. This inflexibility was criticised as an obstacle to the efficient use of bandwidth. The Radio Act was amended in 2010 to facilitate the flexible use of spectrum and allowed the MIC to grant licences covering multiple uses. For example, a terminal on a train can now be licensed for transmission of data for operation of the train (use for operation of public services) and voice data over a pay phone equipped in the train (use for telecommunication). As of 2016, the MIC had granted 1,500 licences permitting multiple uses, and the MIC expects that the number of such licenses will continue to increase.

iii  Broadband and next-generation mobile spectrum use

The MIC annually reviews spectrum usage and revises a spectrum allocation plan to reflect spectrum needs for new technologies and services.

By 2015, LTE networks operated by NTT DOCOMO, KDDI and SoftBank achieved 99 per cent coverage of the national population. LTE is technically categorised as 3.9G, even though the International Telecommunication Union permitted it to be commercially referred to as 4G. In March 2015, NTT DOCOMO was the first among the major Japanese mobile service providers to launch its LTE-advanced next-generation mobile communication service, called PREMIUM 4G, which uses carrier aggregation technology and is technically categorised as 4G. PREMIUM 4G’s maximum transmission speed reached 788Mb per second in limited areas. KDDI (au) and Softbank, the other major mobile phone companies in Japan, have also begun implementing the same service.

NTT DOCOMO, KDDI and SoftBank each plan on launching the next-generation mobile communication service (5G), which will enable data transmission speeds of up to 10Gb per second. As described above, 5G spectrum was finally allocated to NTT DOCOMO, KDDI, Softbank, and Rakuten Mobile in 2019.

The MIC monitors the development of new technologies and their need for spectrum. For example, the MIC has facilitated the development of intelligent transport systems through its spectrum policy by allocating appropriate bandwidth among each of vehicle information and communication systems, electronic toll collection systems and car-mounted radars. In June 2019, the MIC issued a roadmap to establish a ‘connected car society’, including a plan to begin use of automatic driving systems in a limited geographic area during 2020.

Additionally, the Tokyo Organising Committee of the Olympic and Paralympic Games announced in November 2017 a ‘Basic Spectrum Plan’ for the 2020 Games, pursuant to which the Committee is granting permits to use radio devices during the Olympic Games, including wireless microphones, transceivers, wireless cameras and wireless measurement equipment.
Spectrum auctions and fees

The MIC imposes spectrum usage fees on broadcasters, mobile phone carriers and other businesses that use radio spectrum, as provided for in the Radio Act. The formulae used to establish the usage fees have been criticised as unfairly favouring broadcasters at the expense of mobile service providers. Until 2005, fees were determined, in the case of broadcasters, on a per-broadcaster basis, and in the case of mobile phone carriers, by the number of base stations and mobile devices connected to the respective network. Notwithstanding a series of changes in 2005, 2011 and 2014, the formulae continued to favour broadcasters, satellite operators and other vested rights holders. No changes have been made to the usage fee formulae even after a further change in 2017 involving the formation of the Council of Spectrum Policy 2020, which discussed potential changes to the usage fee formulae but eventually concluded that no change should be made. The total amount of spectrum fees the MIC imposed for the fiscal year ending March 2015 was approximately ¥74.7 billion (up from ¥68 billion in 2010), 74 per cent of which was paid by mobile phone carriers and only 8.9 per cent of which was paid by broadcasters, which has raised concerns since the bandwidth of spectrum occupied by mobile phone carriers is actually narrower than that occupied by broadcasters. This gap existed because the discounted usage fees applying to broadcasters were less than those applying to mobile phone carriers on the grounds that broadcasting is of a public nature. In light of the 99.9 per cent mobile phone penetration rate, the MIC announced a plan in May 2018 to discount usage fees imposed on mobile phone carriers to match those imposed on broadcasters. The MIC planned to submit the relevant amendment to the Telecommunications Business Act to the legislature in 2019. The amendment to the Radio Act resulted in an increase to spectrum fees for 5G services and IoT, which applies to both mobile phone carriers and broadcasters.

While spectrum fees are purportedly charged to cover spectrum administration costs, such as monitoring illegal spectrum use, the MIC has been criticised for using the fees to pay for miscellaneous expenses that appear to have little connection to spectrum administration. In August 2010, an MIC committee charged with exploring spectrum usage fee reform announced a policy to strengthen the link between the amount of spectrum usage fees charged to licence holders and the bandwidth of spectrum they occupy, and to more efficiently use the spectrum usage fees collected. In May 2011, a bill to amend the Radio Act to implement the revised spectrum usage fee scheme was passed.

An action plan published in November 2010 by the MIC committee charged with studying spectrum allocation recommended that the MIC consider the introduction of spectrum auctions as a way to allocate spectrum licences more efficiently and transparently. However, the plan also warned that the transition would raise questions of fairness between existing licensees who did not pay for their licences at auction, and future licensees who would bear this additional auction-related cost. The committee also raised related concerns that the cost of auction fees could ultimately be passed along to consumers by way of increased service fees.

From March 2011 to December 2011, the MIC held 15 meetings led by scholars for the purpose of considering the implementation of spectrum auctions, and in March 2012 a bill was submitted to amend the Radio Act to include spectrum auctions. The amended Act would have established a mechanism through which the MIC could conduct auctions to grant licences to applicants offering the highest bid price. The spectrum auction was envisaged to be first used for the licensing of the 3.5GHz band, which was planned to be used for 4G mobile phones starting in 2014. However, discussions regarding the bill were put on hold in anticipation of a change in the controlling political party from the Democratic Party...
of Japan (DPJ) to the Liberal Democratic Party (LDP), which took place in December 2012. In January 2013, the Minister of Internal Affairs and Communications under LDP Prime Minister Abe announced that the LDP government would not resubmit the bill for spectrum auctions. The DPJ subsequently resubmitted the bill, but it was voted down. However, the DPJ was able to obtain the LDP’s consent to adopt a non-binding resolution by a committee of the legislature acknowledging that spectrum auctions have benefits and detriments and should be reviewed through public hearings. Efforts to implement spectrum auctions as a method to provide greater transparency into the MIC’s spectrum allocation process have effectively returned to square one. The MIC formed a study group in November 2017 to improve the effectiveness of spectrum use. In August 2018, the study group issued a report focusing on reform of the spectrum allocation system. This report discusses the feasibility of an auction system. It does not advocate a pure auction system under which only the offered amount is decisive, though it does recommend to using the offered amount as one of elements for spectrum allocation.

Following the issuance of this report, the Radio Act was amended in May 2019 to adopt what some commentators refer to as a ‘partial auction’ system, whereby the MIC will consider the amount of special fees offered by the applicant based on their own valuation of the spectrum. The applicant’s offer alone is not a decisive element, but it does serve as an element in the MIC’s consideration.

V MEDIA

i Restrictions on the provision of service

While freedom of broadcasting is an underlying premise of the Broadcast Act, the Act includes certain content requirements, including:

a an obligation to be politically impartial;
b a prohibition on reporting ‘manipulated facts’;
c an obligation to present diverse opinions on controversial issues; and
d an obligation to provide closed captioning, audio commentary or other forms of aid for the hearing-impaired and visually impaired where possible.

Main broadcasting licence holders are also required to provide a balance of entertainment, news and educational programming.

ii Internet-delivered video content

The internet and dedicated networks are widely used to deliver video content. Internet television services available in Japan vary widely, from simultaneous transmission of terrestrial and satellite television broadcasts, to exclusive IPTV channels with programming provided by domestic and foreign third-party programme providers, to VOD services. The methods of video delivery vary from free video-sharing sites (such as YouTube), to membership-based video-sharing sites (such as Nikoniko Douga), to partially fee-based video delivery sites (such as Gyao!) and to full fee-based video delivery sites (such as Hulu and Netflix). Many traditional television stations (i.e., Nippon Hoso Kyokai (NHK), a public broadcaster formed under the Broadcasting Act, and commercial television broadcasters) also offer VOD services, and are streaming broadcast programmes through personal computers and smartphones. A survey published in December 2017 indicated that there were 14.4 million fee-based video delivery service users in 2017, and the number was expected to increase to 20.1 million by 2020.
The Supreme Court has ruled that services that record and forward Japanese television programmes and those that provide real-time streaming of Japanese TV programmes via the internet breach the originating television station’s copyright. Therefore, third-party recording or streaming of Japanese television programmes without a licence constitutes a breach of Japanese copyright law.

For regulatory purposes, the MIC has taken the view that video delivery over the internet is not a broadcast under the Broadcast Act and, consequently, the content restrictions under the Act discussed in Section VI do not apply. While the term broadcast is defined in the Broadcast Act as the ‘transmission of telecommunication for the purpose of being directly received by the public’, the MIC’s position is that video delivery over the internet does not fall within this definition because content is not transmitted until a specific user makes a corresponding request, such that the broadcast is not being made to the public. This interpretation allows ICPs to distribute multimedia offerings without being regulated as traditional broadcasters. However, the MIC’s technical distinction has been criticised as resting on shaky ground, and calls have been made for clearer legislation clarifying that content restrictions will not apply to internet broadcasts.

VI THE YEAR IN REVIEW AND OUTLOOK

Throughout 2018 and 2019, Japan has continued to show its commitment to further improving its telecommunications infrastructure and developing new telecommunications and media technologies to be implemented in future years.

Looking ahead, the MIC is targeting the implementation of infrastructure to broadcast the 2020 Tokyo Olympic Games in 4K and 8K ultra-high-definition formats. In furtherance of this goal, the MIC in January 2017 granted broadcasting licences covering 4K broadcasting via broadcasting and communication satellites located over 110 east longitude to NHK and 10 commercial television broadcasters. At the same time, the MIC also granted broadcasting licences for 8K broadcasting to NHK. 4K and 8K broadcasting have been launched over 17 channels beginning in December 2018.

In addition to its ongoing objective of expanding access to free public Wi-Fi, the MIC has also announced its vision to have 5G mobile technology in place ahead of all other countries in anticipation of the 2020 Olympic Games. The public and private telecommunications sectors in Japan are working together as an ‘All Japan’ platform to achieve this lofty goal, and major telecommunications providers that have secured 5G spectrum allocation are already preparing to launch 5G services in 2020.

The development of media and telecommunications policies and technology in Japan has seen a resurgence over the past several years, and further significant progress is likely in the near future.
Chapter 10

LATVIA

Andris Tauriņš and Madara Meļņika

I OVERVIEW

ICT is one of the driving forces of the Latvian economy. In 2017, 6,559 companies\(^2\) with 33,990 employees\(^3\) contributed to 4.2 per cent of national GDP\(^4\), while in 2018 the export of computer and IT services generated €12,733.5 million in revenue.\(^5\)

For the period running from 2018 to 2022, the National Media Strategy for the Electronic Media Sector envisages the withdrawal of public media from the advertising market and promoting the impartiality and accuracy of the news. Another important long-term project is Cabinet of Ministers Order No. 102 ‘On the Electronic Communications Sector Policy Plan 2018–2020’, signed on 12 March 2018, which outlines the actions necessary to reach the goals of the EC communication 5G for Europe – An Action Plan.

The year 2019 has been marked by severe disagreements between public broadcasters and the National Electronic Mass Media Council, which functions as a platform for debate regarding the independence and future of public media. Moreover, due to the changes regarding the regulations on advertising, problems have arisen also regarding the financial situation of the public media.

II REGULATION

i The regulators

The field is mainly regulated by two institutions: the Public Unities Commission and the National Electronic Mass Media Council. Likewise, the state stock company Electronic Communications Office plays an important role.
Electronic communications

The Public Utilities Commission (Regulator)\(^6\) is an autonomous body that, inter alia, regulates business activities in the electronic communications sector and protects users’ rights from a technological perspective. The Regulator’s actions are based on the Law On Regulators of Public Utilities\(^7\) (LORPU), which came into force in 2001, as well as other legal acts covering specific regulated sectors.

In the field of electronic communications, the Regulator monitors the services provided by electronic communications companies, including voice telephony, transmission of data and electronic messages, leased lines, internet access, broadcasting of radio and TV programmes, and access to networks, infrastructure and interconnections.\(^8\) To do this, the Regulator assigns usage rights (licences) of scarce resources: RF spectrum and numbering.\(^9\) Additionally, it registers ECS providers, evaluates draft tariffs submitted by providers,\(^10\) acts as an out-of-court body to resolve disputes where providers are involved\(^11\) and carries out other tasks provided by law.

However, according to the Electronic Communications Law\(^12\) (ECL), the Electronic Communications Office (ECO) is mainly responsible for the administration of the RF spectrum and numbering resources.\(^13\) ECO provides electromagnetic compatibility, assigns RFs for the operation of radio equipment, and undertakes other tasks as provided by law.\(^14\)

Media

The other primary regulator, the National Electronic Mass Media Council (NEMMC),\(^15\) is also an autonomous institution. It monitors the legality of the content of electronic mass media.

On the basis of the Electronic Mass Media Law\(^16\) (EMML), the NEMMC, inter alia, maintains a register of the issued broadcasting and retransmission permits, analyses suggestions and complaints submitted by consumers regarding the operations of the electronic mass media, monitors the electronic mass media, and approves the list of the television programmes distributed to end users via digital terrestrial broadcasting free of charge.\(^17\) Additionally, it develops and approves the National Development Strategy of the Electronic Mass Media Sector.\(^18\)

The NEMMC has considerable powers regarding the public electronic mass media. Upon consultation with the public electronic mass media, it develops and approves annual

---

6 See https://www.sprk.gov.lv/.
8 Section 4 of the Decision of the Council of the Public Utilities Commission of 30 November 2017 No. 1/32. Regulations on the registration of electronic communications merchants and the list of electronic communications networks and services.
9 Article 9(1(4)) of the LORPU.
10 Article 19(2) of the LORPU.
11 Article 32(1) of the LORPU.
13 Article 4(2) of the ECL.
14 Article Section 6(1) of the ECL.
15 See https://NEPLPadome.lv.
17 Article 60(1) of the EMML.
18 Article 60(3) of the EMML.
plans for programmes. Additionally, it develops and approves the statutes of the public electronic mass media, determines the allocation of the state budget subsidy and the resources granted in the annual Budget, and appoints and dismisses the boards of the public electronic mass media. Finally, it can also make decisions regarding the termination of the activities of the public electronic mass media, and the reorganisation thereof, and make changes in equity capital.

**ii Main sources of law**

The main sources of law in the field of electronic communications are the above-mentioned Law On Regulators of Public Utilities from 2001, the Electronic Communications Law from 2004 and the Electronic Mass Media Law from 2007. The Law On the Press and Other Mass Media from 1990 contains the norms applicable to mass media.

Additionally, more detailed regulations are contained in the specific regulations issued by the Regulator or the Cabinet of Ministers. Some examples of these regulations are the Decision of the Council of the Public Utilities Commission No. 1/35 ‘General authorisation conditions in the electronic communications sector’ of 20 December 2018, Cabinet of Ministers Regulation No. 24 ‘Regulations on the State Fee for the Issuance of a Broadcasting Permit and the Review of the Basic Conditions, the Issuance and Re-Registration of a Broadcasting Permit, and the Supervision of the Exercise of Broadcasting Rights’ of 9 January 2018, Cabinet of Ministers Regulation No. 1226 ‘Regulations Regarding Types of Regulated Public Utilities’ of 27 October 2009, Decision of the Board of the Public Utilities Commission No. 1/32 ‘Regulations on the registration of electronic communications merchants and the list of electronic communications networks and services’ of 30 November 2017 (Regulations on Registration), among others. The Regulations regarding the general authorisation conditions are updated regularly.

**iii Regulated activities**

As stated in the LORPU, licences have to be acquired only by the providers of public utilities that are specifically named by the Cabinet of Ministers or the Regulator. The operations of providers of public utilities must be regulated, but the special laws and regulations of the regulated sectors do not provide for licensing or other registration, and such operators can start providing public utilities if they are registered on the register of providers of public utilities.

---

19 Article 62(1) of the EMML.
20 Article 62(4) of the EMML.
21 Article 62(5) of the EMML.
22 Article 62(7) of the EMML.
23 Article 62(1) of the EMML.
28 Article 181(1) of the LORPU.
Electronic communications

Providers of ECSs do not need a licence, but only a general authorisation.29 This regulation follows the Access Directive.30

Under the Regulations on Registration, providers must send a notification before the provision of:

- a fixed ECN;
- a mobile ECN;
- voice telephony services;
- public data and electronic message services;
- leased line services;
- public internet access services;
- access services; and
- interconnection services.

On the basis of the notification, a general authorisation is issued, and the rules thereunder must be followed by providers. All registered providers are recorded in a public register31 available on the website of the Regulator.32

On 20 December 2018, the classification of the above-mentioned services was amended by including a direct reference to the fact that notification must also be sent before the provision of the services offered through the virtual mobile electronic communications network.33

RF spectrum can be utilised for radio equipment operations after the receipt of an RF assignment use permit from ECO or in accordance with a common RF assignment use permit.34

Broadcasting and retransmission

Broadcasting rights are granted on the basis of an application. If an electronic media operator requires a RF resource, the broadcasting rights are awarded on a competitive basis.35 The basic criteria for evaluation are the creative, financial and technical provisions of a broadcast’s concept and the amount of the state language used during the broadcasting period.36

Upon payment of a state fee, a broadcasting permit is issued to the winner of the tender for 10 years. Upon expiry, a new broadcasting permit is issued to the electronic media operator without a competition if there has been no court judgment regarding violations of the ECL during the previous year.37

29 Article 32 and following of the ECL.
31 Article 18.1.(3) of the LORPU.
34 Article 50 of the ECL.
35 Article 15(4) of the EMML.
36 Article 17(1) of the EMML.
37 Article 18(6) of the EMML.
The retransmission and distribution of programmes on public ECNs requires the consent of the holder of the retransmitted programmes and the permission of the NEMMC.38

iii Ownership and market access restrictions

A foreign company can send the necessary registration notification and carry out the business of providing electronic communications services if it is established as a commercial business in any EU Member State or has established a subsidiary in Latvia. The registration notice also requires the company to identify itself using its united registration number.

The market can only be accessed if the service provider has a permission or relevant licence. Competition is also restricted due to the limited nature of the radio spectrum. Additionally, mergers and acquisitions are stringently controlled to avoid market concentration and abuse of dominance.

Corporations that are the owners of the media are obliged to inform the commercial registry authority of their beneficial owners in the cases and according to the procedure prescribed by the Commercial Law.

iv Transfers of control and assignments

In Latvia, the licences are issued on an individual basis. The Regulation Regarding the Licensing of Public Utilities states that the service provider is not entitled to transfer the licence to other persons.39 Likewise, permissions and rights to broadcast40 cannot be transferred.

However, companies can merge, and the general Latvian merger control framework applies to the TMT sector. The provisions on market participant mergers can be found in the Competition Law.

The Competition Council must be notified about every merger. Within the meaning of the Competition Law, mergers are considered to be transactions that result in the acquisition of influence in another undertaking, or even only the assets of a company or the right to use them.41

Notification is required prior to a merger if the total turnover of the merger participants in the previous financial year in the territory of Latvia constituted at least €30 million, and the turnover of at least two of the merger participants in the previous financial year in the territory of Latvia constituted at least €1.5 million each.42 Additionally, within 12 months from a merger’s implementation, the Competition Council is entitled to request that the participants submit a notification on an already implemented merger that does not conform to the above-mentioned provisions in the following circumstances: in the relevant market, the aggregate market share of the participants exceeds 40 per cent and there is a suspicion that the merger might result in or strengthen a dominant position, or competition in the relevant market might be notably reduced.43

38 Article 19(1) of the EMML.
39 Clause 16 of the Cabinet of Ministers Regulation No. 664 Regulations Regarding the Licensing of Public Utilities of 30 August 2005.
40 Article 15(2) of the EMML.
42 Article 15(2) of the Competition Law.
43 Article 15(21) of the Competition Law.
Mergers that create or strengthen a dominant position, or that may significantly reduce competition in any relevant market, are prohibited. However, such mergers can be permitted if the Competition Council imposes binding provisions on the relevant market participants, thus preventing negative consequences.44

If a notification has not been given in the cases specified in the law on or an unlawful merger has occurred, the Competition Council can impose a fine on the new market participant or on the acquirer of a decisive influence. The fine amounts up to 3 per cent of the participant’s or acquirer’s net turnover in the last financial year.45

During 2017, politicians and specialists in the field debated on the possible merger of mobile telecommunications operator Latvijas mobilais telefons (LMT) and Lattelecom, a telecommunications, technology and entertainment company that provides internet and electricity services. In November 2017, the government decided that the merger would not take place,46 and a memorandum of mutual understanding on the further development of these companies was signed in July 2018.47 Nevertheless, some players in the field still believe that the merger of these companies is inevitable.48 This was supported by the fact that on 9 May 2019 the relevant shareholders – the ministries of the Republic of Latvia and the company Telia Company – again debated on the merger.49

Another topic of considerable discussion is the merger of public media companies.50

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation
The ECL, adopted on 28 October 2004, regulates, inter alia, both traditional telephony services and the internet and IP-based services. In addition, the Regulations on Registration regulate all types of electronic communications.

Specific regulations cover, for example, rules regarding public internet access service providers storing data and the liability exemption regime.

ii Universal service
The regulations regarding universal services obligations51 have been implemented in Latvia through the ECL52 and the 17 November 2016 Decision of the Council of the Public Utilities Commission No. 1/24 ‘Provisions on universal service in the electronic communications sector’.

These Provisions state the duty of the universal service provider to provide access to a public ECN for voice telephony calls and the transmission of fax and data messages at data

44 Article 16(3) of the Competition Law.
45 Article 17(1) of the Competition Law.
47 ibid.
48 ibid.
49 ibid.
51 Directives Nos. 2002/22/EC and 2009/136/EC.
52 The last amendments in the relevant chapter were made on 13 June 2016.
rates that are sufficient to provide internet access all over Latvia. Currently, Lattelecom is the official provider of the universal service. Its tasks also include the duty to provide special services to persons with disabilities, such as discounts on such subscribers’ telephone lines, domestic calls, installation fees for broadband internet access services and subscription fees for broadband internet access services.

In accordance with the Next Generation Broadband Electronic Communications Network Development Strategy for 2013 to 2020, broadband coverage is being improved in the rural regions of Latvia. This means that the quality of the universal service will also be raised. Additionally, free internet, which is directly financed by the state budget, has already been available in all libraries, including those in the rural regions, for more than 10 years.

iii Restrictions on the provision of service

Restrictions on tariffs

Tariffs are strictly controlled by the Regulator.

Article 20 of the LORPU states that tariffs are to be set to the extent that payments made by users cover the economically justified costs of public services and ensure the profitability of public services, unless special laws on the field provide for other tariff setting principles. If factors affecting tariffs (such as profitability) change, the Regulator may propose a tariff review. The Regulator may apply tariff regulation measures to ECS that have a significant market power.

Prerequisites for providing services

To receive permission to provide services, providers must comply with the general rules regarding the electronic communications field. These general rules include, for example, data protection requirements, the duty to carry out any planned scheduled maintenance at the lowest possible hourly load and the duty to protect the ECN from unauthorised access. They can be seen as general restrictions on the provision of service, especially as in cases of repeated violations the Regulator can suspend the activities of a violating provider for a period up to five years.

Theoretically, service providers are free to choose which services they provide. However, the ECL regulates the minimal content of contracts between providers and users. There are also some norms in the general rules that apply specifically to service provision: for example, providers must comply with the restrictions on the transmission of illegal content specified in regulatory enactments. Providers must also not facilitate access to information on the internet the distribution of which is prohibited in accordance with regulatory enactments. Also the norms regarding consumer protection and the prohibition of unfair commercial

53 Section 4 of the Provisions on universal service in the electronic communications sector.
55 Article 60(2) of the ECL.
57 Article 33(3) of the ECL.
58 Article 22(3) of the ECL.
59 Section 18 of the General licence terms in the electronic communications sector.
60 Section 19 of the General licence terms in the electronic communications sector.
practice apply. Specific obligations and duties, such as those regarding transparency, equal
treatment, accounting separation, tariff regulation and cost accounting, can be imposed by
the Regulator upon ECS providers with significant market power.

**Rights and duties of providers**

ECS providers that provide public data and electronic message transmission or public
internet access services with temporary storage of transmitted information, provided that
the information is not stored longer than necessary for its transmission, are responsible for
the content transmitted if such provider proposes the transmission of information, chooses
the transmitted information recipient, and chooses or converts the broadcast information.\(^61\)

All other ECS providers are not obliged to monitor the transmitted information or
search for circumstances indicating the transmission of illegal content.\(^62\)

The exact terms and conditions of the provision of ECSs depend on a contract
concluded between the user and the provider. Nevertheless, the general licence terms state
the cases when the provider has the right to suspend the provision of the service:

\[\begin{align*}
 a & \text{ the end user uses unauthorised access to the operator’s ECN;} \\
 b & \text{ the end user, without the consent of the ECS provider, uses the end-user connection for } \\
 & \text{business in the electronic communications sector;} \\
 c & \text{ the end user does not comply with the terms of use of the services; and} \\
 d & \text{ in cases of usage contrary to those specified in the contract between the user and the } \\
 & \text{provider on the use of the ECSs, the rules for the use of ECSs or regulatory enactments.}\(^63\)
\]

End users and subscribers have equal rights to receive ECSs, and they have the right to
choose several ECS providers simultaneously.\(^64\) The ECL also specifically provides that a
service provider who offers digital television and digital radio services must ensure that the
services provided do not limit subscribers’ rights to a free choice of the service supplier, and
interoperability with other ECS providers’ services.\(^65\) Owners of private ECNs have a duty to
ensure the interoperability of their network if such private network is connected to the public
ECN.\(^66\) Additionally, the Regulator has the right to fairly, proportionally and with equal
treatment impose obligations regarding access and interconnections upon ECS providers to
ensure the access necessary to end-users.\(^67\) The Regulator has the same right regarding the
obligation on public ECN operators to ensure access to application software interfaces and
electronic programme guides.\(^68\)

---

\(^{61}\) Section 20 of the General licence terms in the electronic communications sector.

\(^{62}\) Section 21 of the General licence terms in the electronic communications sector.

\(^{63}\) Section 17 of the General licence terms in the electronic communications sector.

\(^{64}\) Articles 23(1) and 23(2) of the ECL.

\(^{65}\) Article 67(1) of the ECL.

\(^{66}\) Article 26 of the ECL.

\(^{67}\) Article 36(1) of the ECL.

\(^{68}\) Article 36(2) of the ECL.
iv Privacy and data security

Decisions on the basis of national security

On 20 June 2018, amendments to the EMML were adopted to strengthen Latvia’s information space. The general rules for creating media programmes were amended with the addition of the principles of neutrality and accuracy, and the imposition of a prohibition on presenting facts in informative documentaries and news in a deliberately misleading way. Additionally, the law requires media owners to disclose the true beneficiaries of electronic media in order to ensure transparency. The functions of the NEMMC have also been widened regarding the prohibition on hate-inciting television programmes.

The NEMMC generally also plays an active part in the field of security. For example, on 16 May 2018, together with the European Commission it discussed restricting the freedom of reception of Rossiya RTR, a television programme, in the territory of Latvia owing to content that allegedly incited hatred. On 31 January 2019, the NEMMC adopted the decision to prohibit the retranslation and distribution of ‘Rossia RTR’ in the territory of Latvia for three months. However, the decision was deficient as it explicitly prohibits only the retranslation of ‘Rossia RTR’, while the same content could be and has been provided also in other programmes, such as ‘RTR Planeta’ and ‘Rossiya-24’.

Cybersecurity

The Law on the Security of Information Technologies (LSIT) was adopted in 2010. It sets out the most important requirements for the security of information technologies for state and local government institutions and private legal entities. The law imposes some obligations on the providers of private entities that provide critical infrastructure, such as the duty to monitor and eliminate security loopholes.

On the basis of the LSIT, the Information Technology Security Incident Response Institution (CERT.LV) was established in 2011. Its main tasks are to maintain information on IT security threats, provide support in the case of IT security incidents, advise government institutions and organise informative and educational activities. CERT.LV is also in charge of security throughout the Latvian electronic information space and under the TLD.lv top-level domain.

The National Guard Cyber Defence Unit, established in 2013, and the Military Information Technology Security Incident Recovery Team (MilCERT), established in 2016, also have a key role in ensuring cybersecurity. Additionally, based on the National...
Security Concept, the National Information Technology Security Board was established on 28 May 2018 by appointing representatives from various ministries, the State Revenue Service, the Bank of Latvia, CERT.lv, MilCERT and other institutions.\(^{76}\) In addition to regulations mentioned above, in summer and autumn 2019 the Cabinet of Ministers debated on the Latvian Cybersecurity Strategy for 2019 to 2022.\(^{77}\) Taking into account the priorities set by the European Union and the objectives set out in national policy planning and other documents, the guidelines outline five fields of action for the period up to 2022:

\( a \) promoting cybersecurity and reducing digital security risks;
\( b \) resilience of ICTs, strengthening of provision of ICTs and services critical to society;
\( c \) public awareness, education and research;
\( d \) international cooperation; and
\( e \) cyber justice and the reduction of cybercrime.\(^ {78}\)

Article 9 of the LSIT states the duties of ECS providers, such as:

\( a \) ensuring the integrity of the network;
\( b \) drawing up an action plan for ensuring the continuous operation of the network, indicating therein the technical and organisational measures implemented to appropriately manage the risks posed to the security of the network and the provision of services;
\( c \) informing the relevant institutions regarding breaches of security or integrity that have had a significant impact on the operation of the ECN or the provision of services;
\( d \) upon the request of the relevant institutions, organising a security audit to be carried out by a qualified body governed by public law if essential breaches of security and integrity have been detected; and
\( e \) upon the request of the relevant institutions, disconnecting an end user from the ECN for a short period of time if such end user significantly endangers the rights of other users or the information system, or the security of the ECN.

On 25 October 2018, the LSIT was amended to implement Directive 2016/1148.\(^ {79,80}\) The amendments establish the obligation of basic service providers and digital service providers to comply with certain IT security requirements and to report security incidents. Certain tasks are set for CERT.LV, the Digital Safety Monitoring Committee, the Ministry of Defence and ministries monitoring individual sectors.

In October 2018, the Constitution Protection Bureau stated that within the past few years the Russian military intelligence service had repeatedly attacked targets in Latvia, including the defence and foreign affairs sectors. Some of the attacks had also been targeted towards the media.

---

\(^{76}\) Prime Minister Order No. 146 of 28 May 2017 On the National Information Technology Security Board.


\(^{80}\) Information available at https://likumi.lv/ta/id/302455-grozijumi-informacijas-tehnoloģiju-drosibas-likuma.
On the day of 13th Saeima (parliamentary) elections, attacks were carried out on the Latvian social network ‘draugiem.lv’ as well as some email systems, websites and network infrastructure in the public sector. However, no politically motivated cyberattacks, carried out by the Russian military intelligence service, which would have had an impact on the elections, had been observed.

**Data security**

To maintain high professional standards in the processing of personal data in the electronic communications sector and to develop new societal services and technologies, while respecting individuals’ rights to data protection and privacy, in May 2019, the Latvian Information and Communication Technology Association (LICTA) published the guidelines for personal data processing. These guidelines specify how the requirements of the GDPR must be applied to the specific nature of personal data processing within the electronic communications.

**Fraud**

To limit the number of cases of fraud in the electronic communications sector using numbering, on 11 February 2019, the Regulator modified the Numbering Fraud Prevention Rules. This was done taking into account the growing variety of fraudulent practices and the pleas of the businesses that had suffered from such fraud.

The rules supplement and clarify the signs of fraud, as well as explaining the necessary conduct of the victim in cases of suspected fraud, both nationally and internationally.

**Criminal law measures**

Unauthorised access to automated data processing systems is prohibited by Article 241 of the Latvian Criminal Code, while Article 243 stipulates liability for interference with the operation of automated data processing systems and illegal actions with the information included in such systems. The Criminal Code also prohibits illegal operations with devices that could influence automated data processing systems, violation of the safety provisions of information systems and other TMT-connected crimes.

**IV SPECTRUM POLICY**

**i Development**

For many years, there was a fee for the usage of spectrum. A significant change was its revocation in 2014. The respective amendments were made because the ECL provided (and still provides) that ECO collects a fee for provided public paid services, including a monthly...
payment for the provision of the electromagnetic compatibility of radio equipment. The Parliament concluded that, practically, the charge for an electromagnetic compatibility service is, in fact, a fee for use of the RF spectrum.

Additionally, ECS providers must pay a state fee for the regulation of public utilities. The procedures for granting the spectrum use rights are set out in the 16 June 2011 Decision No. 1/7 of the Board of the Public Utilities Commission ‘Regulations Regarding the Rights of Use of the Radio Frequency Spectrum’ (Regulations on the Spectrum Use), which were last amended on 6 August 2018. These amendments, inter alia, widened the list of cases when the Regulator can refuse to grant the rights to use RFs and set new regulations for the evaluation of applications. These were the first amendments to the Decision since 2013.

From 2021, the spectrum in the 700MHz frequency bands will be used solely for the provision of 5G services in Latvia.

ii Flexible spectrum use

An ECS provider cannot transfer the right to use the RF spectrum if it has not paid for the acquisition of this right. All other limitations in law apply regarding the transfer of the right to use numbering. Thus, it can be presumed that the flexible transfer of the use of radio spectrum is generally encouraged. This encouragement is proven also by the Regulator’s duty to ensure that RFs are used efficiently to promote competition and the harmonised transfer of RFs. The Regulator assesses the necessity of transferring the right of use of the RFs taking into account the competition.

Additionally, commercial activities without a Regulator’s permit for the right to use the RF spectrum can be carried in RF spectrums or channels for which a sharing RF allocation use permit has been specified.

However, no specific developments to enable new uses of the spectrum (terrestrial use of satellite spectrum, mobile use of spectrum previously licensed for fixed use, etc.) have been observed.

iii Broadband and next-generation mobile spectrum use

In 2017, 4G coverage reached 98 per cent of households in Latvia. Similarly, a large part of internet coverage in Latvia is ultrafast broadband (88 per cent of households), in which regard Latvia, as recognised in the Digital Economy and Society Index, stands far above the EU average. Latvia is also named as one of the top OECD countries for mobile data usage.

In 2018, more than half of all download speed measurements in the territory of Latvia exceeded 30Mbit/s. Also the quality of the signal has been described as outstanding when

---

88 Articles 6(1(2)) and 6(4) of the ECL.
89 Article 12 of the ECL.
90 Article 47(31) of the ECL.
91 Article 47(61) of the ECL.
92 Article 47(51) of the ECL.
looking at such parameters as latency, jitter and packet loss ratio. In this manner, as noted by the Regulator ‘the mobile internet quality indicators mark the further development of technology, both by improving and expanding the existing 4G technologies, as well as by providing a suitable platform for the gradual transition to the latest 5G technology.’

In 2012, however, there still were 363 white territories that needed the development of the optical network. Thus, and in line with the Europa 2020 strategy, in 2014 Latvia adopted the Next Generation Broadband Electronic Communications Network Development Strategy for 2013–2020. It was amended in 2016 and will be valid until 2020.

In accordance with the strategy, broadband coverage will be improved for the rural regions of Latvia with the help of state aid through the development of next-generation ECNs. Private providers have to deliver the last-mile connection. Within this project, between 2012 and 2015 a 1,800km-long optical line with more than 177 access points was developed. It is planned that this project will allow 83,000 new households to access the internet. The long-term NGA aims are 100 per cent coverage with 30Mbps and 50 per cent household penetration with 100Mbps by 2020.

On 12 March 2018, the Cabinet of Ministers signed Order No. 102 ‘On the Electronic Communications Sector Policy Plan 2018–2020’. The Order, inter alia, confirms Latvia’s readiness to reach the goals noted in the EC communication 5G for Europe – An Action Plan. The tasks include the release and reprogramming of the 700MHz band for mobile communications. An informative report on this issue, which outlines plans for the release of the 700MHz band from January 2022, was reviewed by the government in August 2018. The implementation of this project will take place two years later than demanded by the EU, as Lattelecom has the right to provide pay-TV services in the band until 31 December 2021.

On 11 January 2019, the Regulator annulled the rights of Lattelecom to use the specified bands after 1 January 2021.

On 19 June 2019, LMT started the provision of 5G network in Latvia. Similarly, on 18 June 2019, its competitor company ‘Tele2’ had already started the 5G base station to

---

96 Information available at https://infogram.com/id-qualityreport_2018_summary-1h0n250e0nz4pe?live.
103 Information available at www.sam.gov.lv/sm/content/?cat=433.
provide the network within a business centre. Thus Latvia was one of the first countries in the world to launch the 5G network. Additionally, Latvian firm MikroTik has announced the production of 5G internet routers in Latvia.\textsuperscript{105}

In 2018 and 2019, 27 Latvian municipalities were awarded financing from the European Commission to create WiFi points in their territories.

\textbf{Spectrum auctions and fees}

The right to use radio spectrum bands is acquired via auctions. In August and September 2018, an auction took place for the allocation of rights for use of the 3,550MHz–3,600MHz spectrum band.\textsuperscript{106}

Since 2014, no spectrum fee exists.\textsuperscript{107} It does not seem likely that any fee will be created again, as the monthly payment for provision of electromagnetic compatibility of radio equipment, collected by the ECO, fulfills the same goal. Licensed operators also contribute to the financing of the universal services.

\textbf{V \quad MEDIA}

\textbf{i \quad Regulation of media distribution generally}

Network operators and content providers are regulated separately. While network operators are mainly regulated by the Regulator in accordance with the ECL, content providers are governed by the NEMMC in line with the EMA.

Many restrictions on the provision of service were included in the 2018 amendments to the EMA (see more in Section VI). In addition, the EMA stipulates that the electronic media cannot include in their programmes:

\begin{itemize}
  \item[a] stories highlighting violence;
  \item[b] pornographic material;
  \item[c] encouragement of incitement to hatred or a call to discriminate against a person or group of persons;
  \item[d] a call to war or a military conflict;
  \item[e] an invitation to violently overthrow the state’s power or violently change the state machinery, to crush territorial integrity or to commit another crime;
  \item[f] scenes that discredit Latvia’s statehood and national symbols.\textsuperscript{108}
\end{itemize}

Providers must respect human rights and defend the idea of a democratic and independent Latvia.\textsuperscript{109} All television broadcasts in foreign languages, with specific exceptions, must be provided with subtitles in Latvian,\textsuperscript{110} while films must have either an audio translation or subtitles.\textsuperscript{111} If a public electronic medium creates and distributes television news broadcasts

\begin{itemize}
  \item[105] Information available at www.la.lv/tiesraide-no-rigas-un-liepajas-latvija-tiek-palaists-pirmais-5g-internets-lmt-tikla.
  \item[106] ibid.
  \item[107] Amendments in the Law on Taxes and Duties of 19 December 2013.
  \item[108] Article 26 of the EMA.
  \item[109] Article 24(2) of the EMA.
  \item[110] Article 28(4) of the EMA.
  \item[111] Article 28(3) of the EMA.
\end{itemize}
in a foreign language, a summary must be provided in the form of a line in the national language.\textsuperscript{112} European audiovisual works must occupy a minimum of 51 per cent of broadcast time, with the exception of news, sports events, games, advertisements and television stores.\textsuperscript{113}

The retransmission of an electronic media audiovisual programme from another EU Member State or EEA country can be restricted if its provider has unequivocally, seriously and materially violated specific provisions of the EMA at least twice during the previous 12 months.\textsuperscript{114}

Emerging platforms are treated differently from traditional media outlets. While the traditional outlets are considered as media, regulated by the Law on Press,\textsuperscript{115} platforms that are not registered as mass media or in their style are not identical to online news portals\textsuperscript{116} do not fall under the scope of this law. By now the criteria of an identical style, developed by the Supreme Court, have been applied only to platforms that work in cooperation with printed magazines, or which are publicly recognised as trustworthy news portals.\textsuperscript{117} Therefore, it is not known whether these criteria could be applied also to fight against the fake news outlets.

In 2017, Parliament adopted at first reading a draft Law on Public Electronic Media and its Management, which provides for a new and separate regulation for public electronic media, addressing their governance, financing, supervision and other issues. Initially, the bill was scheduled to be adopted by mid 2017, but in June 2019, the bill was on its second reading.

\textbf{ii Internet-delivered video content}

Latvian television provides access to many of its programmes on the Latvian Public Media portal.\textsuperscript{118} The same practice is evolving in some other television stations.\textsuperscript{119} However, here the distribution has not moved from television to the internet: rather, both are offered in parallel to cover Latvians living abroad, as well as people who do not have a television at home. Due to the plans on universal services, as well as the accessibility of the internet in libraries, this has a positive impact on consumers.

Many smart-television options are also offered to consumers in Latvia. Non-linear services have specific regulations within the EMMA. These regulations include, for example, the duty to ensure that minors under normal conditions cannot access the services that might seriously impair their physical, mental and moral development.

Since 2018, the NEMMC has the rights to limit access to websites that provide audiovisual content illegally. In August 2019, the NEEMC carried out a massive inspection of internet websites to find such channels. So far it has resulted in the blocking of two internet web pages, by restricting the use of their domain names until 15 January.\textsuperscript{120}

\begin{thebibliography}{9}
\bibitem{112} Article 28(5) of the EMA.
\bibitem{113} Article 32(1) of the EMA.
\bibitem{114} Article 21.1(1) of the EMA.
\bibitem{115} Law On the Press and Other Mass Media of 20 December 1990.
\bibitem{116} 17 October 2012 Judgment of the Supreme Court of the Republic of Latvia No SKC-637/2012.
\bibitem{118} See: https://www.lsm.lv/.
\bibitem{119} See: https://tvplay.skaties.lv.
\end{thebibliography}
VI  THE YEAR IN REVIEW

The year 2019 can be marked as one of public media crisis. Up to 2019, the EMML stated that the boards of public electronic media were to be appointed and removed by the NEMMC. Any person with a good reputation, high-level education and at least five years' professional experience in the field of media or business could be appointed as a board member. In spring 2019, the NEMMC appointed two new members of the Board of the National Television (LTV). This decision was opposed121 by the Latvian Journalists Association and other media representatives, who claimed that the chosen members of the board were not qualified enough as they did not have any media work experience. The chosen board members resigned122 and the NEMMC amended the statutes of the Board of the National Television stating that the Board is made up of one person.123

As a reaction to these events,124 on 20 June 2019, Parliament adopted amendments to the EMML, which clarify both the requirements for the members of the public media board and their selection procedure, as well as the procedure for the recall of the board. With the amendments125 the competences of the NEMMC have been limited, especially due to the creation of the Nomination Commission for Public Media Board Members.

This is one of the examples of disagreements between the NEMMC and the media. Additionally, in May 2019, the NEMMC initiated an administrative case against one of the commercial television stations in Latvia. The core of the proceeding was the distribution of the critical opinion, expressed by the State Audit Office of the Republic of Latvia, regarding the NEMMC. The politicians highly criticised this decision to initiate the proceedings by as it seemed that the law was being used to oppress the freedom of expression.126

Another important question has been the public radio crisis. On 15 July 2019, following the critical statements and the expression of distrust by the radio journalists,127 the Board of the Latvian Radio announced a human resources and financial crisis in the media.128 It was stated that at present, lack of funding critically endangers the ability to provide high-quality, objective and diverse information in sufficient quantities. The consequences of bad governance, as alleged by the journalists, was worsened by the decision in 2018 regarding the withdrawal of public media from the advertising market. Another financially negative effect was caused by the amendments to the Consumer Protection Law prohibiting the advertisement of consumer loans in the public media. Therefore, in August 2019, the

NEMMC had to demand €10 million extra funding from the state for the stabilisation of the financial situation of the public broadcaster.\textsuperscript{129} However, there is no clarity regarding the long-term solution yet. Additionally, even the additional budget does not solve the disagreements between the radio journalists and the board regarding the political influence on the content.\textsuperscript{130}

On another note, in September 2018, the Baltic Transport Ministers signed a memorandum of understanding on the development of connected and automated driving and 5G technologies along the Via Baltica corridor. The purpose of this memorandum is to promote connected automated driving with the aim of supporting sustainable mobility, improving road safety and promoting innovation. In addition, it is in line with one of the three strategic objectives set by the European Commission for the rollout of electronic communications networks by 2025 (i.e., to provide 5G in all major cities for continuous highways).\textsuperscript{131}

i Mergers, acquisitions and licensing

In 2019, there were no important mergers in the field of TMT. The only merger that was somewhat connected to electronic communications was between ALSO Holding AG, which owns Latvian registered companies, engaged in the provision of computer programming services and the wholesale of computers, their peripherals and software, and Solytron Bulgaria OOD, a company active in the wholesale of information and communication technology.

In 2018, the key TMT field merger was between SIA Bite Latvija, SIA Stream Networks and SIA LATNET SERVISS.\textsuperscript{132} Bite Latvija is a public mobile operator, while the core business of Stream Networks and the LATNET group is the provision of telecommunications and IT services over the fixed network.

ii Sector trends

When analysing sector trends, focus should be directed at the security issues regarding both cybersecurity and the information space. Those issues were highlighted, for example, in the decision regarding the temporary blocking of Rossia RTR channel and the following debates on the legality of their statements regarding the newly elected President of Latvia,\textsuperscript{133} as well as the declarations by the Security Police, Central Election Commission and other institutions regarding the Parliamentary elections. On 18 June 2019, the NEMMC demanded additional amendments to the EMMC, which would change the way in which the NEMMC may derogate from the country of origin principle and restrict the retransmission and distribution of programmes in the territory of Latvia.\textsuperscript{134}


\textsuperscript{130} Information available at https://www.lsm.lv/raksts/zinas/latvija/saeima-sagaida-aktivu-neplp-ricibu-konflikta-risinasana-latvijas-radio.a326686/.

\textsuperscript{131} Information available at www.sam.gov.lv/satmin/preview/?cat=433&action=print&.

\textsuperscript{132} Decision of the Competition Council No. 6 of 29 March 2018.


Also important are the disagreements between NEMMC and the public media\textsuperscript{135} regarding issues of media independence and the competence of the NEMMC as well as the discussions regarding the financial future of the public media. Some of the issues could be solved by the new Law on Media, which should be actively debated in Parliament this year.

Additionally, the communications companies are strongly focusing on the creation of 5G network infrastructure. Noteworthy is the cooperation between two telecommunications companies Bite and Tele2, which have agreed to share the network infrastructure.\textsuperscript{136} This partnership is expected to boost the 5G network development process, benefit the economies in Latvia and Lithuania and also enable companies to increase service quality and optimise each party’s network infrastructure maintenance and development costs. This agreement is the first of its kind in the Baltic region and currently it is under the scrutiny of the regulators.

\section*{VII \hspace{1em} CONCLUSIONS AND OUTLOOK}

In the field of media, the actual implementation of a decision that the public media will exit the advertisement market from 2021 is being discussed. This decision has already created severe financial challenges for the public media. It is necessary to find a permanent source of financing that would not depend on the political situation and would not make the media vulnerable.

Additionally, it is yet not known how the disagreements between the public media, politicians and the NEMMC, as well as the crisis of trust in the Latvian Radio, will turn out.

In addition to that, Latvia must strike a careful balance between protecting its own information space and avoiding accusations about censoring the Russian media.

\textsuperscript{135} Information available at https://www.lsm.lv/raksts/zinas/latvija/mediju-eksperete-rozukalne-neplp-sevi-diskreditejusi.a327519/.

I OVERVIEW

An effective innovation system, which would encourage the growth of an innovative economy, is seen by the Lithuanian government as a strategic objective. Lithuania is focused on the development of high-level scientific knowledge, scientific research, experimental development, as well as fostering innovative business, intersectoral business cooperation and technology transfer.

Lithuania is particularly strong in the health and biotechnology area (worth about 1 per cent of the GDP), where the government is continuously committed to provide support. Photonics is another advanced area in Lithuania, where 700 specialists are employed in the laser industry. In fintech, with the support of the Lithuanian Bank, Lithuania is experiencing the emergence of many new pilot projects, such as the Fintech Sandbox, Blockchain Sandbox, Open Banking Sandbox and Energy Sandbox.

Advancement in the aero cosmic field, particularly driven by the successful launch of the first Lithuanian nano satellites, inspired the government to adopt the Aerocosmos development programme for 2016–2020.

Information technology sector production in Lithuania is close to €2 billion, which to a large extent is driven by software engineering, programming and consulting services, where over 31,000 IT specialists (18,100 software developers) are employed (about 2.3 per cent of the total workforce in Lithuania). Business service centres established by Barclays, Dassebank, WesternUnion, SEB, skandia, Paroc, Swedbank and Euromonitor international account for a large portion of the IT workforce in Lithuania.

Electronic communication market revenue grew by 0.5 per cent in 2018. At the end of 2017 there were 4.3 million active mobile communication subscribers (149 per cent of the total Lithuanian population). The internet is used by almost 80 per cent of the population, and average broadband speeds are 50MB/s with fast public WiFi.
The use of electronic governance services in Lithuania grew to 48 per cent of the total residents. In the area of electronic governance Lithuania ranked in 11th place in Europe in 2017.8

II REGULATION

i The regulators

Electronic communications is one of the most regulated technology areas in Lithuania. The Law on Electronic Communications (LEC)9 transposes the EU regulatory framework for electronic communications. On the basis of the LEC further government regulations have been adopted to regulate certain more technical or more detailed issues of the framework.

The Communications Regulatory Authority10 is the main regulator in the electronic communications area, and is also responsible for adoption of a number of delegated legal acts, as well as supervisory measures (market review, imposition of measures for entities with significant market power, etc.).

The LEC applies to electronic communication services, the definition of which is equivalent to the EU Framework Directive, public communication networks, universal services, as well as governance of electronic communication resources (frequencies, numbering plan). The law also contains provisions on privacy in electronic communications, transposing the e-Privacy Directive.

Information society services are regulated by the Law on Information Society Services,11 transposing the Directive on electronic commerce, which is based on non-discrimination, technological neutrality, functional equivalency and other principles. Liability exemptions for transmission service, caching service, and hosting service providers are established, without imposing a general obligation for providers to monitor stored or transmitted information.

Media services are regulated by the Law on Provision of Information to the Public (LPIP).12 The law establishes the procedure for collecting, producing, publishing and disseminating public information and the rights, duties and liability of producers and disseminators of public information, their participants, journalists and institutions regulating their activities. The law establishes licensing and notification requirements for broadcasting (TV, radio) organisations, limitations on ownership, requirements for media content, programme composition, language, advertising restrictions, ethics, etc.

The media area is supervised by an independent regulatory authority – the Radio and Television Commission (RTC).13 The RTC is responsible for licensing of radio and television broadcasting and rebroadcasting activities, notification procedures, approval of ownership transfers, monitoring and supervision of content control, and advertising requirements.

---

9 Latest English version: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/05cd4e020f0a11e7b6c9f69dc4ecf19f?jfwid=-502q00eth.
10 Website: https://www.rrt.lt/en/.
11 https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.277491/FGVmSopPwK.
13 Website: https://www.rtk.lt/en/.

© 2019 Law Business Research Ltd
Other regulatory bodies that may exercise supervision over ECS providers pursuant to their competence include (not exhaustively) the State Consumer Rights Protection Authority, the State Data Protection Inspectorate, the Competition Council, and the Inspector of Journalist Ethics.

ii Main sources of law

The main sources of law in the field of electronic communications are the Law on Electronic Communications, the Law on Information Society Services and the Law on Provision of Information to the Public.

More detailed regulations are contained in the specific regulations issued by the Communications Regulatory Authority or the government, for example, Order No. 1V-340 of the Communications Regulatory Authority regarding General Terms on Engaging in Electronic Communication Activities and Order No. 1V-125 of the Communications Regulatory Authority on Allocation of Spectrum for Broadcasting Radio and Television Programmes.

iii Regulated activities

Under the LEC, the provision of public communication (fixed, mobile and over electricity networks) networks or services, as well as public satellite communication networks and services is subject to a prior notification obligation. The notification form is publicly available on the website of the Communications Regulatory Authority (CRA).

All public communication service providers who engage in the provision of public communication networks and services, dedicated lines, internet access, data transfer services, television (satellite, cable, multi-channel microwave, digital terrestrial, IPTV) services, cable radio services, optical fibre network services, and TV and radio transmission services are subject to quarterly reporting obligations. The reporting form is publicly available on the website of the CRA, which can be submitted electronically.

There is no requirement for communication service providers to be established or registered locally.

RFs are assigned by the CRA in accordance with the approved national plans. They can be assigned directly to the applicant, or by way of a public auction (e.g., in case of mobile communications networks). Telephone numbers are distributed according to the national numbering plan.

The RTC is responsible for licensing of radio and TV broadcasting and rebroadcasting activities. Licences are required for radio and TV broadcasting via terrestrial stations or networks, cable networks, multi-channel microwave networks, and networks the main purpose of which is not radio or TV broadcasting. Broadcasting via websites or web portals is not subject to licensing. Other broadcasters or subscription media service providers are subject to notification requirements.

Ownership and market access restrictions

In Lithuania, there are no general ownership restrictions for communication services providers. However, where national radio spectrum is allocated via public auction, participants usually are required by the CRA to comply with European and transatlantic integration criteria (i.e., entities must be established in countries of the EEA, EFTA, OECD or NATO).

The Law on Companies having Strategic Importance for National Security recognises information technology and telecommunications and other high technologies as economy sectors having strategic importance for national security. When an investor in this sector acquires ownership of more than one-quarter of the entity of the strategic sector, this acquisition must be notified to the Commission on Coordination of Security for Objects of Importance for National Security.

Radio and TV broadcasting licence holders may be owned by entities, who comply with certain restrictions. Licence holders cannot be owned by state or municipal institutions, governmental organisations, companies owned by the government or municipalities, banks, and political parties. Licence holders must also comply with reputation requirements (i.e., absence of criminal convictions for management or owners). Licence holders can be owned only by entities established in the EU or NATO, and which had no relations with entities or governments outside the EU or NATO that would pose a threat to national security.

Local and regional public information disseminators (newspapers, journals) must report their ownership to the RTC.

The telecommunication, media and technology sectors are also subject to general concentration controls from the perspective of competition law. In certain cases, an acquisition transaction may require notification and approval from the Competition Council.

In general, Lithuanian law does not limit market access, except for the limitations specified above.

Transfers of control and assignments

Telecommunication service providers are usually not subject to ownership change notifications or approvals.

A change in the ownership of at least 10 per cent in the radio or TV broadcasting licence holder requires prior consent from the RTC. Prior to the ownership change, the licence holder has to apply to the RTC for consent and provide all information required to prove the reputation and origin of the new owner. Consent is granted usually within one month. In the event a concentration permit is required from the Competition Council, the consent is only issued after the permit is granted by the Competition Council.

The Commission on Coordination of Security for Objects of Importance for National Security reviews notifications regarding compliance of the investors with the restrictions of the Law on Objects having Strategic Importance for National Security and must adopt its conclusions within 15 days after receipt of notification.
III  TELECOMMUNICATIONS AND INTERNET ACCESS

i  Internet and internet protocol regulation

The LEC does not contain rules dedicated specifically to internet or IP-based services. Certain electronic communication services, which are based on IP technology (e.g., VoIP), are subject to the same regulatory regime as other public access telecommunication services. For example, services that include inbound and outbound call services qualify as equivalent to public access telecommunication service, and the same legal and regulatory regime applies to such services. Call services provided via PSTN, ISDN based on IP, coaxial based on IP, STP or UTP based on IP, FTTP based on IP, GSM technology based fixed line services all qualify as substitute services by the CRA.

The CRA is supervising the implementation of Regulation (EU) 2015/2120 on open internet access and the BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.17

Information society services (other than electronic communication services) are subject to the regulation of the Law on Information Society Services, which is based on the principles of technological neutrality and non-discrimination. Information society service providers are required to provide the following directly and permanently accessible information to the recipients of the service:

- the name of the service provider;
- the service provider's registered address;
- contact details, including the electronic mail address;
- the register, where the service provider is registered, and registration number;
- supervisory authority; and
- VAT payer code.

If reference is made to the fee charged for the service, information on whether the fee includes taxes and delivery charges must be provided.

Information society service providers who engage in information transmission (mere conduit), caching and hosting service provision are exempt from liability for the information transmitted. Additionally, such information society service providers are not required to monitor information upon the mere transmission thereof or provision of access thereto, temporary storage thereof in cache memory or storage thereof at the request of the recipient of the service, nor is the service provider obligated to actively seek facts or circumstances indicating illegal activity. However, these information society service providers are required to remove illegal content once they are notified by the right holders or those affected by the illegal information.

ii  Universal service

In Lithuania, universal electronic communication services include provision of a subscriber line, internal calls and foreign calls, and call-box stations. Universal services are provided by Telia Lietuva, AB, a fixed-line communication service provider.

iii Restrictions on the provision of service

Price regulation

In Lithuania, the CRA has imposed price limitations to certain providers for universal services, for call termination in public access telephone services, wholesale line rental services, wholesale local fixed access services, wholesale central access for massive market products, mobile call termination services, and broadcasting transmission services.

Access

Communication network service providers have to provide access to their infrastructure in cases where the user of infrastructure cannot implement its right to electronic communication infrastructure, or where the costs of such implementation would be disproportionately high. The network operator is required to conclude the agreement with the user of the infrastructure following the principles of non-discrimination and transparency.

Contracts with consumers

The Lithuanian Civil Code (Article 6.161) qualifies public communication service contracts as public contracts (i.e., public communication service contracts have to be concluded with any customer who applies for the services, where it is technically possible to provide the service). Service providers may not refuse to conclude contracts or to provide discriminatory terms to certain groups of customers. Standard terms on electronic service contracts are controlled by the general contract law provisions as well as specific terms in the LEC.

Net neutrality

Regulation (EU) 2015/2120 laying down measures concerning open internet access is directly applicable in Lithuania. Thus all communications service providers in Lithuania are under the obligation to treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.\(^{18}\) Observance of net neutrality and open internet access is supervised by the CRA.

Unsolicited phone calls, faxes, emails and texts

Lithuania has implemented the e-Privacy Directive 2002/58/EC\(^{19}\) in the LEC. The LEC provides the same requirements regarding marketing communications for natural as well as legal persons. Under the LEC, the use of electronic contact details of a natural or legal person for direct marketing is allowed only with the person's prior consent (opt-in).

If a communications service provider obtains the electronic contact details (email, phone number) of a customer, who is a natural or legal person, in connection with selling a product or providing a service, such contact details may still be used for direct marketing of its similar products to the customer if the customer is given, upon the initial collection of

\(^{18}\) Articles 3 and 4 of Regulation (EU) 2015/2120.

electronic contact details and each time when the buyer’s electronic contact details are used for direct marketing, a clear and distinct opt-out opportunity free of charge and in an easy manner; and the customer is allowed to exercise its right to refuse over an ECN.

The exemption described above does not apply to voice calls, or calls placed with automated calling machines.

iv Security
Lithuania adopted the Law on Cyber Security in 2014, which was recently amended to implement EU Directive 2016/1148 (the NIS Directive). The law provides for the requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities’ network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents.

The LEC provides the obligation for network service providers to retain certain electronic communication data for at least six months, for the purpose of investigation of serious crimes.

As of 25 May 2018, the General Data Protection Regulation (GDPR) has been applicable in Lithuania. This was also of extreme importance in the communications sector, as the general rules set out in the GDPR are also applicable in the communications sector. In addition to the GDPR, Lithuania still has the Law on Legal Protection of Personal Data as amended to comply with the GDPR.

In addition to the GDPR and the Law on Legal Protection of Personal Data, some data protection requirements are also set out in the LEC, in particular related to e-Privacy Directive implementation.

Minors are protected by the Law on Protection of the Underaged from Negative Impact of Public Information, which applies to TV, radio content, as well as advertising, trademarks, computer games and other public information.

IV SPECTRUM POLICY

i Development
The CRA has approved a number of plans for development of radio spectrums (3,410–3,600GHz, 380–385MHz, 390–395MHz, 220–2,300MHz, 2,500–2,690MHz, 2,300–2,400MHz, 3,600–3,800MHz and 790–862MHz).

There is a list of spectrum approved by the CRA, which can be used without authorisation.

Recently the government decided to open the spectrum at 700MHz, which will be used for 5G communication.

The 4G network was developed in Lithuania from 2014.

ii Flexible spectrum use
There is a list of spectrum approved by the CRA, which can be used without authorisation.

21 https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/VCRunrZydD.
iii Broadband and next-generation mobile spectrum use
Spectrum for mobile networks is traditionally made available by auction to three operators. Recently the government decided to open the spectrum at 700MHz, which will be used for 5G communication. It is expected to be launched by 2020.

iv Spectrum auctions and fees
The latest spectrum auction was held in 2015 for 880–915MHz, 925–960MHz, 1,710–1,785MHz and 1,805–1,880MHz, where the frequencies were assigned to three MNOs in Lithuania.

The next auctions for developing 5G are likely to be for spectrum around 700MHz.

V MEDIA
i Restrictions on the provision of service
Censorship
Censorship of public information is prohibited in Lithuania. In order to ensure freedom of information, the LPIP prohibits exerting pressure on the producer or disseminator of public information, their participant or a journalist, compelling them to present information in the media in an incorrect and biased manner. The producer, disseminator of public information, their participant or a journalist shall have the right to keep the confidentiality of the source of information and not to disclose it, except where a court orders such disclosure.

Restriction
The LPIP prohibits publication in the media of information that:

a incites to change the constitutional order of the Republic of Lithuania through the use of force;

b instigates attempts against the sovereignty of the Republic of Lithuania, its territorial integrity and political independence;

c spreads war propaganda, instigates war or hatred, ridicule, humiliation, instigates discrimination, violence, physical violent treatment of a group of people or a person belonging thereto on grounds of age, sex, sexual orientation, ethnic origin, race, nationality, citizenship, language, origin, social status, belief, convictions, views or religion;

d disseminates, promotes or advertises pornography or propagates or advertises sexual services and paraphilias;

e promotes or advertises addictions and narcotic or psychotropic substances;

f is slanderous and offensive to a person or degrades his or her honour and dignity; or

g violates the presumption of innocence and impedes the impartiality of judicial authorities.

Language requirements
The LPIP requires public information to be produced and disseminated in the state language. Radio or television programmes that are broadcast in a language other than Lithuanian must be translated into Lithuanian or shown with Lithuanian subtitles, except for educational, occasional, special, music and rebroadcast foreign radio or television programmes or parts of programmes as well as programmes produced by broadcasters of radio or television
programmes intended for the ethnic minorities of Lithuania. Broadcasters of television programmes are prohibited from showing audiovisual works that have been translated from an official EU language into a non-EU language. When rebroadcasting television programmes, rebroadcasters or other persons providing services of dissemination of television programmes or individual programmes via the internet for Lithuanian users must give priority to the official EU languages.

**EU content**

Broadcasters of television programmes must, where possible, reserve more than half of the television programme time remaining after deducting the time allocated for news, sports events, games and advertising programmes, teletext services and teleshopping for European works. Broadcasters of television programmes must, where possible, reserve at least 10 per cent of the television programme time remaining after deducting the time allocated for news, sports events, games, advertising programmes, teletext services and teleshopping for European works created by independent producers not earlier than within the past five years.

**Advertising restrictions**

Advertising and audiovisual commercial communications must be decent, correct and readily recognisable. It is prohibited to publish in advertising and audiovisual commercial communications information that degrades human dignity, promotes any discrimination based on race, sex or ethnic origin, nationality, citizenship, religion or belief, disability or age, or contains manifestations or promotion of sexual orientation, is offensive to religious or political convictions or promotes behaviour prejudicial to health or safety or behaviour grossly prejudicial to the protection of the environment.

Advertising of tobacco and alcohol products and audiovisual commercial communications intended for advertising of tobacco and alcohol products is prohibited.

The total time of television advertising spots and teleshopping spots within a given hour must not exceed 20 per cent.

**ii Internet-delivered video content**

Besides television services, on-demand audiovisual media services are becoming increasingly popular. On-demand audiovisual media services do not require a licence, but do require a notification to be submitted to the RTC.

Most of the biggest TV channels in Lithuania have started their own video distribution services. Internet news portals are also including video publications as part of their service.

**VI THE YEAR IN REVIEW**

The most important changes in the legislation concerning the ICT sector in 2017 and 2018 are the GDPR and the Law on Cyber Security.

The GDPR became applicable on 25 May 2018, and required companies to adjust their data processing and gave people a greater control over the use of their personal data.

The Law on Cyber Security was updated to implement the Networks and Information Security Directive 2016/1148.

Significant recent transactions include the acquisition of previously Viasat-owned TV channels (TV3, TV8).
In March 2017, it was also announced that the Swedish media holding Modern Times Group had signed an agreement to sell its Baltic businesses to the US Providence Equity Partners. The value of the transaction was approximately €115 million. The transaction concerned the sale of three TV channels in Lithuania (TV3, TV8 and TV6), five TV channels in Latvia and three in Estonia. The sold entities form the third-largest commercial television operator in the Baltic region, nationwide commercial radio stations, digital assets and an online advertising consultancy operating across the Baltic region.

VII CONCLUSIONS AND OUTLOOK

Generally, Lithuania follows the European policies and has successfully implemented the various pieces of EU legislation into national law.

It is likely that the government will continue its policy of supporting key technology areas.

In the telecommunications sector, the most important development in the upcoming year should be the development of the 5G network.
Chapter 12

LUXEMBOURG

Linda Funck

I OVERVIEW

The Luxembourg TMT sector has evolved from being predominantly a provider of voice services into a diverse, competitive and interconnected industry using terrestrial, satellite and wireless transmission systems. Today, Luxembourg has first-class infrastructure and telecommunication networks and is counted among the top locations for electronic communication services and infrastructures. In the 2018 edition of the Global Competitiveness Report (GCR Report) published by the World Economic Forum, Luxembourg is listed (after Singapore) second out of 140 countries with regard to agility and future readiness, and Luxembourg’s steady upward trend relating to its overall score is recognised.\(^2\)

The ICT development index 2017, when analysing the introduction of ICT and the potential for ICT-related development, ranked Luxembourg ninth out of 176 countries.\(^3\) Luxembourg ranked sixth out of the 28 EU Member States in the latest edition of the Digital Economy and Society Index (DESI) published in June 2019 by the European Commission (EC), and is considered to be a high-performing country.\(^4\)

Traditionally, the sector was limited to a very few players. Telecommunication and postal services were operated for several decades as a public monopoly of the state-owned Entreprise des Postes et Télécommunications (EPT).\(^5\) The radio and television sector was controlled and developed from its early years by a privately owned company. Indeed, the first radio broadcasting in Luxembourg was initiated by the founders of the current broadcaster, CLT-UFA. The privately held operator was ensured a leading role in the national and international development of the radio and television sector, and today RTL Group ranks as the top television and radio broadcaster in Europe. Luxembourg has also been a pioneer in non-terrestrial communication technology. SES-Astra (SES), a Luxembourg-based company created in 1985, was Europe’s first private satellite operator, and today SES has global standing.

The presence of important market players in the TMT and TMT-related sectors in Luxembourg and the related know-how and experience have led the government to make efforts to maintain, create and further develop its electronic telecommunication technologies with the aim of being among the best places in Europe and abroad to do business within the sector and being a hub for e-services in Europe. This aim has been constantly pursued

---

1 Linda Funck is a partner at Elvinger Hoss Prussen.
4 ec.europa.eu.
5 The new commercial name is Post Luxembourg.
and reaffirmed by the government since 2010 until 2019. The government together with a group of private investors has set up a fund dedicated to ICT start-ups named the Digital Tech Fund. The GCR Report confirms the success of these efforts, as Luxembourg is in ninth position in relation to its product market. According to the DESI of the EC, Luxembourg is ranked second among all European Union countries with regard to its connectivity and third with regard to its human capital.7

Luxembourg combines many features that are beneficial to the development of an ICT sector, including the diversity and multilingual skills of the population and workforce, a geographical location in the centre of Europe and an important financial industry in need of high-performance communication technologies. In addition, Luxembourg has gradually developed state-of-the-art digital infrastructure, international telecommunication connections (offering fast and reliable connectivity to other European cities at very low latency rates), efficient national communication networks, performant data centres, a comprehensive, evolving and innovative legal framework, cutting edge research, and safety and security, all of which contribute to Luxembourg’s increasing attractiveness to technology organisations and electronic communication services, but also to financial institutions, companies active in biotechnology and medicine, and other e-businesses. Luxembourg figures among the top locations for ICT infrastructure (data centres, high-speed connectivity and internet traffic, low latency internet) and it offers specialised expertise to keep data safe.

The presence of regulated ICT support professionals of the financial sector, who are subject to the same confidentiality obligations as banks, provides considerable comfort and security to clients in the financial sector in areas such as the outsourcing of IT functions.

More recently, Luxembourg has been focusing strongly on the development of the fintech industry, for which Luxembourg is very attractive as it combines a huge range and variety of financial services, performant and innovative technology and open-minded regulators, public authorities, private players and associations who are ambitious to follow and develop a sector that is evolving rapidly and that is omnipresent in the overall global economy. Luxembourg as a hub for financial services offers an ideal environment for fintech companies to develop their services and expand their business. In fact, many start-ups have chosen Luxembourg to develop fintech activities from compliance and risk management, through blockchain and cryptocurrency, security and authentication, automated investment services, big data analytics, to mobile and e-payments.8

The quality of the communication infrastructure has led numerous actors in the gaming sector (online video games) and gambling sector to set up their headquarters in Luxembourg.9 Global brands in the media and internet world such as Amazon, eBay, PayPal, Vodafone Procurement, Intelsat, RTL Group, Milicom, Fanuc (robotics and computer numeric control) and Skype all have European headquarters or major operations in Luxembourg.

The presence of Level 3 in Luxembourg (one of the most important operators of telecommunication services at the level of the backbone internet) confirms Luxembourg as a centre of excellence in the internet sector. Luxembourg is also attractive to a number of e-payment and e-money services institutions and can be considered as Europe’s e-payment hub.

---

6 Information and communication technologies.
9 Big Fish Games, Bigpoint, Innova, Valve.
hub, with brands including Digicash, Amazon Payments, Mercedes Pay SA, Yapital, Six Payment Services, Rakuten, Wordline and Mangopay all based in Luxembourg. Several software giants including Microsoft, Symantec and Open Text also have places of business in Luxembourg.

Luxembourg also has a strong reputation for service availability, security and data protection, and responsive and open-minded authorities.

The CSSF, Luxembourg’s financial sector supervisory commission, has granted Bitstamp a payment institution licence, and has made the company the first nationally licensed Bitcoin exchange. There are many other companies active in the virtual currencies sector that want to establish themselves in Luxembourg and that are currently trying to obtain their licence, confirming once more the attractiveness and open-mindedness of Luxembourg for ICT businesses.

Luxembourg has a longstanding official policy of welcoming pan-European companies in addition to creating the appropriate framework for the development of local businesses, and offers multiple opportunities to start-ups by creating an environment that allows existing market players to come into contact with young entrepreneurs. For example, the House of Start-Ups is hosting the Luxembourg city incubator, a project conducted by the Luxembourg Chamber of Commerce, and currently supports a large number of innovative start-ups in a variety of industry sectors. In 2019, the House of Start-Ups has hosted the Luxembourg House of Financial Technology, the City of Luxembourg Incubator, the Hub@Luxembourg and the International Climate Finance Accelerator Luxembourg.10

In 2018, the proportion of employees in the ICT sector in relation to the total number of employees is 5 per cent, which constitutes the fifth-highest proportion in the European Union (the average in the European Union is only 3.7 per cent).11

Efforts are also being made in ICT research, with a focus on the security, reliability and trustworthiness of ICT systems and services.12 In the context of increasing the influence of digital technologies in every aspect of our lives and throughout all business areas, and with the further and constantly evolving development in cloud computing and e-archiving, digital security is a key element of the success of the digital economy. Important improvements are being made to the legislation in order to adapt the national legal framework to overcome barriers related to the use of new technologies.

Luxembourg joined forces with other European countries and started planning in 2016, in cooperation with the EC, France, Spain and Italy, an European super-calculator, allowing private and public players access to top-notch software tools. The declaration of European cooperation in the context of high performance computing (HPC) was signed by Luxembourg Minister of Economy on 23 March 2017, which marked the official start of the collaboration between the signatory countries (Luxembourg, Germany, Spain, Italy, Portugal, France and the Netherlands). These countries have joined forces to implement the strategy of a European HPC network, of which the Grand Duchy is the initiator.13 Indeed, Luxembourg

10 www.host.lu/.
12 Interdisciplinary Centre for Security, Reliability and Trust (SnT), Computer Science and Communication.
hosted the first meeting of the EuroHPC Joint Undertaking in November 2018.14 In the context of the HPC, Luxembourg has been given a leading role in the Driveless cars: The Future Smart Mobility made possible by High Performance Computers project.15

Luxembourg is highly present at European-level discussions and negotiations and stout in its defence of its position in the global process of harmonisation and liberalisation, while supporting the direction of European regulation. At a national level, research and development in the ICT sector is conducted by a number of government-promoted institutions.16 In developing its communication networks in the context of the investment realities and opportunities in the telecoms and media sector, the challenge is to direct investment in a way that ensures that the right type of network is built and that public investment works in cooperation with the private sector so as to promote a more competitive telecoms environment. The government has actively taken part in the discussions regarding the Data Protection Regulation17 (GDPR) adopted on 14 April 2016, which came into force the 25 May 2018. In addition, separate national legislation been adopted in August 2018 in relation to the entering into force of GDPR.

The development of the information society is one of the key priorities of the government. In addition to the aforementioned policies, it has created an action plan called e-Luxembourg with the ultimate goal that Luxembourg administrations, corporations, education personnel and individuals may efficiently use and have access to electronic communication means to help improve their quality of life. Today, many filings, registrations and requests to public administrations (such as those of the tax, social security and energy sectors) can be made online. In 2017, the government launched administrative online platforms such as eHealth to facilitate the possibility of carrying out administrative procedures electronically via online applications.18

The government has adopted a GED system (electronic document management) and banned the use of paper with the aim of streamlining internal government structures so as to become more cost-effective. Luxembourg has also introduced electronic identity cards. The government is very keen to actively assist and encourage Luxembourg small and medium-sized companies to develop and enhance the digitalisation of their businesses and operations, and to familiarise them with such digitalisation so as to increase the productivity, competitiveness and sustainability of their enterprises.19 In that context, a Digital Skill Bridge Programme has been created to enable businesses and their employees to get support regarding the possibilities that digitalisation may offer. To promote Luxembourg as a European logistics hub, a Single Window Logistic Programme has been introduced that shall simplify and digitalise relations between all actors in the logistic chain and thus increase efficiency and competitiveness.

In 2014, the Council of Government announced the launch of a new strategy, Digital Luxembourg, which focuses on developing high-level ICT infrastructures, facilitating the regulation and flow of data, promoting digital competences, modernising online administration and creating an innovative ecosystem. The Digital Luxembourg platform aims

16 For instance, the Luxembourg Institute of Science and Technology (LIST).
19 Fit 4 Innovation financed by the Ministry of Economy is one of the initiatives.
to assemble private players and public institutions and foster inter-sectoral and cross-sectoral interaction. Recognising the continual need for a workforce with strong IT skills, Luxembourg has implemented the Digital (4) Education strategy. The first WebForce3 school, which aims to train people in a very short time to allow them to become qualified for a developer or junior integrator job, has been implemented.20 The school is part of the Fit4coding initiative launched by the government and co-financed by the European Social Fund. Other initiatives such as Start to code, Open Class Room and the House of Training assist in education and providing digital skills in technology.

In the context of Digital (4) Education and the effort to raise awareness of the importance of technologies at a very early stage, high schools innovating in ICT have been able to use the Future Hub label since 2017. For this purpose, college students participated in the International Computer and Information Literacy Study (ICILS) 2019 in order to assess their IT skills. The aim is to make students aware that technologies will be an integral part of their future whatever sector they might be working in and to raise interest in those subjects. A Luxembourg Tech School has also been launched. The Ministry of Education, Children and Youth is currently also updating the infrastructure of all high schools to provide high-speed internet through fibre. Luxembourg ranks third out of the 28 EU Member States in the ‘Women in Digital Index 2018’ attesting to the effectiveness of government ‘Women in Digital Empowerment’ (WIDE) initiatives that actively support girls and women in the acquisition of digital skills.

Luxembourg is also aware of the need for skills from outside Luxembourg, and in a view of recruiting IT skills from abroad, the government has adapted its legislative framework so as to facilitate the obtaining of residence permits for highly skilled individuals.

Luxembourg strongly encourages the development of a Digital Single Market, as it will strengthen Luxembourg's position within the European area. The government is involved through various organisations in the discussions and adoption of regulations and directives at EU level, such as notably the Single Digital Gateway Regulation 2018/1724, which entered into force on 2 October 2018, electronic cards for services and the Single Market Information Tool.

In addition, the government is fully aware of the fact that the continuance of the success and the competitiveness of Luxembourg's financial sector will depend, inter alia, on the availability of cutting edge services based on fintech.21 A fintech working group has been established with representatives from different associations active in the financial and technological sectors, and it aims to solve and answer specific problems and questions related to fintech. A House of Financial Technology been officially launched on 25 April 2017 as an initiative of Luxembourg for Finance. It is a public-private partnership that established Luxembourg as a European fintech centre by offering start-up incubation and co-working spaces.22

In January 2017, the Secretary of State of the Economy presented the new Creative Industries Cluster Luxembourg, which aims to support the economic development of the sector, and includes activities such as architecture, crafts, visual arts, design, styling, the games industry, marketing and communication, literature, publishing, the performing arts and new media.

21 Financial sector related technology.
Convergence has been achieved by creating rules and regulations, regulatory authorities and consulting entities at the national, European and international levels that embrace the diversity, interconnectivity and interrelatedness of the various industries and players. The increasing convergence between telecommunications, information technology and media has led to the adoption of the regulatory framework that was introduced into Luxembourg law by two laws of 27 February 2011 (Telecoms Package). The Telecoms Package is designed to provide for one set of rules for all electronic communication services and networks. The continuing development of the ICT sector constantly calls for adjustment of the current legislation and regulations at the national and European levels (see Section II).

As a result of convergence, it is extremely important that interconnectivity and free access to all operators and service providers within the TMT sector are ensured in an equal manner. The use of one infrastructure for different types of services is of particular importance, and it is crucial that the operators and owners of the infrastructure or networks make these available to the other participants in the TMT sector. This is particularly true in Luxembourg because of the small size of the market. Constant efforts are made to ensure competitiveness among the players in the TMT sector. Ensuring Luxembourg’s international connectivity is at the top of the agenda for future years, with the aim being ensuring the lowest latency rates with major capitals, the lowest prices and the presence of the most important carriers.

Importantly, the government supports the principles of network neutrality (i.e., keeping a free architecture, open and non-discriminatory terms, guaranteed access without unjustified conditions on ECNs), and has pushed for the adoption of EU Regulation 2015/2120, laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users’ rights relating to ECNs and ECSs, and Regulation (EU) No. 531/2012 on roaming on public mobile communications networks within the European Union, which was finally adopted on 25 November 2015 during Luxembourg’s presidency of the European Union Council. This Regulation is seen as major achievement for the Digital Single Market.

Competition among incumbent operators and alternative operators remains an important element for e-industry players.

II REGULATION

TMT services cover an extremely wide scope of technology and services, with different laws and regulations applicable that entail various regulatory authorities to supervise different services and related technology. The competent ministry in Luxembourg for the telecommunication and media industry is currently the Ministry for Communication and Media.

i Regulators and regulated activities

The Law of 1997 created the Luxembourg Institute of Telecommunications (ILT), whose duty is to supervise and regulate the telecommunications sector. In 2000, the tasks of the ILT were widened to encompass the Luxembourg energy sector and postal services and, as a consequence of the Law of 1997, it was renamed the Luxembourg Institute of Regulation (ILR).23 The scope of the ILR’s tasks has been modified on several occasions, and for the

23 www.ilr.lu.
last time by the Laws of 27 February 2011 and 26 July 2011. The ILR is an independent regulator and is not funded by public state funds paid for by taxpayers, but is rather financed by the operators of the sector supervised and regulated by the ILR.

The Electronic Communication Law and the Spectrum Law clarify the allocation of competences between the Minister for Communication and the ILR in different sectors. The ILR is entitled to set rules in accordance with European directives and national law. Additionally, it controls the efficient use of infrastructure for the benefit of consumers. It is entitled to determine the fees and conditions under which communication networks are operated and services rendered so as to allow the formation of a competitive market. It also has the authority to draw up reports and proposals, which it must submit to its board and the government. It gives advice, and prepares statistics and regulations. It also hosts important events such as the 4th meeting of the Body of European Regulators for Electronic Communications (BEREC) held on 15–16 November 2018.24

The ILR is competent to receive notifications, and to grant authorisations or licences in relation to the provision or operation of electronic communication network services, and assists the competent minister in the allocation of licences for radio spectrum. It is also in charge of establishing the plan for frequencies and updating the public registers required by law for the various TMT sectors. It has the power to issue administrative sanctions against operators that breach laws or regulations. It may also act as a dispute settler between competing operators, and as mediator between customers and operators.25 In 2018, the ILR received 129 mediation requests with more than 90 per cent of these concerning the field of electronic communication services.26

The ILR is not empowered to monitor and regulate abuses of dominance. It is, however, responsible for ensuring that dominant players do not exclude other competitors from the sector, and it may take measures and issue rules to ensure a competitive market if, in its opinion, proper competition is no longer possible.

Regarding media, the Media Law (as defined hereafter) was amended by the Law of 27 August 2013. The government commissions existing under the former law (i.e., Communication Media Service, Independent Radio Broadcasting Commission and the National Programming Council (CNP)) have been replaced by one single authority: the Luxembourg Independent Audiovisual Authority. Its main responsibilities are to:

a ensure service providers’ compliance with the law;

b grant or withdraw broadcast permits;

c ensure access to audiovisual programmes for persons with a visual or hearing disability;

d stimulate on-demand audiovisual media service providers to promote and distribute European works;

e encourage audiovisual media service providers to elaborate codes of conduct concerning the broadcast of inappropriate content; and

f impose sanctions on non-compliant service providers such as fines, withdrawal of permits, warnings and suspension of transmission.


26 ILR annual activity report 2018 of the mediation service.
The National Commission for Data Protection (CNPD), initially created by the Law of 2 August 2002 on the protection of individuals with regard to the processing of personal data (repealed following the entering into force of GDPR) and governed by the Data Protection Law, is the authority in charge of the supervision of the electronic communication market as far as data protection issues are concerned.

The CNPD controls the processing of personal data in Luxembourg and ensures compliance with the data protection regulations, in particular those relating to the confidentiality and security of processing operations. In addition, it has advisory competence towards the government. The CNPD participates in numerous conferences and contributes to the activities undertaken by the European Data Protection Board such as the European Commission’s assessment adequacy decision of Japan related to international transfers of personal data. Although the CNPD is a public institution, it enjoys independence in carrying out its mission.

It has investigative competence that allows it direct access to data of processing operations. As an investigative body, the CNPD is allowed to issue administrative sanctions. Since the entry into force of the GDPR in 2018, the CNPD is responsible for monitoring its application to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union. The CNPD’s powers have been enhanced and it is, inter alia, able to impose fines of up to 4 per cent of a company’s worldwide turnover, and derives powers from both the GDPR and Luxembourg-specific legislation for residual matters (e.g., the recently adopted Luxembourg Data Protection Law).

The TMT sector is extremely broad and diversified. Due to the specifics of the various industries on the one hand and their interrelatedness on the other, it appears that laws and regulations apply to more than one specific service within the TMT sector, resulting thus in a large amount of applicable legislation and regulations.

The main laws are as follows:


b) the Law of 11 April 2010 on freedom of expression in electronic media, amending the Law of 8 June 2004 (as amended) on the freedom of expression in the media sector;

c) the Law of 27 February 2011 on electronic communication services and networks (Electronic Communication Law), abrogating the Law of 30 May 2005 on electronic communication services and networks (Former Electronic Communication Law) as amended for the last time by a law of 27 June 2018;

d) the Law of 30 May 2005 as amended by the Law of 27 February 2011 on organisation and management of radio spectrum (Spectrum Law);

e) the Law of 30 May 2005 regarding the organisation of the ILR as amended (most recently by a law of 19 June 2015);

f) the Law of 30 May 2005 on the specific provisions regarding the protection of individuals as to the processing of personal data in the electronic communication sector and amending Articles 88-2 and 88-4 of the Criminal Instruction Code and as amended for the last time by a law of 27 June 2018;

the Law of 14 August 2000 on electronic commerce as amended (Electronic Commerce Law);

the Law of 18 April 2001 on copyrights as amended (Copyright Law);

the Law of 1 August 2018 on the organisation of the CNPD and the general data protection regime (Data Protection Law);\(^{29}\)

the Luxembourg Constitution;

the Law of 11 August 1982 on privacy (Privacy Law);

Article L222-12 to L222-23 of the Consumer Code regarding distance contracts on financial services, abrogating the Law of 18 December 2006 on distance selling of financial services;

Article L222-2 to L222-11 of the Consumer Code;

general laws are applicable to all aspects not specifically regulated by specific laws or regulations, and in particular the provisions of the Luxembourg Criminal Code (LCC) (e.g., in relation to pornography, discrimination, racism, violence, theft and piracy) and the commercial code with the amended Article 567 (See Section VI.i);

the Law of 2 April 2014, amending, inter alia, the Consumer Code, Electronic Data Protection the Law and Electronic Commerce Law (2014 Law);

the Law of 18 July 2014 on cybercrime,\(^{30}\)

the Law of 25 July 2015 on electronic archiving as amended by the Grand-Ducal Regulations of 21 September 2017 on the execution of Article 4 Section 1 of the Law and on the dematerialisation and conservation of the documents (Electronic Archiving Law);

the Law of 22 March 2017 on measures to reduce the cost of deploying high-speed electronic communications networks;

the Law of 7 June 2017 on electronic communication services and networks;

the Law of 27 June 2018, amending, inter alia, the Criminal Procedure Code, the Law of 30 May 2008 and the Electronic Media Law (2011 Law);

the Law of 22 February 2018 on the exchange of personal data and information in policy matters;

Bill of Law No. 6763 modifying the Criminal Procedure Code and Electronic Data Protection Law;

the Law of 1 August 2018 relating to the protection of individuals as to the processing of personal data in criminal matter and for national security measures;

the Law of 28 May 2019 relating to the implementation of the Directive on security of network and information systems (NIS Directive);\(^{31}\) and

the Law of 28 May 2019 on public websites and mobile applications accessibility of public sector entities.

In addition, a large number of Grand-Ducal regulations and other regulations (particularly from the ILR) have been adopted in relation to the implementation of the various laws.

\(^{29}\) The GDPR harmonises the applicable data protection law and the Luxembourg legislator has adopted relevant legislative texts to cover matters where Member States retain a certain level of autonomy.

\(^{30}\) See Section III.iv, Cybersecurity.

\(^{31}\) The Directive on security of network and information systems (EU) 2016/1148.
ii Ownership and market access restrictions

Luxembourg rules and regulations do not, in principle, impose ownership restrictions within the TMT sector, except in certain specific sectors. Regarding telecommunications services, the previous authorisation regime has been replaced by a less stringent notification regime.

There are no ownership restrictions for being granted a concession to operate Luxembourg satellite systems or broadcast a Luxembourg programme via satellite or cable except that for the latter, a broadcasting licence may only be granted to a legal entity incorporated under Luxembourg law.

Because spectrum is considered a rare resource, its management and use is reserved to the state. Licences to use spectrum may, however, be granted to third parties subject to the conditions of national legislation, related regulations, or international or European agreements and treaties.

There is no specific national regulation on cross-ownership of media companies. However, general laws on competition still apply.

iii Mergers and acquisitions

There is no specific Luxembourg authority regulating mergers and acquisitions in the TMT sector. The ILR’s competences are to guarantee competitiveness on the Luxembourg TMT market, and as such it will monitor acquisitions and mergers in the sector so as to evaluate their position on the market ex post.

The Law of 23 October 2011 on competition, which prohibits restrictive agreements and abuses of dominant position, provides for an independent authority, the Council for Competition Matters (CCM), which is in charge of investigating cases, consultative missions and sectoral inquiries (or investigating types of agreement). The Investigation Division for Competition Affairs has been abolished. The CCM is also a decision-making body and exercises various powers for the execution of its mission (i.e., finding and sanctioning legal violations, drafting opinions, undertaking market studies, gaining information about companies and executing missions allotted to the CCM). Decisions by the ILR in relation to regulation of competition must be taken in agreement with the CCM. None of the relevant authorities has ex ante powers; nor may they prevent mergers or acquisitions.

III INTERNET AND IP-BASED SERVICES

i Internet and internet protocol regulation

Internet services were regulated, prior to the Electronic Communication Law, by the Law of 21 March 1997 relating to telecommunication services and the operation of telecommunications networks (Law of 1997).

Even though the Law of 1997 did not provide for specific internet or internet protocol regulations, but covered telecommunications services and networks more generally, in
the absence of the express exclusion of internet services and in light of the definition of telecommunication services and networks, internet services were considered to be governed by this Law.

The Electronic Communication Law introduced certain changes, widened the scope of existing regulation to a larger range of communication technologies, and introduced the definitions of electronic communication network and electronic communication services, as opposed to telecommunication services. The new terminology reflects the increased scope of the services and networks that are regulated. Express reference to internet services is made.

Neither the Law of 1997 nor the current Electronic Communication Law provide for any specific rules applicable to internet services or IP-based services as opposed to traditional telephony services, except that due to the specific nature of the telephony services, certain additional rules apply to the provision of telecommunication services that are offered to the public. The Electronic Communication Law provides for certain specific obligations applying to publicly available telephony services and public telephone networks. These specific regulations are to ensure a universal service to the resident population and apply only to traditional telephony.

As previously noted, the ILR is the competent regulator in charge of the supervision of the services rendered both in relation to internet services and traditional telephony services. The operation or provision of electronic communication services or networks is subject to notification to the ILR. No distinction as regards the notification requirement is made between traditional telephony and internet or IP-based services, other than details on the differences of the various services notified. To the extent the definition of electronic communication services can be broad, there are circumstances where a follow up might be of interest, as certain case-by-case exemptions do apply. Although no licence is required, notified entities are subject to a certain number of formalities and filings, and have to pay an administrative fee.

The Electronic Communication Law provides for a global legal framework applicable to all electronic telecommunication services and networks, with certain specifics depending on the type of service or network, ensuring, however, that the whole sector is consistently governed by the same legislative and regulatory national framework.

### ii Universal service

The development of communication infrastructure in Luxembourg is among the top priorities of government programmes in the information and communication technology field. The government has been developing the broadband infrastructure services for approximately 10 years.

Since the end of 2011, Luxembourg has had 100 per cent standard (fixed) broadband coverage (DSL up to 25Mbps) available to all Luxembourg households. Similarly to neighbouring countries, there is a trend of increased use of fixed lines provided via IP and a

---

32 The abrogated Law of 1997 provided for a definition of telecommunication services and telecommunication networks, with telecommunication having been defined as ‘each transmission, issue or reception of signals, images, sounds or data of any nature, by wire, radio, by optical or by electromagnetic means’.

33 Articles 11 and 12 of the Electronic Communication Law.

34 Article 5 of the Electronic Communication Law.

35 Luxembourg 2011 Telecommunication Market and Regulatory Developments.
reduction in the number of standard fixed lines. Operators in France have decided to provide for a withdrawal of standard fixed lines, and it is very likely that this might also happen in Luxembourg. In 2019, NGA\textsuperscript{36} reached 98 per cent (compared to a European Union average of only 83 per cent of the households),\textsuperscript{37} and 4G broadband availability in Luxembourg reached around 99 per cent in urban and rural areas.\textsuperscript{38} Luxembourg residents are very connected (92 per cent are internet users).\textsuperscript{39}

The installation of the optical fibre has made constant progress since 1997, and Luxconnect,\textsuperscript{40} the city of Luxembourg and EPT are joining the efforts to cover the whole territory with optical fibre under the ‘national ultra-high speed network strategy – ultra-high speed network for everyone’. FTTH, using fibre optic cable, is further progressing, and 60 per cent\textsuperscript{41} (+3 per cent since 2017) of all Luxembourg households are connected to FTTH per statistics of the ILR as of 30 June 2018.\textsuperscript{42} In addition to work being carried out on the deployment of optical fibre throughout the country, efforts are also being made on the existing networks to increase the broadband speed. The Grand Duchy is connected through 27 different fibre routes to the main internet exchange hubs in Europe: Frankfurt, London, Paris, Brussels, Amsterdam and Strasbourg, with particularly low-latency rates between 4 and 8 milliseconds.\textsuperscript{43}

The ILR statistical report confirms the continuing trend of Luxembourg’s population to subscribe to high-speed broadband. According to an analysis of OpenSignal,\textsuperscript{44} Luxembourg ranks 19th in the world in terms of performance: the average speed in the country is 29.61Mbps.

In Luxembourg, a notable market trend towards bundled offers (broadband mobile or fixed telephony and TV) continues. At the end of 2017, 81.8 per cent of all internet access services were commercialised with at least one other service.\textsuperscript{45} Luxembourg benefits from an extremely developed FTTH architecture.

An ultimate aim of the government is to provide households and businesses with downstream speeds ranging up to 1GB/s and upstream speeds of 500Mbps in 2020. EPT and other alternative operators offer ultra-high speed internet access.

iii Restrictions on the provision of service

Pursuant to the Electronic Data Protection Law and GDPR, ISPs and operators of electronic communication services and networks are compelled to ensure the confidentiality of communications exchanged by way of electronic communication means. The general rule is that other than the user, no person is allowed to listen to, intercept or store communications and data relating to the traffic and location without the agreement of the user.

\begin{itemize}
\item[36] NGA (VDSL, data over cable service interface specification 3 cable and FTTP).
\item[38] https://ec.europa.eu/digital-agenda/en/scoreboard/luxembourg.
\item[40] Luxconnect was created at the initiative of the government.
\item[43] www.surprisinglux.com/#page=did-you-know.
\item[45] ILR statistical report 2017, p. 37.
\end{itemize}
This prohibition does not apply to communications relating to emergency calls, commercial transactions to the extent that they constitute proof of the transactions, or authorities investigating and acting in relation to a flagrante delicto act or within the scope of criminal offences to ensure national and public security.

A regulation adopted on 14 December 2017 provides for the conditions and limitations of any permitted interceptions.

In relation to data resulting from commercial transactions and cookies, the user or parties to a transaction must be informed that their data may be processed, the conditions (in particular the duration) and aim of the storage, and the possibility of the user opposing such data processing. The use of cookies can only be carried out with the express consent of a user. The user must have a real choice and no risk of deception or negative consequences if he or she chooses not to give his or her consent.

For the purpose of criminal law enforcement, specific conditions must be met to have recourse to intercepted communications data. In addition, for the purpose of research, monitoring and pursuit of criminal offences, and with the sole aim of providing relevant information to the judicial authorities, each ISP or operator must store traffic information and locational data for a period of six months. The Law of 24 July 2010 has amended the scope of criminal offences by limiting the possibility of only consulting the data that relates to criminal offences resulting in penal sanctions of more than one year’s imprisonment. The Grand-Ducal Regulation of 24 July 2010 relating to traffic data and localisation data determines the category of traffic data that may be useful for the research, observation and prosecution of criminal offences, as well as the manner pursuant to which such information is made available to the authorities. The Law of 28 May 2019 implementing the NIS Directive provides legal measures to further enhance and strengthen the level of cybersecurity.

Intellectual property theft and piracy are regulated by the Copyright Law, the LCC, the Privacy Law, the Electronic Data Protection Law and the GDPR.

There is currently no public authority in Luxembourg that exercises global supervisory or monitoring power over the content and traffic data of network operators, ISPs and users, as this would violate the essential privacy principles.

Similarly, and for the same reasons, network operators may not control the content, application and services accessed by their network users.

The practice of deep packet inspection is prohibited in Luxembourg, as it infringes confidentiality rules and constitutes an invasion of privacy in complete violation of the above-mentioned legislation. The same analysis would apply to the filtering of data processed by means of electronic communication means.

However, network operators, data centre operators and professionals of the financial sector are obliged to comply with the secrecy or confidentiality requirements, and to avoid invasion of privacy, piracy or intellectual property theft, to take appropriate technical and organisation measures, and to have systems and procedures (firewalls, encryption, secured and restricted access, etc.) in place that render the network and data processing via their network secure.

46 Articles 309, 460, 488, 505, 509-1 and following of the Luxembourg Criminal Code.
iv  Security

National security

The Electronic Communication Law, the Electronic Communication Data Protection Law and the Data Protection Law provide for specific applicable measures to ensure national interests.

In certain circumstances, where national security (including public health and public order) is endangered, the government may requisition the entire electronic communication network established in Luxembourg, as well as the connected equipment, or prohibit the provision of some or all electronic communication services.

To maintain access to the emergency services, the government may also dictate special conditions for the use of electronic communication services and networks. Although storage of personal data is generally prohibited, the Electronic Communication Law provides for an exception in relation to storage of traffic data relating to emergency calls or inspection of false alerts or attacks or abusive calls.

The Law of 23 July 2016, as amended by the Law of 28 May 2019, creating a High Commission for national protection, attributes special powers to this High Commission to prevent, anticipate or manage crises and their effects, and consequently encourage the return to a normal state. For example, the protection of critical infrastructure includes all activities aiming to prevent, attenuate or neutralise the risks of a reduction or discontinuity of services essential to the protection of vital interests or personal needs for all or part of the country or its population.

Furthermore, following the recent terrorist attacks, a law on the exchange of personal data and information in police matters was adopted on 1 August 2018.

Finally, the Law of 7 June 2017 abolished anonymous prepaid SIM cards for mobile phones. Mobile operators will have to deactivate prepaid SIM cards with a Luxembourg number whose holders have not yet been identified. Consequently, they will have to collect certain data in relation to the identification of their clients before activating the purchased prepaid cards.

The Law of 28 May 2019 relating to the implementation of the Directive on security of network and information systems (the NIS Directive) creates a computer security incident response teams (CSIRTs) network to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation.

Privacy and consumer protection

Privacy and consumer protection in the electronic communication domain is guaranteed by both the Consumer Code and the Media Law. They set guidelines and restrictions in relation to commercial advertisements and specific provisions for the protection of children.

Information about consumers must be treated confidentially and may not be rendered accessible to third parties, and the processing of consumer data is allowed only if it falls within the criteria defined by the relevant laws. Processing of data is subject to the principle of legitimacy of processing.

Luxembourg law prohibits in principle the addressing of advertisements or other unrequested communications to persons by electronic means without their consent. In
any event, the consumer shall be able to object. If the supplier of a product received email addresses during a previous sale, he or she can use those email addresses to promote analogous products and services unless the concerned persons request such actions to be stopped.47

Specific Luxembourg provisions related to certain sectors (e-payment, financial services concluded or offered via electronic means) apply when a contractor and a prospective client conclude transactions or receive services over the internet or other mobile means that do not necessitate direct human contact.

The e-Privacy regulation that is currently being negotiated at the EU level will further enhance consumer protection, as will the contemplated European Electronic Communication Code.

Protection of children

There is no specific legislation or regulation that ensures the protection of children online.

In 2011, Luxembourg ratified the United Nation Convention in relation to children’s rights and the Convention of the Council of Europe concerning protection of children against exploitation and sexual abuses, and is involved in the implementation of their provisions.

Moreover, the government is issuing a number of recommendations and supporting various projects to make children and their parents aware of the risks related to the use of the internet. The BEE Secure project was drawn up in the context of the EU Safer Internet Programme, which gives directions for the use of the internet to children, parents and educational staff. In this context, the ‘BEE Secure’ provides training that is mandatory for all 7th grade classes in Luxembourg’s secondary schools. Luxembourg is the only country in Europe that has introduced mandatory training for safe internet use within the education system.48

Generally, the policy is to familiarise children with new technology rather than filtering or blocking access to various types of information (which might, however, be an alternative); the intention is to teach children how to use the internet safely and to always be aware of the risks related to such use.

Children’s rights are protected by provisions of the Luxembourg Criminal Code (LCC). Further to the adoption of the Law of 21 February 2013 amending Articles 372 and 377 of the LCC, the LCC provides for enhanced sanctions in relation to sexual child abuse matters. BEE Secure Stopline is a project operated by a national consortium that provides a structure to report illegal information transmitted over the internet anonymously. The E-commerce Law requires information service providers to withdraw or render inaccessible any illegal content that they become aware of. The Media Law includes specific child protection provisions.

The University of Luxembourg is an active member of the EU Kids Online project, which is a multinational research network seeking to enhance European children’s opportunities and safety, and to minimise risks.49

In relation to the adoption of the 2014 Law, CNP lobbied to introduce an appropriate visual warning obligation. A Grand-Ducal Regulation was adopted on 8 January 2015 for the protection of minors regarding audiovisual media services.

The GDPR establishes enhanced protection for children when it comes to the processing of their data in relation to information society services. The processing of the personal data

47 Article 11 of the Electronic Data Protection Law.
49 www.saferinternetday.org/web/eu-kids-online/home.
of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.\textsuperscript{50}

\textbf{Cybersecurity}

Cybersecurity is one of the priorities of the government. Individuals and companies are encouraged to take appropriate technical measures to defend themselves against cyberattacks.

Similarly to the internet project for children, the government has created CASES Luxembourg, a project that is accessible by all internet users and whose purpose is to make the public aware of potential cyberattacks that are inherent in internet use, and that advises on how to identify potential cyberattacks. In this context it is worth mentioning the certification authority, Luxtrust, which manages electronic certificates with the highest level of security.

Network operators and ISPs are required by applicable law to comply with stringent security measures.

As a response to the increasing number of cyberattacks, the LCC has been amended so as to include offences in the electronic communication sector.

The government pursues efforts to prevent and fight cybercrime, and in 2011 created two dedicated structures: the Luxembourgish Cybersecurity Board (CSB), whose mission is to work on a strategic plan against attacks via the internet; and the governmental computer emergency response team (GOVCERT), linked to the National Agency for Information Systems Security (ANSSI), which is the competent body to deal with incidents of cybercrime in the public information systems.

GOVCERT also cooperates with the High Commissioner for Protection (HCPN) and the Technology Centre for State Information. Both HCPN and GOVCERT have adopted a cybersecurity plan that has been submitted to the counsel of government. The CSB has determined five priorities (on both the national and international level) on which Luxembourg shall focus,\textsuperscript{51} and has asked a working group to review the national strategy regarding cybersecurity to determine whether any amendments are necessary. Furthermore, the government has signed a letter of intent with Belgium and the Netherlands to cooperate on the prevention of and fight against cybercrime. Luxembourg regularly hosts conferences on cybersecurity that are mainly dedicated to experts in security matters.

The CSB acts as a central point of information and contact for users to report cybersecurity incidents, which should allow the CSB to supply businesses with such information and put them in a position to take appropriate action to fight risks against security.

The Computer Incident Response Center Luxembourg, which is the official computer emergency response team (CERT) of Security made in Lëtzebuerg (SMILE), is competent for the private sector, municipalities and non-governmental entities in Luxembourg.

After the delay in the implementation of the European Council Convention on Cybersecurity (CCC) and Directive 2013/40/EU relating to attacks against information systems, a law relating to cybercrime was adopted on 18 July 2014. Such law adapts the national substantive and procedural criminal law to the specific needs of fighting cybercrime. The law introduces certain new criminal offences into the LCC, including in particular the misuse of identity, phishing and illegal interception of computer data, supplementing the

\textsuperscript{50} Article 8 of the regulation (EU) 2016/679

\textsuperscript{51} Ministry of State: National Cybersecurity Strategy.
legal instrument of computer-related crimes, which include the illegal access, hacking and deletion of computer data. The law also amends the Criminal Procedure Code to achieve the requirements of the CCC regarding the prompt preservation of stored computer data and traffic data.

ANSSI, which is responsible for the security of the information systems for the public sector and critical infrastructures, was created in 2015. Further, SECURITYMADEIN.LU, launched in 2015 by SMILE, is an initiative with the objectives of coordinating governmental initiatives, and supporting and making the public more aware of cybersecurity issues. In addition, SECURITYMADEIN.LU aims to develop an ecosystem for cybersecurity that will reinforce the visibility of Luxembourg information security players and services. SECURITYMADEIN.LU and the activities of SMILE are an integral part of the national strategy that intends to position Luxembourg as a trusted ICT centre.52

In May 2016, the government announced a collaboration between the new national agency of the security of information systems and SMILE through their respective CERT53 in relation to all activities in connection with the detection, management and notification of incidents.

Given the importance of international cooperation on cybersecurity at an EU level, the NIS Directive establishes that CSIRTs should be able to participate in international cooperation networks in conjunction with national authorities.

Furthermore, the eIDAS Regulation will enable an appropriate security level for electronic identification means to be reached, and consequently enhance security for e-businesses and electronic communication services.

In October 2017, a national centre of expertise in regard to cybersecurity in Luxembourg was created, helping to strengthen the positioning and the economic attractiveness of the country for undertakings in the ICT sector.54

Within the framework of the European Cybersecurity Month, an annual advocacy campaign organised by the European Union Agency for Network and Information Security and the EC whose aim was to promote cybersecurity internationally, the Cybersecurity Week-Luxembourg, took place in October 2019.

Luxembourg is fully aware that security in the increasingly high technological environment is an important pillar to continue to be successful in a data-driven economy. Luxembourg participates in initiatives and programmes that aim to share information on cybersecurity-related subjects for instance through MONARC and MISP (malware information sharing platform and threat sharing).

The International Telecommunication Union (ITU) Global Cybersecurity Index (CGI) ranked Luxembourg seventh in Europe and 11th in the world in its latest edition highlighting the commitment of Luxembourg to cybersecurity and its climbing in the leader board.55

**Emergency response networks**

Traditionally, Luxembourg first responders and other emergency responders (such as police, customs and civil protection) benefit from a dedicated network. This network, RIFO, was

53 www.gouvernement.lu/6037806/30-cybersecurite-anssi.
580725845061e01abe83a969.
55 Global Security Index (CGI) 2018.
still analogue. With the adoption of the Law of 20 May 2014 as amended by the Law of 1 March 2019 for the financing of a national integrated radio communication network for Luxembourg, RIFO was replaced by RENITA. RENITA is based on the terrestrial trunked radio digital technology and, in the case of a congestion of mobile networks, the RENITA network is less exposed to inherent risks. RENITA has been operational since July 2015.

On an international scale, the government has actively cooperated on strengthening emergency telecommunications and rapid responses in the event of disasters. It has developed a nomadic satellite-based telecommunication system, emergency.lu, which aims to assist humanitarian agencies to respond to communities affected by natural disasters, conflicts or protracted crises.\(^{56}\) As of 2012, this platform was available as a public global service. At the end of 2014, the emergency.lu solution was extended for a period of six years by the government.\(^{57}\) At the beginning of 2018, the government decided to join the European Response Coordination Centre, and Luxembourg will be the first state to bring in a common module to the voluntary pool.

At an EU level, harmonisation of the digital frequency relating to these services has been achieved, thereby permitting interoperability. Consultations on the usage of 700MHz frequency band raised RENITA’s interest in Luxembourg.

### IV SPECTRUM POLICY

#### i Development

The increasing development of wireless communication, media and information technology also affects spectrum policy in Luxembourg.

The need for radio spectrum has increased significantly over the past few years, and Luxembourg actively participates in the elaboration of a pan-European spectrum policy and favours a more flexible and efficient use of spectrum.

In its contribution paper to the EC in 2010, Luxembourg indicated that it is in favour of a more flexible use of spectrum, emphasising however that it is crucial that the more flexible use will not negatively impair the current quality of services or entail harmful interferences. Luxembourg has expressed its concern that a more flexible use would need to take into consideration the characteristics of more specific and sensitive technology, which would be more prone to harmful interference than others.

During the negotiations that led to the adoption of the European regulatory framework, Luxembourg explained that one of its top priorities was to maintain national competence in relation to the management of spectrum and a full subsidiarity in this area.

#### ii Flexible spectrum use

As a result of the Law of 27 February 2011 amending the Spectrum Law, allocated licences are no longer personal.\(^{58}\) On that account, it is currently possible to sell, transfer or sublease allocated spectrum, thus enhancing the flexibility of spectrum use. The Spectrum Law also provides for the possibility of spectrum sharing.

The mobile use of spectrum dedicated to fixed use is possible as a matter of applicable law and regulations, and is in line with the principle of technological neutrality.

### iii  Broadband and next-generation mobile spectrum use

According to the 12th edition of the eGovernment benchmark of the EC, fixed high speed internet is accessible by 100 per cent of the population of Luxembourg, compared with 97 per cent for the rest of the European Union. Regarding new-generation high speed internet (>30Mbps), 98 per cent of the Luxembourg population is covered compared with only 83 per cent in the other EU Member States.  

In Luxembourg, the increasing need for spectrum for the offer of increasing broadband services is partly solved by opening additional frequencies or releases of spectrum for the use of broadband and next-generation mobile services.

Luxembourg completed the switch-off of analogue television broadcasting in 2006, which was replaced by DTTV. The released spectrum (referred to generally as the first digital dividend) is used for next-generation mobile services.

The ILR adopted a new frequency plan on 13 August 2018. The new frequency plan takes into account the following recent decisions: EU 2017/899 concerning the 470–790MHz frequency band, EU 2018/637 concerning the 900MHz and 1,800MHz frequency bands, and decision EU 2018/661 of 26 April 2018 amending decision (EU) 2015/750 of 8 May 2015 of the EC on the harmonisation of the 1,452–1,492MHz frequency band for terrestrial systems capable of providing ECSs in the European Union.

In October 2011, Luxembourg concluded an agreement with its neighbouring countries regarding reducing the risks of interference due to overlapping coverage in the frequency band 790–862MHz. Additional agreements were entered into in May 2017 with the administrations of Belgium, France, Germany, Switzerland and the Netherlands with respect to frequency usage and frequency coordination in border areas. Another multilateral agreement between France, Germany, Switzerland and Luxembourg was concluded in 2014 concerning the allotment of preferential frequency blocks in the 406,100–410,000MHz band to ensure equal spectrum access in the respective border areas. A bilateral agreement was signed with Germany regarding Luxembourg and Germany’s common approach on dealing with the 470–694MHz and the 694–790MHz frequency bands. A similar bilateral agreement was signed with France in 2016.

The licences within the 900MHz band have been renewed to the existing operators and one new operator, and the use thereof has been expanded to different technologies. These licences allowed the introduction of 4G technology in Luxembourg specifically (LTE). In addition, the three operators have spectrum in the 1,800MHz band, allowing flexibility for the introduction of innovative new technologies.

Following a public consultation launched in July 2016 for frequency band 2.1GHz, EPT, MTX Connect Sà rl, Tango and Orange will each be allocated 14.85MHz in the 2.1GHz band to be used by no later than 1 January 2020.

At a European level, the EC has adopted a decision to make more spectrum available for mobile services in the 700MHz band (694–790MHz) by 2020 to allow the provision

---

of high-quality internet to users, whereas the sub-700MHz area (470–694MHz) will remain available, as a priority, for audiovisual services.\textsuperscript{60} This development is in line with the deployment of 5G, foreseen as from 2020.

In August 2017, the ILR launched a public consultation to establish interest in the 700MHz band, and the possible use thereof and quantity needed to cover mobile services, security and emergency services. Three interested parties have responded (one of which, RENITA, is in charge of the emergency call network) and expressed their interest in obtaining broadband in that frequency, in particular with a view to the upcoming introduction of the 5G network. Two consultations were opened in May 2019 to establish the criteria allowing the competent Minister to issue rights-of-use of 3,400–3,800MHz and 700MHz bands.\textsuperscript{61}

European telecommunication ministers have signed the common Making 5G a success for Europe declaration, and they envisage the deployment of the 5G network between 2018 and 2025, with the aim to cover major cities and major transportation routes by 2025.\textsuperscript{62} On 12 September 2018, Prime Minister Xavier Bettel presented the 5G strategy for Luxembourg, whereby Luxembourg’s vision is to be among the leaders in 5G. Indeed, the Luxembourg government wants to launch several pilot zones in Luxembourg to enable a timely deployment of 5G.\textsuperscript{63}

\textbf{iv} Spectrum auctions and fees

Given the small size of the market and the limited number of operators, the experience of the authorities shows that allocations of spectrum through auctions or beauty contests do not produce satisfactory results. Hence, although theoretically possible as a matter of law, auctions are not currently practised.

The Spectrum Law provides for various procedures for the allocation of spectrum licences such as competitive selection, comparative selection or by a public bidding procedure for the best offeror. The competent minister will determine the applicable procedure on a case-by-case basis after having undertaken a public consultation and publish this decision in the Luxembourg Official Gazette and in the EU Official Journal at least one month prior to the launch of the procedure.\textsuperscript{64}

The fees payable to the state (as owner of the national spectrum) for the allocated spectrum are determined by a Grand-Ducal Regulation of 21 February 2013 on royalties for radio frequencies.\textsuperscript{65} The Spectrum Law has modified the allocation and recovery of the fees payable in relation to spectrum licences in favour of the ILR. Public services and authorities are not subject to the payment duty to the extent that spectrum is used for the provision of services within the scope of national defence, public security or emergency services.

\begin{itemize}
  \item \textsuperscript{60} \url{http://europa.eu/rapid/press-release_IP-16-207_en.htm}.
  \item \textsuperscript{61} \url{https://web.ilr.lu/FR/Professionnels/Frequences-radioelectriques/Consultations}.
  \item \textsuperscript{62} Government activity report (March 2018) p. 9.
  \item \textsuperscript{63} \url{https://www.luxinnovation.lu/event/luxembourg-5g-conference-2/}.
  \item \textsuperscript{64} Article 6 of the Spectrum Law.
  \item \textsuperscript{65} Grand-Ducal Regulation of 21 February 2013 on royalties for radio frequencies.
\end{itemize}
V MEDIA

i Restrictions on the provision of service
The Media Law has been amended several times, with the most recent amendment having taken place in January 2018. The Law aims to cover all types of audiovisual and sonorous media. High importance is attributed to content regulation, protection of children, non-discriminatory content, and the form and content of commercial advertising.

ii Internet-delivered video content
It is difficult to measure the importance of internet video distribution in Luxembourg given the absence of surveys or statistics on this phenomenon. The only indicator is the fact that, as in most other Western countries, people watch less traditional TV, which seems to indicate that internet video is becoming more popular, particularly with the younger public. Given the general availability of cable and satellite TV, the impact so far has been minimal. In addition, based on the high connection rates of Luxembourg residents to the internet, it should be expected that this move will not pose dramatic problems for consumers.

VI THE YEAR IN REVIEW

i Key legislation
Luxembourg is the first state in Europe to adopt a legal and regulatory framework ensuring property rights to private companies owning space resources by adopting the law of 28 July 2017 on the exploration and use of space resources (Space Law).

Given the growing interest of various actors to develop space activities, Luxembourg is working on a bill of Law No. 7317 on space activity which would go beyond the matters covered by the Space Law. Such new law would, inter alia, submit all Luxembourg space activities to prior authorisation, and thus would allow Luxembourg to accede to the Convention on Registration of Objects Launched into Outer Space of 1974 by creating a register of Luxembourg space objects.

Given the ‘Europeanisation’ of the legislation, national laws tend to be more and more linked to European regulations or directives. One major challenge is the recent entering into force of the GDPR, which has an impact on a large number of businesses. Luxembourg actively cooperated with other European countries on the implementation of the GDPR through its participation in the Article 29 Working Group, and continues to do so in relation to the implementation through its presence on the newly created European Data Protection Board (replacing the Article 29 Working Group), which is working on the guidelines for the implementation of the new provisions of the GDPR. Furthermore, in October 2018, Luxembourg signed the protocol of amendment to the Convention on Automatic Processing of Personal Data (Convention 108) of the Council of Europe.

In the era of the development of internet payment services, in which one of the main challenges remains compliance with know-your-customer requirements, Luxembourg has adopted a regulation that provides for lighter identification requirements for transactions.

66 Information in this section has been largely drawn from the government’s annual reports (latest available, 2017).
67 Activity report of Luxembourg government, p. 18.
below certain threshold amounts. The law of 13 February 2018 amended a relevant portion of the Luxembourg anti-money laundering law to include the lighter identification requirements under certain conditions.

EU Regulation 2015/2120, which definitely abolished roaming charges in June 2017, resulted in enhanced competition among operators and created attractive offers for consumers. This is of particular importance to Luxembourg residents, given the small size of the Luxembourg territory.

The government’s ongoing efforts in its Digital Letzebuerg strategy, launched in August 2014, and Digital (4) Education strategy, launched in May 2015, evidences the government’s efforts to continue the development of the ICT sector with the aim of making and keeping Luxembourg a high-tech centre of excellence. Luxembourg’s creation of an easier procedure through the adoption of a law of 8 March 2017 for highly qualified persons to get a residence permit shows its willingness to attract talents to the country.

In the context of the adoption by the EC of the Intellectual Property Package, Luxembourg is working on a bill of law and has also adopted a new law on the Benelux Convention relating to intellectual property. In a period where innovation is key to the success of society, businesses and prosperity, it is important that adequate protection is granted to innovators.

Focusing strongly on innovation, the Luxembourg legislator adopted a law on the promotion of research on 17 May 2017, renewing the current regime applicable in Luxembourg in R&D.

ii Key mergers and takeover activity

No major takeover activity has taken place over the past six months, but the actors in the ICT sector have taken the opportunity to develop their activities and services in the respective areas of predilection in the light of new technologies (cloud, e-archiving, roaming, digital payment services, etc.).

VII CONCLUSIONS AND OUTLOOK

The digital economy is an important Luxembourg pillar, and is a top priority of the government. Luxembourg is considered to be located in the middle of the Golden Ring.68 Continuing efforts are made to favour the development of new communication and information technologies. The development of international connectivity and security in the current context remain key priorities. Digital Letzebuerg’s ongoing actions and initiatives show the government’s commitment and awareness of the importance of the ICT sector and ICT-related services. The development of fintech services is strongly supported by many market players and the government.

The Grand Duchy reinforces its position as a European hub for the exploration and use of space resources as it continues to pursue its path towards innovation and constantly search for new opportunities. Luxembourg’s launch of a space research initiative in 2016 and the adoption of the Space Law shall ensure that private operators working in space can be confident about their rights to the resources they extract in outer space shows how progress-oriented Luxembourg is and will continue to be. The newly created Luxembourg
Space Agency is actively working on projects from which various industries may benefit. The space activities sector will certainly be one of the areas where Luxembourg will focus on specifically, given its history in the satellite industry.

In the satellite sector, SES has continued to expand its fleet of satellites, offering a global connectivity covering 99 per cent of the world’s population. It is investing in new onsite infrastructures. SES has ordered seven ultramodern satellites to increase its services starting from 2021. SES wants to enter into the new connectivity area with O3b mPower, the next-generation MEO system allowing SES to establish the world’s most powerful satellite based-communications system. For this purpose, SES launched four additional O3b satellites in 2019, and more launches are planned until the end of 2021 with the aim of expanding its activities in Europe, Asia and South America. The broadcasting of ultra HD content is another SES priority. SES is part of a 16-member consortium that has been tasked with integrating satellite into 5G networks, enabling ubiquitous and instantaneous 5G coverage and capacity.

SES supports the EC’s action plan for the deployment of 5G in Europe, and strongly believes that Europe has the potential to become the global leader in 5G, permitting the enablement of economic growth, sustainability and high-quality jobs. In this context, SES invests in multi-orbit capabilities in GEO and MEO to address the massive bandwidth growth expected in 5G networks and in the revolutionary O3b mPOWER next-generation satellite system, which are expected to be launched in 2021.

Furthermore, SES has signed a partnership agreement with the LIST that will allow cooperation through their international network of research partners with unique expertise in satellite communications, and widening the scope of SES’s international research activities together with other reputable universities. The new partnership agreement further enhances Luxembourg’s technology ecosystem by attracting start-ups to develop their businesses in Luxembourg, and will facilitate the transfer of new technologies stemming from national public and private research.

In partnership with the European Space Agency (ESA), SES established QUARTZ, a quantum cryptography telecommunication system that is a new platform aimed at providing a global service for next-generation encryption keys for use in geographically dispersed networks. Luxembourg and ESA have also signed a joint statement on future activities concerning related technologies and space exploration.

Government policy also aims at further promoting ICT-related infrastructure (data centres, etc.) as one of the pillars of the economy. The government is continuing to invest heavily in the security of the networks and infrastructures as one of the main pillars of the development of the electronic communication systems. As of January 2017, Luxembourg, with its eight Tier IV data centres, had 40 per cent of the total number of Tier IV data centres

73 https://infrachain.com/.
in Europe, Tier IV being the highest level possible for a data centre with very high security and availability standards.\textsuperscript{74} Discussions are underway between the government and Google for the creation in Luxembourg of one of the biggest data centres.

In June 2017, Luxembourg signed an agreement to establish Estonia’s first ‘data embassy’ with the aim of storing sensitive data for the Estonian government on servers in the Grand Duchy. This innovative legal framework ensures the security and non-violation of its premises and data. This again shows how innovative Luxembourg is.

Recently, a collaborative initiative co-funded in July 2019 by the Luxembourg Space Agency and Spire Global Luxembourg aims to launch an open source data lake so that Luxembourg is now home to one of the world’s largest data lakes for space data analytics, which is accessible free of charge to all start-ups, research institutes and public agencies in Luxembourg.\textsuperscript{75}

The creation of various structures at the national level evidences the government’s priority to prevent and combat cybercrime and other attacks on electronic communication services and infrastructures.

The continuing development of the online video games sector in Luxembourg and the establishment of internationally known companies such as Nexon and Valve Corporation are encouraging LU-CIX, Luxembourg’s commercial internet exchange, to develop its services. The government has renewed previous efforts to establish efficient technical infrastructures and a business-friendly legal environment to assure the best development possible for these companies in Luxembourg.

The government, through its competent organ, has continued its ICT promotion efforts, and visited various countries and states in 2017 and 2018. A Luxembourg delegation continues to travel to various countries to show the government’s support and interest, and promote Luxembourg start-ups. In July 2018, the Digital Tech Fund signed an agreement with artificial intelligence computing leader NVIDIA was a focus on skills training. This new cooperation will strengthen Luxembourg’s digitalisation efforts and will make Luxembourg an even more attractive place for the developing of machine-learning and deep-learning technology.\textsuperscript{76} Following this agreement, the Luxembourg government and NVIDIA announced the creation in January 2019 of an artificial intelligence joint research laboratory. In this context, LIST researchers could work very efficiently in areas of innovation that require high-performance computing such as 4.0 industry, finance, RegTech, environmental and driverless vehicles.\textsuperscript{77}

In addition, two buildings in the House of BioHealth have been made available for start-ups active in the health field in Luxembourg.\textsuperscript{78} Luxembourg actively takes part in the promotion of CleanTech. To reduce negative ecological impacts and optimise the use of the earth’s natural resources, Luxembourg supports the development of CleanTech innovators such as APATEQ, a Luxembourghish company focused on oil–water separation systems, wastewater treatment and water conservation solutions.\textsuperscript{79}

\textsuperscript{74} www.innovation.public.lu/en/decouvrir/pourquoi/secteursinnovants/finance/index.html.
\textsuperscript{75} https://meco.gouvernement.lu/fr/actualites.gouvernement.
\textsuperscript{77} https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2019/01-janvier/30-bettel-partenariat-nvidia.html.
\textsuperscript{78} Luxembourg 2020, Plan national pour une croissance intelligente, durable et inclusive.
Luxembourg has also participated in various conferences organised in Luxembourg and throughout the world.

Luxembourg hosts the annual ICT spring conference. In 2019, the conference was organised around four different themes: fintech, artificial intelligence and digital transformation, space and cybersecurity. The conference attracted approximately 5,000 attendees.

The Infrachain project (a common blockchain infrastructure project), launched in 2016, is also moving in the right direction. A non-profit organisation putting in place Community-driven governance for blockchain use was incorporated in May 2017, showing the interest of various actors in that technology.

Luxembourg is keen to take advantage of the growing demand for high performance infrastructure bandwidth capacity and the connectivity needs of the e-economy. Its geographical location close to the major European cities is a clear advantage. Luxembourg will actively participate in the deployment of the 5G bandwidth both at the national and European levels.

Luxembourg will continue to develop high-standard data centre services and facilities. It had the first green centre worldwide, showing its commitment to research and development into new infrastructure and technologies. Many Luxembourg data centres (eight out of a total of 23 data centres) offer Tier IV design, and most of the other centres are classified Tier III. Luxembourg is actively working on cybersecurity, and participated in the European Data Protection Board. Luxembourg is already hosting the EC’s data processing centres, and at the end of 2016 a new data centre for the EC was been inaugurated in Betzdorf. This centre, according to the former European Commissioner for Digital Economy and Society is a world-class data centre that ensures a modern, reliable and economic IT infrastructure for the EC.80

Besides the importance of developing networks and guaranteeing security, the government and its partners are aware that the long-lasting and efficient development of the digital economy requires e-skills, and it is thus active in promoting ICT businesses to students. Awareness of training opportunities and carriers in the ICT sector is one of the areas of development of the digital economy in Luxembourg (e-skills project) and goes hand in hand with the new Digital (4) Education strategy. Children, students and teachers are, for instance, granted free access to Office 365, an environment proposing platforms and computer applications to satisfy administrative and educational needs for the national education. MathemaTIC has also been created, which proposes a digital mathematical learning environment for children.

BEEcreative is another initiative of the Ministry for Education, constituting a place of discovery and creation intending to stimulate the creativity of the next generation.

A pilot project launched in 2016 resulted in the new Luxembourg Tech School.81

The entry into force of the Law of 28 May 2019 which implemented the NIS Directive will have an impact on the national legislative framework, and Luxembourg is keen to count itself among the countries that can ensure very high standards in terms of security.

Finally, the eIDAS Regulation entered into force in July 2016, enhancing security for e-businesses and electronic communication services.

---

I OVERVIEW

The state monopoly carrier was privatised in 1990. Five years later, the sector was liberalised, a new law was issued and a new regulator established. Although for more than 15 years there was some progress and the sector was growing each year, there were major problems to tackle.

In 2012, the OECD published a study that described the weakness of the telecommunications sector in Mexico and recommended the implementation of different actions to foster the market. The study presented the following market shares:

- 80 per cent of Telmex in fixed telephony;
- 70 per cent of Telcel in mobile telephony;
- 45 per cent of Televisa in pay-TV; and
- 28 per cent of Megacable in pay-TV.

The report also stated that the penetration rates for fixed line, mobile and broadband were among the lowest in the OECD.

Considering the foregoing, a historic telecommunications constitutional reform (Reform) was published in June 2013 with the main aim of improving and securing effective competition with the respective benefits for the end users.

The Reform was followed by the formation in September 2013 of the new Federal Telecommunications Institute (IFT) and the publication in July 2014 of new convergence legislation, the Federal Telecommunications and Broadcasting Law (FTBL).

Since its creation, the IFT has been issuing various regulations and guidelines, and has been in charge of implementing the Reform and the FTBL through the drafting and execution of various policies, some of which we review below.

In August 2017, the OECD published a new study that weighs the developments derived from the Reform and acknowledges the important evolution and tangible benefits to the people through the regulatory changes, but also identifies areas of opportunity and new actions to be implemented.

---

1 Federico Hernández Arroyo is a partner at Hogan Lovells BSTL, SC. The author thanks Rodrigo Méndez Solís and David Amado Monroy for their help in the preparation of this chapter.
3 Telmex and Telcel are part of the same economic interest group and are held by América Móvil.
In December 2018, a new government took office and so far in 2019 we are witnessing some relevant impacts in the telecommunications sector and we expect some additional challenges in the near future.

II REGULATION

i The regulators

The main regulator is the IFT, which was created as a constitutional entity with enhanced powers covering almost all decisions concerning the telecommunications and broadcasting sectors, except as mentioned below. It has a new institutional design, specific rules for the designation of its commissionaires, as well as rules for transparency and contact with the regulated industry.

The IFT has the following main features:

- constitutional autonomy;
- management of its own patrimony and budget;
- independence of resolutions, including its own statutes and general provisions;
- public deliberations;
- powers to directly grant, revoke and approve all acts regarding telecommunications and broadcasting concessions and authorisations; and
- exclusive powers in economic competition matters regarding the broadcasting and telecommunications sectors, and the power to regulate content transmissions except with respect to the following content: electoral, childhood, health, copyrights and education (in which the respective authorities shall intervene accordingly).

Norms, acts or omissions of the IFT can be appealed only through a constitutional trial (amparo indirecto), and there is no injunction. Such trials will be held before specialised judges (two federal judges) and courts (two federal tribunals comprising three magistrates) in broadcasting, telecommunications and economic competition matters that were established as part of the Reform.

Another regulator in the sector is the Federal Consumer Protection Agency through a Telecommunications Deputy Attorney (Profeco) introduced by the Reform, which is in charge of protecting the rights of telecommunications consumers (although it appears that will be changed). The Profeco shall approve adhesion agreements to balance the obligations and rights between telecommunications service providers and end users.

The Ministry of Communications and Transportation (SCT) continues to participate as an authority (but to a much lesser extent), such as by issuing non-mandatory opinions with respect to specific acts of the IFT; implementing social, universal and broadband programmes; and in international negotiations of treaties and orbital resources.

The Ministry of Finance and Public Credit (SHCP) has the option to issue non-mandatory opinions to the IFT regarding considerations applicable to the grant and use of frequency bands.

The main sources of law in the telecommunications and broadcasting sector are the following:

- the Mexican Political Constitution;
- the FTBL;
- the Federal Economic Competition Law (FECL); and
- the Foreign Investment Law (FIL).
In addition to the foregoing, there are numerous international treaties, specific regulations, guidelines and rules, and other administrative and technical provisions issued by the IFT and the prior regulator that continue to be applicable.

ii Regulated activities

The FTBL contemplates two types of approval for the provision of telecommunications and broadcasting services: concessions and authorisations, each of which has its own modalities as detailed below.

Public telecommunications and broadcasting services are defined as those ‘services of general interest provided by concessionaries to the general public with commercial, public or social purposes’. On the other hand, the concept of telecommunications is defined as ‘every emission, transmission or reception [except of broadcasting] made through threads, radio electricity, optic means, physical or other electromagnetic systems of: signs, signals, data, writings, images, voice, sounds or information of any other kind’. In turn, broadcasting is defined as follows: ‘dissemination of electromagnetic waves of audio or associated audio and video signals, using, enjoying or exploiting the frequency bands of the radio spectrum, including those associated to orbital resources [….] with which the population may directly and freely receive the signals of its transmitter using the proper devices’.

The unique concession is a figure put forward by the Reform and the FTBL that allows the provision of all services that are technically feasible, excluding spectrum or orbital resources. According to its purposes, the unique concession shall be for commercial use (for profit), public use (government agencies), private use (private experimentation and testing, when spectrum or orbital resources are required) and social use (not-for-profit cultural, scientific, education, community and indigenous). There are specific guidelines issued by the IFT that describe the procedure, terms and conditions to secure unique concessions through the submission of the corresponding application formats.

An additional concession shall be granted for the use and exploitation of determined frequency bands and orbital resources (geostationary orbital positions or satellite orbits assigned to Mexico). Such concessions are also divided depending on their purpose as detailed above and the type of service to be provided (telecommunications or broadcasting).

Frequency band concessions for commercial and private use are granted through public bids, where the economic factor (consideration) shall not be the sole element to determine the winner of a bid. Frequency band concessions for public and social purposes for the provision of telecommunications services are assigned directly, and for broadcasting services are granted through a specific plan and procedure conducted by the IFT. The secondary use of spectrum can be authorised under certain circumstances for specific events or commercial and industrial activities.

Orbital resources concessions are in principle granted through public bids, but there are two exceptions under which they can be directly assigned: if there is a justified application from an interested private party and in the case of public entities.

An authorisation granted by the IFT is required to:

\(a\) establish a reseller of telecommunications services without being a concessionaire;

\(b\) install, operate and exploit earth stations to transmit satellite signals;

\(c\) install telecommunications equipment and transmission media that cross the borders of the country;
d) exploit the emission and reception rights of signals and frequency bands associated with foreign satellite systems that cover and could provide services in the Mexican territory; and
e) use temporary spectrum bands for diplomatic visits.

There are specific guidelines issued by the IFT that describe the procedure, terms and conditions to secure each of these authorisations through the submission of the corresponding application form.

On the other hand, products, equipment or devices intended for telecommunications or broadcasting services that are to be connected to a telecommunications network or use the spectrum shall be homologated or certified by the IFT.

Value-added services are no longer regulated under the new regulatory framework so they can be freely provided, although internet access is now considered as a telecommunications service and subject to concession or authorisation.

iii Ownership and market access restrictions

The frequency bands and orbital resources concessions can only be granted to Mexican individuals or entities, but as a result of the Reform, there is no limitation with respect to foreign investment for telecommunications services. In broadcasting, foreign investment is limited to 49 per cent control of an entity, subject to reciprocity from the country of the ultimate investor, but through neutral investment it is possible to secure larger economic participation. In its 2017 report, the OECD recommended eliminating any foreign investment restriction in broadcasting.

All authorisations (except one) are also granted to Mexican individuals or entities and are not subject to foreign investment restrictions. The authorisation for the use of temporary spectrum bands for diplomatic visits can only be granted to the Ministry of Foreign Affairs and cannot be assigned.

The frequency bands and orbital resources concessions for commercial purposes are subject to public bidding procedures, which usually contain spectrum caps depending on the particular bid. The winner of an auction must make an up-front payment for the grant of the concession and periodical payments for the use and exploitation of such resources. The latter payments are also applicable for authorisations concerning the exploitation of frequency bands associated with foreign satellite systems.

On the other hand, to level the playing field, the Reform introduced a new concept, called preponderance, which triggers asymmetrical regulation in an expeditious manner in addition to the standard concept of dominance (substantial market power in one or more telecommunications or broadcasting markets under the FECL). Preponderance applies to agents who hold a participation of more than 50 per cent in the telecommunications or broadcasting sectors. In March 2014, the IFT declared as preponderant agents and imposed different measures on Telcel, Telnor and Telmex (and other companies within the same group) in the telecommunications sector, and Televisa (and other companies within the same group) in the broadcasting sector.

The measures imposed by the IFT, which were reviewed and amended in 2017 (and are in the process of being revised again), have the purpose of preventing abuses by the preponderant agents and granting access to the rest of the players to services, infrastructure and other information that would foster competition. Moreover, in 2018, the IFT resolved
that Temex and Telnor shall incorporate two new companies that will provide access to the local network, dedicated circuits and passive infrastructure to other carriers on a non-discriminatory basis.

In 2014, the IFT declared the Televisa Group as an agent with substantial market power in the pay-TV market. Such resolution was challenged, and the Supreme Court resolved in favour of Televisa Group; subsequently the IFT resolved that the substantial market power was not proven.

Finally, the rollout of infrastructure and networks is subject to state and municipal restrictions that are inconsistent, costly and burdensome. Although the IFT and the SCT have worked to improve the situation, there is a long way to go. However, the state of Hidalgo (out of 32) has simplified the procedures regarding the installation of telecommunications infrastructure in all of its municipalities.

iv Transfers of control and assignments

The IFT is in charge of authorising the total or partial assignments of concessions for commercial or private use, as long as at least three years have passed since the granting date of the concession. It shall also authorise the assignment of any public or commercial concessions between Mexican public entities. The regulator has 90 calendar days to approve the assignment, in which case the assignee shall commit to comply with the pending obligations and new conditions imposed by the IFT.

When the assignment of concessions is between concessionaires that provide similar services in the same geographical zone, the IFT shall review the actual or potential antitrust effects. The assignment, encumbrance, pledge, trust, sale or mortgage, either totally or partially, of any concession in favour of foreign governments or states is prohibited. If a concessionaire subscribes or sells shares or equity, in one or consecutive acts, that represent 10 per cent or more of its capital stock, the following procedure will apply, unless an antitrust concentration procedure is triggered:

- the concessionaire shall notify the IFT, providing a report of the party interested in acquiring the shares that includes information about the ultimate individuals indirectly holding more than 10 per cent;
- the IFT will have 10 business days to request the opinion of the SCT;
- the SCT will have 30 calendar days to issue its opinion; and
- the IFT will have 15 business days, counted from the receipt of the SCT’s opinion or the termination of its term, to justifiably reject the operation. If there is no objection from the IFT within such term, the transaction will be considered as authorised.

The foregoing procedure is not applicable in the case of a subscription or sale of neutral investment shares under the FIL, or when the capital increase is subscribed by the same shareholders and its percentage in the capital stock is not modified.

The assignment approval and the subscription or sale procedure are not applicable in the case of mergers, spin-offs or corporate restructures if such acts are performed within the same group of control or economic agent. In such scenarios, a notice shall be submitted to the IFT within 30 calendar days of the transaction.

If a concentration notice under the FECL is triggered in any case, the IFT shall resolve under the corresponding procedure provided in such law and a new set of merger guidelines issued by the IFT.
Notwithstanding, the Ninth Transitory Article of the FTBL provides that the FECL’s concentration procedure is not applicable as long as there is a preponderant agent in the telecommunications and broadcasting sector, and a simplified process shall be followed. In the 2017 report, the OECD suggested eliminating the foregoing. In September 2019, based on this article, the IFT initiated a procedure to determine the existence of substantial market power in voice, data or pay-TV services whether at a national, regional, state or local levels.

In addition, specific provisions may apply considering the particular rules contained in the corresponding concession. On the other hand, authorisations can also be assigned (except for two types), in which case the IFT has a 30-business-day period.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

The Reform categorises telecommunications and broadcasting services as human rights and public services of general interest. This means that all persons must have access to such services, and the state is obliged to ensure access to information and communication technologies, as well as to telecommunications and broadcasting services, including broadband and internet services. Thus, internet services are currently considered as standard telecommunications services, and a concession or authorisation is required for their provision.

The FTBL includes new provisions regulating net neutrality that are applicable to concessionaires and authorised parties providing internet access services. Such parties shall observe the following principles:

a free election;
b non-discrimination;
c privacy;
d transparency and information;
e management of traffic and quality; and
f sustained development of the infrastructure.

In December 2017, the IFT issued a public inquiry to receive comments on the guidelines detailing the aforementioned principles. The IFT has not yet issued the final version of these guidelines, but two NGOs recently won a constitutional trial obliging the IFT to issue them.

The IFT has launched a website, IPv6, which is focused on new actions to improve the adoption of IPv6. Actions for the adoption of IPv6 were also recommended by the OECD in 2017.

ii Universal service

The SCT is in charge of drafting and implementing a social coverage programme every year, with the aim of increasing the coverage of telecommunications networks and the penetration of telecommunication services (mainly voice and internet) in less developed areas of Mexico. The SHCP and other federal, state and municipal entities shall support and participate in this programme.

Using public funds, the SCT for several years executed a connectivity programme for public places (Mexico Conectado), to grant broadband connections to more than 100,000 sites and spaces around the country. However, this programme has not been a priority in the new administration.

In 2017, the SCT successfully concluded a public-private partnership bidding process for the biggest telecommunications project in the history of Mexico: Red Compartida. It contemplates the design, financing, deployment, operation and marketing of a wholesale national 4G LTE network in the 700MHz band that will provide broadband services to concessionaires and authorised parties under non-discriminatory terms. Red Compartida started operations in March 2018 with coverage of 32 per cent, and is required to cover 92.2 per cent of Mexico by the seventh year of its implementation.

In August 2019, the new government, through the Federal Electricity Commission, created a new state company called ‘CFE Telecommunications and Internet for Everyone’, with the goal of guaranteeing the right of access to information technologies and communications to everyone in the Mexican territory on a non-profit basis, including internet and broadband. The IFT recently granted the concession title to this company.

### iii Restrictions on the provision of service

The FTBL provides several rules for the provision of services. Additionally, the preponderant agents have more restrictions in providing telecommunications and broadcasting services. Some general conditions applicable to the provision of telecommunications services are the following:

- a. any discrimination on whatever ground is forbidden;
- b. concessionaires shall interconnect (directly or indirectly) their network with other requesting concessionaires. The interconnection agreements shall be filed before the IFT and certain obligations must be observed. The IFT will resolve any disagreement through a specific procedure;
- c. traffic between interconnected concessionaires cannot be interrupted;
- d. number portability shall be allowed to all users under strict terms and conditions;
- e. concessionaires must abstain from establishing contractual barriers limiting other concessionaires from accessing telecommunications infrastructure in real estate;
- f. any communications directed to emergency numbers shall be transmitted;
- g. standard service agreements shall be filed before the Profeco and afterwards before the IFT, and must include different rights in favour of users (including disabled consumers) to protect final consumers from any potential abuses (consumer protection regulations);
- h. tariffs of telecommunications services shall be electronically filed with the IFT before their offering; and
- i. must-offer and must-carry obligations will apply on a free basis, subject to the must-carry obligations being applicable to DTH operators if they cover 50 per cent or more of the territory, and the gratuity not applying to preponderant or dominant concessionaires.

As mentioned above, concessionaires and authorised parties that provide internet access services are subject to the following net neutrality obligations:

- a. users must have access to any content;
- b. access to services, content and applications cannot be discriminatory, delayed, interfered with, inspected or filtered;
- c. the privacy of users must be respected and the network must be secure;
they must describe the features of the service provided on their websites; and

network and traffic management shall ensure the quality and speed of the service contracted by users.

Further, the Profeco has implemented a system whereby telephone users can register their phone numbers to avoid receiving marketing or publicity calls.

Finally, the preponderant agents have additional restrictions based on the specific measures imposed by the IFT, such as the following:

- interconnection obligations (including a master interconnection agreement);
- public offer to share passive infrastructure;
- public offer of services to MVNOs;
- public offer to provide national roaming services;
- non-exclusivity agreements; and
- the provision of, inter alia, information, tariffs, quality standards.

iv Security

The FTBL includes different obligations regarding security and judicial matters, which were further detailed by specific guidelines issued by the IFT. In 2018, the IFT amended these guidelines to harmonise their provisions with those applicable to the transparency and data protection statutory framework by reducing obligations to the IFT and to concessionaires, and authorised them since the same corresponded to the Mexican Data Protection and Transparency Authority (INAI). Among other things, concessionaires and authorised parties have the obligation to provide a geographic location in real time for mobile devices, and to store, register and provide specific information about communications made from any line. They are required to answer written requests from security or judicial authorities duly founded and motivated under the applicable laws, and provide the information within the following 24 hours. Private communications are inviolable unless a federal judicial authority requests to tap or block on a private communication.

Although the International Telecommunication Union (ITU) ranked Mexico in fourth place in the Americas region in the 2018 Cybersecurity Index, still more actions need to be taken to protect data and information technology systems from cyberthreats. The INAI has assessed international standards to provide a guide to data controllers and data processors to facilitate their compliance with data security obligations. Likewise, the ICC Cybersecurity Guide for Business is a tool and self-regulatory guide to promote good business practices.

Cybersecurity threats have affected the financial services industry more than anything else in Mexico. The financial regulator has published standards for banks and other financial institutions to protect and safeguard their customers’ information. In 2018 the Central Bank of Mexico suffered a cybersecurity threat that resulted in the creation of a specialised cybersecurity department. However, the new government has no clear agenda to promote cybersecurity.

---

IV  SPECTRUM POLICY

i  Development

Spectrum and the orbital resources are publicly owned goods under the regimen and administration of the state. The IFT is in charge of the administration of the spectrum, which includes:

a  the issuing of plans and programmes;
b  granting, revoking, changing and taking concessions;
c  supervising the radio electric emissions and interferences; and
d  enforcing any applicable sanctions.

To promote an efficient use of the spectrum, the IFT must periodically update the National Frequencies Allocation Chart (CNAF). The spectrum is divided into four categories:

a  determined: for the provision of services specified in the CNAF;
b  free: which may be used for the public in general without concession or authorisation;
c  protected: for radio navigation and security of human life; and
d  reserved: for planning purposes.

On 31 December of every year, the IFT must issue the Frequency Bands Programme, which shall provide the frequencies that will be auctioned the following year. Interested parties may request the inclusion of frequency bands in such programme.

The use of spectrum on a secondary basis is authorised in two particular cases: specific events, and facilities for commercial and industrial activities.

ii  Flexible spectrum use

The FTBL introduced the attribution of frequency bands on a primary basis (protected against harmful interferences) and secondary basis (cannot cause harmful interferences to services provided under a primary basis). This new attribution aims to improve the efficient use of the spectrum.

Likewise, the FTBL put forward the possibility to lease spectrum for commercial or private use, subject to the IFT’s authorisation. Such approval must comply with the following:

a  the lessee must hold or have applied for a unique concession for the same use;
b  the lessee must be joint obligor with the concessionaire regarding the obligations derived from the bands leased;
c  the continuity in providing services cannot be affected; and
d  it cannot generate negative concentrations, monopolisation or cross-ownership.

iii  Broadband and next-generation mobile spectrum use

Currently, Mexico has allocated 584MHz for international mobile telecommunications, which represents 44.9 per cent of the ITU recommended amount of spectrum allocation for 2015. In September 2019, the IFT issued a public inquiry to receive comments in connection with the frequency bands to be used to the development of 5G in Mexico.
iv Spectrum auctions and fees

In February 2019, the IFT published the final 2019 annual programme of use of frequency bands, which plans the auction or assignment of various frequency bands, including 10MHz of the AWS band, various segments in the 2.5, 10 and 37–38.6GHz bands, and various channels for digital television, all of which are still pending.

In April 2019, the IFT initiated an auction for commercial purposes of bands for ancillary terrestrial components for satellite mobile services, which is ongoing.

Also, it is expected that the 2020 annual programme of use of frequency bands will consider auctioning off more spectrum to promote broadband penetration in Mexico.

The spectrum pricing policy in Mexico for telecommunications is mainly divided into two categories: an upfront payment for the granting of the frequency concession as a result of the bidding procedure; and periodical payments concerning the use and exploitation of the bands for the concession’s term. The upfront payment is also applicable in broadcasting, but the periodical payment is made through airtime. Any renewal of frequency concessions is subject to an upfront payment. The level of the fees has been questioned by the OECD in its 2017 report and by other players in the sector. The IFT has proposed for 2020 the reduction of the annual fees to concessionaires that invest in unattended areas. In addition, it has been proposed that community and indigenous spectrum concessions should not be obliged to pay periodical fees, in order to be consistent with its purposes.

V MEDIA

i Restrictions on the provision of service

The FTBL regulates broadcasting services (free-to-air television), and terrestrial and satellite pay television and audio services, which are considered to be telecommunications services. Both services shall be provided through concessionaires.

The FTBL also identifies programmers as individuals or entities that have the capacity to constitute a programming channel based on own or third parties’ production, whether the copyright ownership is Mexican or foreign. Programmers provide programming channels to Mexican pay-TV concessionaires through specific agreements executed by both parties. Concessionaires and programmers have different rights and obligations under the FTBL.

As a general rule, content distributed through free-to-air or pay-TV services shall promote, inter alia:

a integration of families;
b harmonic development of childhood;
c improvement of educational systems;
d artistic, historical and cultural values;
e sustainable development;
f ideas of national identity;
g gender equality;
h scientific and technical knowledge; and
i correct use of language.

Content shall also comply with the Mexican rating requirements on their respective content, and there is a maximum amount of minutes for advertising per hour per channel. Depending on the advertising, specific regulations will be applicable (e.g., health, religious, electoral). In 2018, as a result of numerous lawsuits, the Ministry of the Interior issued the new Guidelines
for the Audiovisual Content Classification of Broadcasting Transmissions and Pay Television and Audio Services, which are basically the same as the prior ones that dramatically increased the hours during which a programme or advert can be broadcast depending on its rating.

**ii Internet-delivered video content**

ICPs are not regulated under the Mexican regulatory framework, but benefit from the net neutrality provisions. OTT online video service providers currently do not require a concession or authorisation to provide services, and differ from standard operators that hold a network to offer services. The IFT has confirmed the foregoing criteria, although some of the pay-TV concessionaires are pushing for regulation of OTTs to level the playing field. We expect that discussions in this respect will continue in the years to come. There is a new initiative to impose VAT in 2020 on entertainment audio and video platforms.

According to the most recent report issued in 2019 by Mexico’s National Institute of Statistics and Geography, Mexico has 74.3 million internet users, which represents 65.8 per cent of the population above five years old. In 2018, 73.5 per cent of the same population used a mobile phone. Of those users, 69.6 per cent have a smartphone, whereby 93.4 per cent connect to the internet. According to the IFT, in December 2018, there were 71 mobile broadband connections per 100 inhabitants, and its penetration has grown 9 per cent since 2018. According to the OECD, Mexico was the fourth-highest country for growth (6.7 per cent) in fixed broadband penetration in 2018.

**VI THE YEAR IN REVIEW**

The main highlights of 2019 were the following:

a creation of the new governmental enterprise ‘CFE Telecommunications and Internet for Everyone’, which aims to provide internet to vulnerable communities that do not have access to the internet without profit;

b the First General Declaration of Unconstitutionality in Mexico, issued by the Supreme Court of Justice in February 2019, which declares unconstitutional an article of the FTBL regarding the floor of sanctions to general breaches;

c implementation of NOM-184-SCFI-2018, which revoked the previous NOM-184-SCFI-2012, under which the regulation of adhesion contacts is strengthened in favour of final users;

d the Disney/Fox concentration was approved by the IFT, with certain conditions regarding economic competition;

e a social use broadcasting concession was granted to a civil association that apparently broadcasts religious matters, which was criticised by some sectors;

f in July 2019, the IFT implemented a new dialling method that consists in 10 digits (adding ‘55’ to all numbers), which will become mandatory in 2020;

g the cancellation of the the Red Troncal auction, which was a nationwide fibre optic wholesale network project;

h the IFT approved the creation of the electronic window to carry out certain procedures before the IFT through internet with the intention of reducing administrative load and be more efficient;

i the telecommunications gross domestic product (GDP) fell 4.4 per cent in the second quarter, which contrasted with the previous four years;
within the following months, Telmex and Telnor must comply with the initiation of the functional and legal separation plan; and

the IFT recently abrogated old regulations that were outdated and issued a few new provisions in certain matters (public telephony and homologation).

VII CONCLUSIONS AND OUTLOOK

Although the Reform has continued, there is a fear that the results may have slowed the pace in 2019, considering the decrease of the telecommunications GDP in the second quarter. To various analysts, there is no certainty and clarity about the policies to be implemented by the new federal government in telecommunications, broadcasting, cybersecurity and generally in other digital areas. Apart from the new ‘CFE Telecommunications and Internet for Everyone’ company, there is no other major public policy anticipated. Such uncertainty and a state-driven vision could negatively impact investments and new projects from the private sector. One important event will be the replacement of the head of the IFT in early 2020. Also, in 2019 the IFT suffered a significant decrease in its budget and the proposal for 2020 is in a better shape but even less than in 2018, which may affect some of the activities of the regulator.
Chapter 14

POLAND

Xawery Konarski and Michał Matysiak

I OVERVIEW

According to market research, in 2018 the value of the telecommunications market in Poland reached 39.2 billion zlotys, which is a decrease of 300 million zlotys on the previous year. Taking into account the data accuracy margin, experts estimate that the value of the telecommunications market in Poland in 2018 did not change in relation to the data of 2017.

The Polish authorities have ambitions to make Poland a leader of the 5G technology on the European market. There is no doubt that the authorities’ intended actions will result in further development of the ICT sector. The 5G network with increased performance parameters will ensure faster data transfer speed, which will be of key importance for market segments that require high data throughput and reduction of data transmission delays (e.g., e-sport, virtual reality, artificial intelligence, internet of things, smart cities or autonomous vehicles).

For the above reasons, on 30 August 2019, the Polish legislature introduced legislative changes to the Act of 7 May 2010 on supporting the development of telecommunications services and networks aimed at improving the legal environment for the planned implementation and development of 5G networks in Poland. Further measures are also planned in the near future, such as the 3.7GHz frequency auction or legislative changes concerning the amendment of regulations to the Telecommunications Law.

II REGULATION

i The regulators

One of the most important regulatory authorities of the ICT sector in Poland is the President of the Office of Electronic Communications (the President of UKE), which is the regulatory authority for telecommunications, postal activities and the management of frequency resources. The detailed competences of the President of UKE are spread over several legal acts, including the Telecommunications Act and the Act on Support for the Development of Telecommunications Services and Networks (commonly known as the Mega Act).

---

1 Xawery Konarski is a senior partner and Michał Matysiak is a trainee legal adviser at Traple Konarski Podrecki & Partners.
Another very important regulatory body is the National Broadcasting Council, whose competences are regulated by the Broadcasting Act. In accordance with Article 6(1) of the Broadcasting Act, the National Council shall safeguard freedom of speech in radio and television broadcasting, protect the independence of media service providers and the interests of the public, as well as ensuring an open and pluralistic nature of radio and television broadcasting.

The President of the Office of Competition and Consumer Protection (the President of UOKiK) is responsible for shaping antitrust and consumer protection policies, as well as providing opinions on state aid projects. The President of UKE shall cooperate with the President of UOKiK on issues concerning the observance of rights of entities using postal and telecommunications services, counteracting competition-limiting practices and anticompetitive concentrations of postal operators, telecommunications undertakings and their associations (Article 192(1) point 14 of the Telecommunication Law).

The President of the Office of the Personal Data Protection (the President of UODO) is a supervisory authority within the meaning of Regulation 2016/679 and Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 (the Police Directive). The President of the UODO controls the performance of the provider of publicly available telecommunications services when carrying out the following duties: ensuring by the provider of publicly available telecommunications services adequate technical and organisational protection measures ensuring security of personal data processing (Article 1741 of the Telecommunications Law), notification of personal data breach (Article 174a of the Telecommunications Law) and keeping a register of personal data breach (Article 174d of the Telecommunications Law).

### ii Main sources of law

At the national level, the activity of the ICT sector is regulated mainly by the following legal acts: the Act of 16 July 2004 on Telecommunications Law (TL), the Act of 7 May 2010 on supporting the development of telecommunications services and networks, the Act of 29 December 1992 on radio and television broadcasting (the Broadcasting Act) and the Act of 18 July 2002 on providing services by electronic means.

It is also worth mentioning the following regulations: the Act of 18 July 2002 on the provision of services by electronic means, the Act of 5 July 2018 on the National Cyber-Security System, the Act of 10 June 2016 on counterterrorist activities (and other acts concerning particular uniformed services, e.g., police or intelligence agencies), the Act of 16 February 2007 on competition and consumer protection (ACCP) and the Act of 10 May 2018 on personal data protection.

Owing to the specific nature of the ICT sector, legal regulations concerning particular sectors (e.g., public, finance or healthcare) may also be of great importance. First of all, it is worth noting the financial (banking) sector, which is regulated in a number of legal acts, for example by the Act of 29 August 1997 on Banking Law and the Act of 19 August 2011 on Payment Services. However, the above-mentioned issues fall beyond the scope of this chapter.

### iii Regulated activities

Telecommunications activities, in principle, do not require a licence. The telecommunications activities that constitute business activities shall be the regulated activities and shall be subject to entry in the register of telecommunications undertaking (Article 10(1) of the TL). An entrepreneur may perform telecommunications activity if they meet the conditions...
specified in the provisions of the TL and after obtaining an entry in the above-mentioned 
register. The above obligations apply to entities providing services via public and non-public 
telemcommunications networks.

Pursuant to Article 209(1) point 2) of the TL, a fine may be imposed on an entrepreneur 
for performing telecommunications activity in the scope not covered by the application for 
entry in the register, and pursuant to Article 209(2), a fine may be imposed on the operator 
of a telecommunications undertaking for such infringement.

Telecommunications law provides a form similar to a licence for a system of frequency 
spectrum) and numbering resource management. The manner of frequency management 
is specified in Article 111 et seq. of the TL. In this respect, the most important are the 
provisions on frequency reservations or decisions that grant the right to dispose of frequencies 
or orbital resources (Article 114 of the TL).

In the absence of sufficient frequency resources, entities to which a general exclusive 
frequency licence is granted shall be appointed by means of a contest, a tender or an auction 
(Article 116(1) of the TL). An entity that has received the right to use a frequency subject to 
general exclusive frequency licence shall pay annual fees for the right to use this frequency 
(Article 185(1) of the TL).

Additionally, under the Telecommunications Law, the use of radio equipment requires 
a radio licence issued by the President of UKE by way of a decision (Article 143 of the TL).

iv Ownership and market access restrictions

Polish law does not, as a rule, provide for any obstacles to conducting business activity in 
the territory of the Republic of Poland by a foreign entity (person). Telecommunications 
activities conducted by a telecommunications undertaking from a Member State or a state 
that has concluded with the European Union and its Member States an agreement on the 
freedom to provide services and that temporarily provides services in the territory of the 
Republic of Poland under the terms and conditions specified in the provisions of the Treaty 
establishing the European Community, Agreement on the European Economic Area or in the 
provisions of another agreement regulating the freedom to provide services, as appropriate, 
shall be also subject to entry in the register of telecommunications undertaking (Article 10(1) 
of the TL). An operator from the Member State applying for telecommunications access shall 
not be obliged to make an entry in the register referred to in Article 10, provided that it does 
not perform telecommunications activities in the territory of the Republic of Poland (Article 
26(4) of the TL).

The President of UKE may specify in the frequency reservations process a limitation of 
the use of the frequencies covered by the reservation where the introduction of such limitation 
is justified by the necessity to achieve a public interest objective (e.g., in terms of supporting 
social, regional or territorial cohesion and promoting cultural and linguistic diversity and 
media pluralism (Article 1151(1) point 6) letter b) and d) of the TL)).

The Telecommunications Law provides restrictions on participation in a tender or 
auction for frequency reservations (Article 118(4a) and (4b) of the TL). The President of UKE, 
when defining the conditions of participation in a tender or auction, may in particular indicate 
the resources that disposal excludes or entitles to participate in the tender (auction), and also 
limits the frequency resources for which reservation may be applied for by a given entity 
(Article 118(4a) of the TL). Moreover, the President of UKE may provide further restrictions 
regarding financial credibility, experience in telecommunication activities or the fact that only 
one entity from a given capital group may participate in a tender, auction or competition.
The above-mentioned restrictions are related to further regulations of the Telecommunications Law concerning the conditions of competition (Article 118a(1) point 1 of the TL). Additionally, the President of UKE in consultation with the President of the Office for Competition and Consumer Protection may, by way of a decision, refuse a general exclusive frequency licence for a subsequent period, if justified by the need to ensure effective frequency usage, in particular in a situation where granting a general exclusive frequency licence for a subsequent period could lead to spectrum hoarding by a given entity or a capital group, involving that entity (Article 116(9) of the TL). Reservation of frequencies may also be refused in the cases set out in Paragraphs 9a and 9b relating to the need to increase significantly the efficiency of frequency use or to circumstances giving rise to a threat to national defence, security or safety and public order. With respect to Article 118a(1) point 1 and Article 116(9) of the TL, the President of UKE shall consult the President of UOKiK.

In addition, Article 21 et seq. TL defines the powers of the President of UKE to regulate the telecommunications market. After conducting proceedings (market analysis), the President of UKE, if it is established that a telecommunications undertaking with significant market power or telecommunications undertakings with collective significant market power exist on the relevant market, issues a decision in which it identifies the relevant market, identifies the undertaking or undertakings with significant market power and decides on the regulatory obligations of such undertakings.

Moreover, telecommunications undertakings, while negotiating the provisions of a telecommunications access agreement, shall take account of obligations imposed on them in accordance with Article 26 et seq. of the TL, for example, concerning technical or operational conditions of access (Article 35 of the TL) or equal treatment of telecommunications undertakings (Article 36 of the TL). The President of UKE may also by way of a decision impose an obligation to prepare and present a draft reference offer on telecommunications access, the degree of detail of which will be specified in the decision (Article 42 of the TL), which is approved by the President under the procedure set out in Article 43 of the TL.

In addition, a vertically integrated telecommunications undertaking with significant market power, in order to ensure that all service providers providing their services to end users, including itself, have the possibility to offer equivalent services to end users, shall inform the President of UKE of its intended transfer of local access network assets or a substantial part thereof to a separate legal entity under different ownership or to a newly established entity (Article 44g(1) of the TL). As a result of the notification, the President of UKE, based on the results of market analysis, conducts proceedings and imposes, maintains, changes or repeals regulatory obligations.

v Transfers of control and assignments

The issue of changing the entity that holds the frequency reservation is regulated in Articles 122 and 1221 of the TL. In accordance with the latest amendment to the Telecommunications Law, analogue TV was deleted from the scope of Article 122 as a result of the switch-off of analogue television broadcasting and the lack of reservation for analogue TV.4 With the exception of frequency reservations, for the purpose of broadcasting radio programmes in an analogue manner, the President of UKE changes the entity holding the frequency reservation if the entity holding the rights and obligations and the frequency agree to transfer

---

the rights and obligations and the entity indicated in the application meets the requirements specified in the Act. The President of UKE shall change an entity holding a general exclusive frequency licence granted by means of a tender, an auction or a contest having sought an opinion of the President of UOKiK with respect to a competitive situation (Article 122(5) of the TL). The President of UKE shall take a decision to change an entity holding a general exclusive frequency licence for the purposes of digital broadcasting or rebroadcasting of radio or television programmes in agreement with the Chairperson of KRRiT (Article 122(6) of the TL).

Regardless of the regulations of the Telecommunications Law, the issue of counteracting anticompetitive concentrations of undertakings and their associations is also regulated by the Act on Competition and Consumer Protection. The intention of concentration is subject to notification to the President of UOKiK if the entrepreneurs participating in the concentration meet requirements set in Article 13(1) of the ACCP. Article 14 of the ACCP establishes a closed list of cases to which the obligation to notify the intention of concentration referred to in Article 13(1) does not apply. The statutory exemption from the notification obligation covers, for example, ‘bagatelle’ (small matter) concentrations and concentrations of undertakings belonging to the same capital group. The process of issuing a decision on a concentration is regulated by Article 18 et seq. of the ACCP. Special regulations concerning the proceedings on concentration are regulated by the provisions of Article 94 et seq. of the ACCP.

Antimonopoly proceedings in concentration cases should be terminated not later than within one month from their institution (Article 96 of the ACCP). However, this time may be extended due to circumstances extraneous to the President of UOKiK (Article 96(2) of the ACCP) and complicated cases (Article 96a of the ACCP).

### III TELECOMMUNICATIONS AND INTERNET ACCESS

#### i Internet and internet protocol regulation

The Telecommunications Act is a comprehensive regulation concerning the principles of performance and control of activities consisting in the provision of telecommunications services, the provision of telecommunications networks or associated facilities (Article 1(1) point 1) of the TL). Telecommunications services using the internet and based on IP address are subject to the regulations of the Telecommunications Law to the same extent as other services. For the application of the TL, it will not matter whether a given entity provides services by means of one’s own network, another operator’s network or selling on one’s own behalf and on one’s own account a telecommunications service performed by another service provider (Article 2(1) point 41) of the TL). Therefore, the above-mentioned services are regulated in a manner similar to traditional telephony.

#### ii Universal service

The Telecommunications Law defines ‘universal service’ as a set of telecommunications services, including facilities for the disabled, provided in any technology, preserving good quality and at a reasonable price, which should be available in the territory of the Republic of Poland (Article 81(1) of the TL). Currently, the set of universal services includes connection of network termination in a fixed location enabling voice, fax and data transmission, including functional access to the internet, the speed of which enables the use of applications commonly used in minor current matters of everyday life, in particular the use of electronic mail or applications enabling making payments (Article 81(3)(1) of the TL).
Currently, the set of universal services includes connection of a network termination point at a fixed location, capable of supporting voice, facsimile and data communications, including functional internet access at rates supporting the use of common applications to handle current daily life matters, in particular using electronic mail or applications that support payments (Article 81(3) point 1) of the TL.

In September 2018, the Ministry of Digital Affairs submitted to public consultation a draft update of the National Broadband Plan – a governmental development programme defining the objectives for universal access to fast and ultra-fast internet, as well as the means to achieve these objectives. The draft NPS update defined the following main objectives of the state in this area: ensuring universal access to the internet with a capacity of at least 100Mb/s on the basis of networks by 2025, which will also enable the provision of services with a capacity measured in Gb/s and ensuring communication in 5G networks in at least one major city by 2020 and in at least all major urban centres and along major railway and road communication routes by 2025.

On 30 August 2019, the amendment to the law on supporting the development of telecommunications services and networks was passed. The purpose of the changes is to implement 5G, eliminate a number of administrative barriers (e.g., reducing the costs of telecommunications investments) and establish a Broadband Fund with an annual budget of approximately 140 million zlotys for co-financing the construction and development of the telecommunications network.

### Restrictions on the provision of service

The price of services may be regulated within the scope of the reference offer. The President of UKE may, by way of a decision, impose on an operator with significant market power an obligation to prepare and submit within a specific time limit a draft telecommunications access reference offer, the level of detail of which shall be specified in a decision (Article 42(1) of the TL). An operator on whom the obligation was imposed shall conclude telecommunications access agreements under the terms that are not worse for other parties to the agreement than those in the approved offer or determined by the President of UKE (Article 43(5) of the TL).

Telecommunications law, in principle, does not regulate the rights of a telecommunications operator to restrict or favour network access on the basis of content. The President of UKE may order the blocking of access to numbers or services where this is justified by the protection of end users against abuse of the telecommunications network (Article 79b of the TL). As a rule, a telecommunications undertaking cannot control the content, applications and services to which its users have access.

The President of UKE may, by way of a decision, impose an obligation on an operator with significant market power to take into account justified requests of telecommunications undertakings to provide them with telecommunications access, including the use of network elements and associated facilities, in particular taking into account the level of competitiveness of the retail market and the interest of end users (Article 34 of the TL). Moreover, the President of UKE may also impose, by way of a decision, an obligation to treat telecommunications undertakings equally as regards telecommunications access (Article 36 of the TL).

Additionally, the Telecommunications Law also provides for a number of requirements concerning the contract for the provision of telecommunications services, for example,

---

concerning a form (Article 56(2) of the TL), the elements it should contain (Article 56(3) of the TL), its terms and conditions (Article 57 of the TL), the possibility to change or terminate its terms and conditions (Article 60a of the TL) and price lists (Article 61 of the TL). The Law also contains legal requirements for the regulations of provided services (Articles 59 and 60 of the TL).

With regard to the limitation of unsolicited transfers via terminal equipment (telephones, faxes, emails or SMS), the Telecommunications Law makes their use conditional on the prior consent of the subscriber or user (Article 172 of the TL). The provisions on the protection of personal data apply to obtaining the consent of a subscriber or end user (Article 174 of the TL).

### iv Privacy and data security

A telecommunications entrepreneur is obliged to perform tasks and duties for the benefit of defence, state security and public security and order within the scope and under the conditions specified in the Telecommunications Law and other acts. Obligations in this respect are regulated by the provisions of Article 176 et seq. of the TL.

Pursuant to Article 179(3) point 1) of the TL, a telecommunications undertaking is obliged to ensure technical and organisational conditions for access and recording of telecommunications transmissions (transmitted or received by the end user) or telecommunications terminal equipment and data held by the undertaking in connection with telecommunications transmissions for the needs of specific services (e.g., the Internal Security Agency or the Border Guard).

Additionally, a telecommunications undertaking is obliged to fulfil their duties in the scope of data retention (Article 180a–180c of the TL). These duties refer to data generated in a telecommunications network or processed by a telecommunications undertaking. It is worth mentioning that security and defence obligations are also included in other legal acts.

According to the regulations of the Telecommunications Law, the provider of publicly available telecommunications services is obliged to implement appropriate technical and organisational protection measures to ensure the security of personal data processing (Article 1741 of the TL). The provider of publicly available telecommunications services notifies the President of UODO about a breach of personal data (Article 174a(1) of the TL) no later than 24 hours after the detection of the personal data breach. If not all the required information is known within this period, the supplier shall send an initial notification within 24 hours and a second notification as soon as possible and at the latest within three days after the initial notification. If this deadline cannot be met, the supplier shall provide the information available to them within three days and explain the reason for the delay in providing the other information (Article 2 of the Commission Regulation (EU) No. 611/2013 of 24 June 2013).6 The provisions of the Act of 10 May 2018 on the Protection of Personal Data shall apply accordingly to the control exercised by the President of the Office for Personal Data Protection over the performance of obligations by the provider of publicly available telecommunications services. The Telecommunications Law imposes on the provider

of publicly available telecommunications services the obligation to maintain a register of personal data infringements, including facts accompanying the infringements, their effects and actions taken (Article 174d of the TL).

IV SPECTRUM POLICY

i Development

According to the strategy of the President of UKE for the years 2017–2021, one of its key areas of activity is making frequencies in the 700MHz band available for broadband systems.

The President of UKE is working to support legal solutions improving the efficiency of radio spectrum management. In this respect, such actions as streamlining the selection procedure, determining the manner of band allocation and preparation of the selection procedure and updating the National Table of Frequency Allocations in terms of changes were introduced at the World Radiocommunication Conference.

Moreover, the President of UKE is pursuing the objectives of changing frequency use, including agreeing new TV channels below the 700MHz band, updating frequency management in the 700MHz and 470–694MHz bands, reconfiguring TV channels, migrating TV services to the 470–694MHz band and changing DVB-T technology to DVB-T2.

There have also been actions taken to implement 5G technology in Poland. In addition to the amendment to the Act supporting the development of telecommunications services and networks, the President of UKE also undertakes other activities, such as taking steps to increase frequency use efficiency through the development of implementation concepts, refarming and optimisation of frequency resources. In addition, the President of UKE envisages active participation in the work of the International Telecommunication Union, the European Conference of Postal and Telecommunications Administrations and groups operating within the EU (the Radio Spectrum Committee, the Radio Spectrum Policy Group and the Communications Committee).

At the beginning of April 2019, the framework action plan of the President of UKE for the allocation of frequencies in the 3,600–3,800MHz band was published. On 19 April 2019, the President of UKE published preliminary assumptions for frequency distribution in the 3,600–3,800MHz band.

In addition, the Ministry of Digital Affairs plans to amend the regulations to the Telecommunications Law and to supplement the list of conditions to be met by participants in tenders or auctions for 5G frequencies.

ii Flexible spectrum use

The Telecommunications Law provides for the lease or transfer of frequencies for use. Article 1221 of the TL provides that an entity holding a general exclusive frequency licence may lease the frequencies covered by the licence or transfer them for use under another legal title to another entity.

---

An entity to whom a general exclusive frequency licence was granted shall notify the President of UKE, and with respect to the frequencies intended for broadcasting or rebroadcasting of radio or television programmes also the Chairperson of KRRIT; of the frequencies leased or transferred for use, not later than within 14 days of the date of concluding an agreement (Article 1221(2) of the TL).

The President of UKE may, by way of a decision, change the conditions for using frequencies or prohibit their use by an entity to which the frequency has been leased or transferred for use, for example, where the use of these frequencies by that entity could lead to distortion of competition (Article 1221(5) point 2) of the TL).

### iii Broadband and next-generation services spectrum use

At the beginning of April 2019, the President of UKE published a framework action plan for the allocation of frequencies in the 3,600–3,800MHz band. On 19 April 2019, the President of UKE, following the 2018 consultation on frequencies intended for 5G, published preliminary assumptions for frequency distribution in the 3,600–3,800MHz band.

In addition, the Ministry of Digitisation plans to amend the regulations to the Telecommunications Law and to supplement the list of conditions to be met by participants in tenders or auctions for 5G frequencies.

### iv Spectrum auctions and fees

As stated in Article 116(1) of the TL, in the absence of sufficient frequency resources, entities to which a general exclusive frequency licence is granted shall be appointed by means of a contest, a tender or an auction, governed by Article 118 of the TL. The announcement of a tender, an auction or a contest shall be published on the UKE BIP website. An announcement of a tender, an auction and a contest shall specify the subject and scope of a tender, an auction or a contest, participation conditions as well as the criteria for selection of offers (Article 118(2) of the TL).

With regard to frequency reservations, the Telecommunications Law provides for the following types of fees: annual frequency management fees (Article 185(1) of the TL) and a frequency reservation fee (Article 185(4) of the TL).

For more information see also Section II.iv.

### V MEDIA

### i Regulation of media distribution generally

The granting of licences for the distribution of television programmes is regulated by the Broadcasting Act. Dissemination of radio and television programmes, with the exception of public radio and television programmes, requires a licence (Article 33(1) of the Broadcasting Act).

The transmission of television programme services exclusively in information and communication technology systems does not require a licence, unless the programme service is to be retransmitted by terrestrial diffusion, satellite or cable networks (Article 33(2) of the Broadcasting Act).

The Broadcasting Act does not provide for the necessity to obtain licences for entities providing on-demand audiovisual media services. However, a number of regulations to apply to the entity (Article 47a et seq. of the Broadcasting Act).
Outside the scope of the Broadcasting Act, there are other types of platforms – the provisions of the Act on the provision of services by electronic means shall apply to them.

**ii Internet-delivered video content**

Video distribution in IPTV form can be divided into three categories: live web TV, time-shifted TV programmes and VOD. Services of this type available in Poland are generally chargeable, therefore people who cannot afford to buy them do not have access to the presented content.

Radio programmes and digital terrestrial television (DVB-T) offer channels available to the general public without prior payment. However, Polish law requires relatively small monthly fees for the use of a radio or television receiver.

**VI THE YEAR IN REVIEW**

In 2018, a number of changes took place on the Polish telecommunications market. The most recent of these was the adoption on 30 August 2019 of an act amending the Act on supporting the development of telecommunications services and networks. The aim of the Act is to eliminate administrative and legal barriers hindering the development of telecommunications infrastructure. The law also provides for the improvement of the coverage of telecommunications services and the assurance of adequate quality of mobile services even in geographically difficult areas.

In addition, Poland is currently entering a key period for the implementation of the 5G network. The President of UKE is conducting activities aimed at preparing tenders for frequencies for the 5G network. In addition, the Ministry of Digital Affairs also plans to take legislative action to issue regulations to the telecommunications law in this area.

**VII CONCLUSIONS AND OUTLOOK**

The implementation of the Act on the national cybersecurity system did not solve all the problems; the relationship of the Act to the telecommunication law is also questionable due to the partial sectoral exclusion contained in the Act on the national cybersecurity system.

In the coming period, it will be crucial for the European Union (and consequently for Poland) to prepare properly for the implementation of the 5G network at both national and EU level and to ensure a favourable environment for the development of new data-based technologies.
Chapter 15

RUSSIA

Maxim Boulba and Elena Andrianova

I OVERVIEW

The TMT sector in Russia is heavily regulated, and is to a very large extent driven by political and lobbying efforts. Such unpredictability also contributes to the sometimes-controversial evolution of the regulatory landscape.

Thus, on the one hand, the governmental authorities are working on reforming the TMT sector in Russia and introducing a set of new principles that could have a significant impact on all sectors of the communications market (including by way of simplification of the licensing regime, efficient allocation of frequencies, development of communication infrastructure and universal access to telecommunications services).

On the other hand, taking into account the current political context in Russia, recent trends in the TMT market in Russia are mainly focused around increasing legislative pressure on market players, restricting foreign investment and strengthening state control over operators, media companies and customers.

II REGULATION

i The regulators

The main regulator in the TMT sector in Russia is the Ministry of Communication and Mass Media of the Russian Federation (Mincomsvyaz).

Broadly, Mincomsvyaz is in charge of elaborating and implementing state policy in the TMT sector. It also, inter alia, participates in the legislative process (namely, by submitting bills to the government) and adopts secondary legislation in the area.

Furthermore, three state agencies that fall under the auspices of Mincomsvyaz:

a the Federal Service for Control over Communications, IT and Mass Media (Roscomnadzor) is the main licensing authority in the telecommunication sector and is in charge of mass media registrations. It also monitors the compliance of telecom operators with the established regulatory requirements;

b the Federal Print and Mass Media Agency; and

c the Federal Communications Agency, which is in charge of certification in the telecom area.

1 Maxim Boulba is a partner and Elena Andrianova is a senior associate at CMS.
Main sources of law

The main regulatory acts in the field of telecommunications are the following (this list is not exhaustive):

a. Federal Law No. 126-FZ ‘On communication’, dated 7 July 2003 (Communication Law), is the key legislation in the telecommunication sector. The Communication Law provides for quite detailed regulation in the areas of communication networks and interconnection between them, licensing of telecommunication activities, allocation of frequencies, etc.

b. Federal Law No. 128-FZ ‘On licensing of particular types of activities’, dated 8 August 2001, provides a general legal framework for the licensing of various types of business activities in Russia, including the provision of telecommunication, TV and radio broadcasting services;

c. Federal Law No. 184-FZ ‘On technical regulation’, dated 27 December 2002, provides a general legal framework for the standardisation and certification of various equipment, including telecommunication equipment, being subject to specific regulation provided by secondary legislation;

d. Federal Law No. 144-FZ ‘Law On Investigative and Search Activities’, dated 12 August 1995, is the main legal act that governs the obligations imposed on network operators in the area of monitoring and interception of communications;

e. Federal Law No. 149-FZ ‘On Information, Information Technologies and Data Protection’ dated 27 July 2006 (Information Law);

f. Federal Law No. 152-FZ ‘On Personal Data’ dated 27 July 2006; and

g. other resolutions and orders of the government, acts of Mincomsvyaz, etc.

The media sector, being traditionally subject to a separate area of regulation under Russia's laws, is governed by the following main legal acts:

a. Law of the Russian Federation No. 2124-1 ‘On Mass Media’, dated 27 December 1991 (Mass Media Law), is the core legislation in the media sector. The Mass Media Law, inter alia, governs in detail the activities of mass media companies and organisations, mass media registration procedures, broadcasting licensing issues and limitations on foreign participation in mass media companies (for more detail, see Section II.iii);

b. Federal Law No. 436-FZ ‘On Protection of Children from Information that May Be Harmful to Their Health and Development’, dated 29 December 2010, introduces additional requirements and restrictions on mass media aimed at protecting children from any kind of destructive and inappropriate information; and

c. Federal Law No. 57-FZ dated 29 April 2008 ‘On the Procedure for Making Foreign Investments in Companies which are of Strategic Importance for Ensuring the Country's Defence and State security’ (Strategic Law). It is important to note that in terms of the Strategic Law, certain types of TV and radio broadcasting activities are viewed as strategic and, therefore, certain transactions involving the shares and assets of the companies involved in such types of activities are subject to control by state authorities and additional clearance requirements (for more detail, see Section II.iv).
iii Regulated activities

As regards the telecommunication sector, further to the Communication Law, a licence is a necessary prerequisite for providing telecommunication services in Russia.

More specifically, Regulation of the Russian Government No. 87 dated 18 February 2005 sets out an exhaustive list of communication service licences that must be obtained by communication service providers wishing to conduct business in Russia. This list includes the following 20 types of communication services:

a local phone services;
b intercity and international phone services;
c phone services in a dedicated network;
d intrazone phone services;
e local phone services via payphone units;
f local phone services via public access points;
g telegraph services;
h personal radio call services;
i mobile radio communication services in a public communication network;
j mobile radio communication services in a dedicated communication network;
k mobile radiotelephone service;
l mobile satellite services;
m provision of communication channels;
n data transfer (excluding voice data);
o transfer of voice data;
p telematics services (including internet services);
q cable broadcasting services;
r on-air broadcasting services;
s wired broadcasting services; and
t postal services.

In accordance with the current legislation, the licensing authority for the above-mentioned communication licences is Roscomnadzor.

A communication service licence may be granted on the basis of an application or as a result of auction or tender proceedings. An auction or tender is held where the provision of a given communication service involves the use of RFs and the competent state authority establishes that the required RF allows for only a limited number of network operators to be active within the relevant territory; or the public communication network on the territory has limited resources and the Ministry of Communication and Mass Media of the Russian Federation (Mincomsvyaz) establishes that the number of network operators active within this territory should be limited.

Furthermore, additional authorisations are applicable to undertakings active in the media sector:

a media broadcasting programmes and channels are subject to registration as mass media carried out by Roscomnadzor;
b a broadcasting licence is required to distribute (broadcast) mass media products in Russia. Such licence may be held either by the holder of the mass media registration itself, or by the licensed operator acting on the basis of the broadcasting agreement with the holder of the mass media registration provided that the mass media product is broadcast by the operator without any changes to the broadcast content.
There are two main types of broadcasting licences provided by the Mass Media Law:

- a universal broadcasting licence that may be obtained by broadcasters registered as an editor of a TV channel or a radio channel. Licence holders are entitled to conduct different types of broadcasting in various environments (satellite, cable, on-air, etc.) over the whole territory of the Russian Federation; and
- a licence that allows holders to broadcast in a particular broadcasting environment only.

Normally, broadcasting licences are issued for a term of 10 years (unless an applicant indicates a shorter term in the application form) with a possibility of renewal.

Should the provision of the services or broadcasting of mass media products also imply the use of the RF spectrum, it is also necessary to obtain specific approval on the allocation of a frequency band (for more detail, see Section IV).

iv Ownership and market access restrictions

Communication licences are only granted to Russian entities, and a foreign company cannot itself apply for a licence. The main restrictions and limitations in the TMT area in Russia relate to foreign participation and investments, namely:

- in accordance with the Mass Media Law, foreign investors cannot hold more than 20 per cent in a mass media company (i.e., a company holding a mass media registration, or a broadcasting company);
- restrictions on foreign participation also exist in the area of audience measurement for the TV sector. Thus, in terms of the Mass Media Law, foreign participation in the company in charge of audience research and surveys (to be appointed by the state authorities) is also limited to 20 per cent; and
- additional limitations on foreign participation exist in the area of online audiovisual services (online cinemas). Thus, audiovisual services can be owned by Russian legal entities or Russian citizens (who do not hold citizenship of other countries) only. Foreign investors are normally allowed to own such Russian legal entities, being the owners of audiovisual services. However, the ownership limitations are imposed on specific foreign operators, namely those foreign operators who own an informational resource whose number of users in Russia is less than 50 per cent of its total audience (number of users). Such foreign operators are entitled to own, manage or control, directly or indirectly, a share exceeding 20 per cent in the Russian owner of an audiovisual service, provided that such ownership has been cleared by the relevant government commission.

v Transfers of control and assignments

As regards the transfer of licences, it is noteworthy that the Communication Law explicitly prohibits any full or partial transfer of a communication service licence to another legal entity or individual.

M&A transactions involving media and telecommunication companies are subject to general merger control requirements and thresholds set forth by the Russian antimonopoly (competition) legislation (namely, Federal Law No. 135-FZ ‘On Protection of Competition’,

---

2 For more details see Section V.ii, ‘Internet-delivered video content’.
dated 26 July 2006). If the respective transaction is subject to merger control in Russia, an application must be filed by the acquirer to the Federal Antimonopoly Service (FAS). It normally takes from one to three months to receive a FAS clearance decision.

In addition, under the Strategic Law, certain TV and radio broadcasting companies are viewed as strategic. Therefore, transactions aimed at the acquisition by foreign investors (including Russian companies controlled by foreign investors) of control over such broadcasting companies or more than 25 per cent of their assets are subject to the prior approval of a governmental commission chaired by the Prime Minister (Commission).

The procedure for the review of applications under the Strategic Law is rather cumbersome and time-consuming, as the Commission only holds sessions two to three times per year. Furthermore, in terms of the Strategic Law, foreign investors are required to inform the Russian authorities on any acquisition of 5 per cent or more in strategic companies.

As regards the telecommunications sector, the Strategic Law applies to the operators (holders of communication licences) that are dominant in certain Russian telecommunication markets (for instance, the all-Russian communication market, the fixed phone services market covering more than five Russian regions or all Russian federal cities).

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation
From the regulatory perspective, there is no specific regulation for internet services as such under Russia’s laws.

Communication services provided over the internet are normally subject to telecommunications licences, such as a telematics services licence or a data transfer services licence (excluding or including transfer of voice data), for the provision of communication channels.

The government adopts further rules regarding the provision of specific services so that each licence holder must provide its services under the licence according to such rules. For instance, the government has adopted specific rules for data transfer services (contained in Regulation No. 32 dated 23 January 2006) and telematics services (contained in Regulation No. 575 dated 10 September 2007). However, these rules do not provide for very detailed regulation of internet services that would significantly distance them from the existing regulations for other types of communication services.

ii Universal service
The principle of universal access to communication services was incorporated in the Russian legislation (and, namely, in the Communication Law) in 2003. Encouraging universal access to communication services is one of the paramount priorities of the government’s policy in the TMT area, and is mainly aimed at ensuring access to communication services in rural areas and hard-to-reach regions of Russia (which are quite numerous due to the vastness of the Russian territory).

Currently, in terms of the Communication Law, universal service includes the following types of telecommunication services:

- telephone services accessible via public payphones (coin stations) or interactive kiosks, which should be available in all residential areas all for all residents within a maximum one-hour walking distance;
data transfer services and access to the internet via public access points ensuring internet access (at 10Mbit/s speed) in all residential areas with more than 250 inhabitants (project on ‘bridging the digital divide’).

One of the biggest Russian telecoms operators, JSC ‘Rostelecom’, is in charge of the project aiming at ensuring universal access to the communication services, which is currently ongoing.

It is also important that all Russian communication services providers are obliged to pay contributions to the Universal Service Fund – a specific fund established for the purpose of financing universal communication services.

iii Restrictions on the provision of service

Under the general rule set forth by the Communication Law, operators are free to determine the prices for their telecommunication services. That said, prices for certain types of telecommunication services are subject to state regulation, such as:

a under Federal Law No. 147 ‘On natural monopolies’, dated 17 August 1995, as well as Government Order No. 637 ‘On rate regulations in public telecommunication and mail services’, dated 24 October 2005, the rates for public telecommunication and mail services are subject to state regulation;

b universal communication services are subject to state regulation on the basis of Government Order No. 242, dated 21 April 2005; and

c following Article 20 of the Communication Law as well as Government Order No. 627, dated 19 October 2005, prices for accession services and traffic transit services rendered by operators occupying an important position in the public communication network are also subject to state regulation.

As regards customer terms and conditions, it is noteworthy that general terms and conditions for certain types of services are set forth by the government and should be complied with by service providers. For instance, the following governmental acts provide for such general terms and conditions: Government Resolution No. 575, dated 10 September 2007, sets forth general terms and conditions for providing telematics services, including mandatory provisions to be incorporated into the customer agreements; and Government Resolution No. 32, dated 23 January 2006, relates, inter alia, to data transfer services.

Restrictions on the content accessed by customers (network users) are mainly based on security considerations (see below).

Furthermore, the Information Law contains a complex procedure as to blacklisting of websites containing information the dissemination of which is prohibited under Russian law. Roscomnadzor is in charge of holding a specific Unified Register of Domain Names, Universal Page Selectors and Internet Addresses whose dissemination is prohibited in Russia (Register).

The Information Law also imposes additional regulatory obligations on operators providing internet access to their customers. Thus, telecommunications operators (providing internet services to their customers) should have access to and regularly upload information from the Register, and restrict access to blacklisted websites within 24 hours starting from the moment when such website is included in the Register.

Furthermore, the Information Law specifically prohibits the use of technologies that allow access to blocked websites (for instance, VPN services, anonymous search engines, etc.).
iv Privacy and data security

Overall, the right to privacy of correspondence, and telephone and other messages and communications, is based on Article 23(2) of the Russian Constitution, further to which the limitation of this right is admissible only based on a court decision, or if expressly provided for in federal laws.

To this end, the principles regarding data privacy restrictions are stipulated in the Communication Law, Federal Law No. 144-FZ ‘On Investigative and Search Activities’, the Code of Criminal Procedure, other statutes containing the necessary prerequisites, and numerous government and administrative regulations that deal with the technical aspects of lawful interception monitoring (LIM).

In terms of these regulations, network operators must cooperate with the law enforcement agencies and ensure their access to data transferred via the network. It is important to note that the current LIM regulations, known as the system of investigative and search operations (SORM), allow the Russian law enforcement agencies access to almost all types of information transmitted via a communication network. Thus, SORM covers wire-tapping on telephone lines, including mobile communications, internet traffic, as well as the collection, long-term storage, analysis and processing of customers’ and statistical data. From a technical perspective, the LIM standards imply a passive role on the part of operators, who are not supposed to know which customers are being controlled at any given time.

In addition, the Information Law provides for specific rules and restrictions aimed at minimising anonymity on the internet.

Thus, in terms of the Information Law, Roscomnadzor enjoys considerable powers in the area of bloggers’ activities: it monitors bloggers’ activities on the internet, runs a register of bloggers and requests data enabling their identification from hosting providers.

The Information Law introduced a broad definition of organisers of dissemination of information over the internet (organisers) that covers all persons responsible for the functioning of information systems and software designed and used for the receipt, transmission, delivery and processing of electronic messages via the internet. Persons falling under the category of organisers are required to comply with significant regulatory obligations. The main obligation imposed on organisers is the requirement to store users’ data (as regards receipt, transmission, delivery and processing of voice data, texts, pictures, sound information or other electronic messages, as well as information on the users) in Russia within one year as from the termination of such actions, and provide such data to the law enforcement and public security bodies, if necessary. Furthermore, from 1 July 2018, organisers have to store the actual content of text messages, voice data, pictures, videos, sound information and other electronic messages within six months as from the processing of that data. Since 1 January 2018, operators of online messaging services are required to identify the users of the messaging services, store this information in the territory of Russia and provide it to investigative authorities on request. Furthermore, in terms of the Yarovaya Law (Federal Law No. 374-FZ dated 6 July 2016, being a set of amendments to the anti-terrorist law and legislation governing the telecommunications industry, including the Communication Law and the Information Law), telecom operators are required to:

a store in Russia for a period of three years information on the fact of the receipt, transmission, delivery or processing of voice data, text messages, pictures, sounds, video or other communications of customers (i.e., metadata);

b store in Russia for a period of six months the actual contents of communications (voice data, text messages, pictures, sounds, video or other communications); and
Russia

provide at the request of the law enforcement agencies the above information on users and the services rendered to them, as well as any other information necessary for these authorities to achieve their statutory goals. When using message encryption and encoding, owners of internet resources will be required to provide the Federal Security Service with the keys for decoding them.

Furthermore, telecommunication services providers can also be required to cease the provision of services to a user (further to a request of the law enforcement authorities) if the user’s identity cannot be confirmed (i.e., the information regarding the user that appears in the agreement with the operator is different from the data of the actual users).

It is also important to note that in terms of Federal Law No. 152-FZ ‘On Personal Data’, dated 27 July 2006, when collecting personal data (including via the internet), an operator of personal data will be required to ensure that the recording, systematisation, accumulation, storage, clarification (updating, modification) and retrieval of Russian citizens’ personal data is conducted in databases located within Russia.

There is also specific regulation aimed at the protection of children from destructive and inappropriate information provided by Federal Law No. 436-FZ ‘On Protection of Children from Information that may be Harmful to Their Health and Development’, dated 29 December 2010. This Law introduces additional requirements and restrictions on mass media (for instance, to classify mass media products and to place specific marks on them carrying information on any potential child-restricted content) and applies to any telecommunication network.

Furthermore, as a result of possible computer attacks, a special law was adopted that deals with specific measures and requirements to be implemented and adopted to ensure the safety of the critical information infrastructure (Federal Law No. 187-FZ ‘On the Safety of Critical Information Infrastructure’, dated 26 July 2017). Although the practical application of this new Law is still not fully clear, the general idea behind it is that all critical infrastructural objects will be categorised depending on their economic, political and social importance (that is, there will be three categories of importance). Depending on the relevant category of importance, specific rules and requirements will apply with respect to security measures to be implemented.

Finally, the Sovereign Internet Law was adopted (Federal Law No. 90-FZ ‘On Amendments into the Communication Law and the Information Law’) in May 2019 and on 1 November 2019 the majority of its provisions will come into force in Russia. The main purpose of the Sovereign Internet Law is to create an autonomous system that can support the operation of the Russian segment of the internet in the event of disconnection from the global network.

The Sovereign Internet Law imposes a number of obligations on certain categories of persons (communication service providers, owners of various communication networks’ infrastructure as well as information dissemination organisers (e.g., social networks, mail services), as well as establishing a specific register of internet exchange points (‘register’). The obligations imposed include:

a providing certain information to Roscomnadzor, information on the purpose of using a communication line that crosses the Russian border, and the means of communication installed on it;

b participating in drills arranged by Roscomnadzor;
restricting interaction between networks (e.g., by allowing only the use of the internet exchange points listed in the register) and prohibiting owners of internet exchange points from connecting communication networks to internet exchange points when such networks fail to comply with the requirements of the law; and

installing hardware and software tools that enable Roscomnadzor to monitor traffic, including access to resources blocked in Russia.

Separately, the Sovereign Internet Law addresses threats to the stability, security and integrity of the internet in Russia. At present, no list of these possible threats has been adopted. However, the main idea is that, in response to the threat, Roscomnadzor can centrally manage public communication networks by issuing mandatory instructions to persons subject to the requirements of the law or through special technical means. These technical means will be mandatorily installed by communication service providers. The Law provides for the adoption of a number of regulations surrounding its application.

IV SPECTRUM POLICY

i Development

The allocation of frequency bands and frequencies in Russia is based on the following principles:

a the use of specific frequency spectrum is granted by licence;
b there is a gradual move towards bringing Russian regulations on frequency allocation into line with international regulations on frequency allocation;
c the state shall have priority in terms of frequency allocation;
d the use of the frequency spectrum shall be provided on a commercial basis (i.e., for a fee); and
e frequency bands, frequencies and RF channels may only be allocated for a fixed period of time.

The Communication Law establishes that electromagnetic spectrum shall be allocated by the State Commission for Radio Frequencies (Frequency Commission), subject to the approval of the government.

The frequency allocation table adopted by the government further specifies which frequencies are intended for fixed satellite services, broadcasting satellite services and mobile satellite services; and which frequencies shall be used for government purposes or civil purposes, or which are intended for shared use.

RF bands are assigned for 10 years or for a shorter term. At the request of the user of the RF spectrum, this term may be extended or reduced.

As a general rule, the following permissions must be obtained to use frequency bands in Russia: an individual decision of the Frequency Commission regarding the allocation of a frequency band; a telecommunication service licence (or licences, as the case may be); and a permit from Roscomnadzor to use specific frequencies within the allocated frequency band.

The regulatory landscape in this area has not changed much during the past few years. However, there have been some simplifications made in respect to the allocation of certain frequency bands (see below).
Flexible spectrum use

Although Russian laws and regulations in this area are rather strict and do not provide for much flexibility, the frequency allocation procedure has been simplified in certain ways.

For instance, very small aperture terminal stations operating in the Ka-band and Ku-band do not require individual decisions of the Frequency Commission provided that certain technical requirements and limitations are met (under Decree of the Frequency Commission No. 10-06-01-3, dated 19 February 2010, and Decree No. 10-06-01-2, dated 19 February 2014).

However, despite the above, this area is quite heavily regulated and does not provide much room for manoeuvre. As regards the growing demand for spectrum for the next-generation services, the Russian governmental authorities are still reluctant to shift their priorities from the state interests to the development of new technologies. For instance, in August 2019, the state authorities refused to ‘clear’ 3.4–3.8 GHz frequencies for 5G developing technologies by keeping them at the disposal of the Ministry of Defence and the Russian Federal Space Agency.

Broadband and next-generation mobile spectrum use

General rules apply to the allocation of spectrum for next-generation mobile services, and all necessary authorisations for such services are normally granted via tenders.

For instance, while deploying 4G infrastructure in Russia, several major mobile communication network operators and state-owned telecommunication companies have expressed strong interest in building their own 4G networks, which resulted in a strong conflict of interests in the Russian telecom market that involved communication authorities at all levels, the FAS and top state officials.

As a result, four Russian telecommunication operators have been granted authorisations for 4G services in Russia.

5G services in Russia are at the early stages of development.

Thus, the governmental authorities as well as major Russian communication operators are still investigating the most efficient scenarios for the development of the 5G infrastructure, and, as a result, the deployment plans are subject to changes. For instance, it was initially expected that 5G infrastructure would be deployed in the five largest Russian cities by 2022. However, this plan has been abandoned for the moment, and it is now expected that 5G deployment will be started in certain industrial zones first.

In addition, some of the territories for testing of 5G infrastructure (‘pilot zones’) have been identified, and it is expected that 5G services will be launched in some of them by the end of 2019 (including in some areas of Moscow).

Furthermore, it is expected that incentives (including state financing) will be provided to local (Russian) telecom producers to develop and launch the production of 5G equipment in Russia. Thus, it is expected that the required research and design work will be completed between 2019 and 2021 and production will be launched between 2022 and 2024.

Spectrum auctions and fees

Tenders are held when the required RF allows for only a limited number of network operators to be active within the relevant territory.

The Russian legislative acts on communication also establish that users of frequency spectrum shall pay both a one-off fee and an annual fee for the use of frequencies. The level of the fees and the payment procedures are established by the government.
V MEDIA

i Regulation of media distribution generally

Content restrictions imposed on the mass media are mainly driven by moral and security reasons. For instance, the following content is prohibited:

a the calling for and promotion of violence, terrorism, any extremist activities and any type of criminal offences;
b influencing the unconscious mind;
c disclosing information and secrets protected by law; and
d the promotion of narcotics, psychiatric substances, drug precursors, etc.

Under certain circumstances, network operators may be also held liable for the content of the media that is distributed via their communication network.

ii Internet-delivered video content

The Information Law regulates the activities of the owners of online audiovisual services (online video services, online cinemas).

The Information Law, as amended in July 2017, defines the owner of audiovisual services as the owner of a website, website pages, an information system or computer programmes that are used to create or organise the distribution of audiovisual works on the internet, subject to the following criteria being met: access to such audiovisual works is provided for a fee or on the condition that the viewers also watch advertisements, or both; and the audience over 24 hours exceeds 100,000 users that are located in Russia. Certain exemptions are listed by the Law. For instance, online mass media that are registered as such in Russia, search engines and information resources where users primarily publish or post their own works and materials by themselves (social networks) are excluded from the scope of the new regulations.

In a nutshell, the owners of audiovisual services are subject to a number of obligations and requirements, namely:

a not to allow the dissemination of certain information such as extremist materials;
b to install specific software that determines the number of users;
c to make publicly available a valid email address to receive legally significant messages, as well as details of the owner of online audiovisual services; and
d to provide for age-based classifications of content.

Roscomnadzor maintains a specific register of audiovisual services, and may request from the potential owners of unregistered audiovisual services all information that is required to add the service to the register.

There is also a number of ownership requirements and limitations as to foreign participation in the owners of online audiovisual services (see Section II.iii).

VI THE YEAR IN REVIEW

The main trend and key legislation and policy developments in the TMT sector in Russia relate to further amplification of state control in the sector. For instance, the highly debated Sovereign Internet Law was viewed by the business community and wider public as aimed at censoring and isolating the Russian internet from the global worldwide network.
VI CONCLUSIONS AND OUTLOOK

The development of the TMT sector in Russia is to a very large extent driven by the political context, and is mostly aimed at strengthening state control over the communication sector and limiting privacy.
I OVERVIEW

The government continues to recognise and places much emphasis on the importance of TMT in society. For the fiscal year ending March 2020, the government is projected to launch tenders in the information and communications sectors worth approximately S$2.7 billion, a slight increase from the S$2.6 billion set aside in FY2018. Of the S$2.7 billion earmarked for the 2019 fiscal year, more than S$1.62 billion has been allocated to supporting Singapore’s digital transformation efforts. One major digital transformation project is the National Digital Identity (NDI) system, which is one of Singapore’s six strategic projects to drive the pervasive adoption of technology in society and the economy through back-end whole-of-nation enabling systems. Citizens and businesses will be issued crypto-based digital credentials to transact with the government more seamlessly and securely without the need for physical tokens or SMS passwords. Another project is Singapore Tourism Board’s Singapore Visitor Centre system, which aims to help officers make more tailored recommendations to tourists. The government also plans to issue bulk tenders for companies to provide software tools and consultancy services in the area of robotic process automation to support the growth of current government services, and for Agile project development and management methodology and ICT technical specialist services to support the co-sourcing of projects in the emerging tech areas of application development, data science, ICT infrastructure, geospatial technology, cybersecurity, sensors and the IoT.

This sustained ICT expenditure will be used to speed up Singapore’s digital transformation and continue its push to become a smart nation under the Smart Nation initiative that was introduced by Prime Minister Lee Hsien Loong in November 2014. The initiative aims to transform the daily life of Singaporeans by more fully integrating life with technology and making technology more accessible to the masses. The government has indicated that it will adopt a whole-of-government, whole-of-nation approach to this, and has set up a dedicated Smart Nation Programme Office under the Prime Minister’s Office to promote the greater integration of technology. The futuristic vision of the initiative is seen in the intention to develop, inter alia, technologies such as driverless cars, integrated 3D mapping and data analytics.

1 Ken Chia is a principal and Daryl Seetoh is an associate at Baker & McKenzie.Wong & Leow.
Smart Nation infrastructure, such as the Smart Nation Platform (SNP), which aims to facilitate the sharing of resources and data among government agencies to contribute to more efficient urban and operational planning as well as improve the running of city services, is already being developed.\(^5\)

The Smart Nation initiative is the newest iteration of the government’s plans to develop ICT usage and integration in Singapore, following the successful conclusion of the 10-year An Intelligent Nation 2015, A Global City, Powered by Infocomm plan (IN2015 Masterplan), which was introduced in 2005. On 11 August 2015, the Infocomm Media Masterplan Steering Committee released the Infocomm Media 2025 report (Infocomm Media 2025), which maps out a holistic plan for developing Singapore’s infocomm media sector over the next 10 years. Infocomm Media 2025 enables and complements the Singapore Smart Nation vision and provides broad directions under three strategic thrusts to further strengthen the infocomm media landscape of Singapore. More recently on 5 June 2018, the government also released its Digital Government Blueprint for building a digital government that ‘uses data, connectivity and computing decisively to re-engineer business processes, re-architect technology infrastructure and transform services for citizens, businesses and public officers’.

The Digital Government Blueprint sets the 2023 goal of getting all Singapore citizens and businesses to cross the digital divide and be able to access all government services at any time, anywhere on an internet enabled device.\(^6\) This follows the Digital Readiness Blueprint released on 2 June 2018, which sets out the government’s strategy for equipping Singapore citizens for digital access, literacy and participation, so that every citizen, young or old, will be able to be a part of the Singapore Smart Nation vision. Some recommendations in the Digital Readiness Blueprint include making access to basic digital enablers (i.e., a network-connected mobile device, internet access, a bank account with card facilities and a national digital identity) as widespread as possible, building up a basic digital skills curriculum for Singapore’s youth, further enhancing the public–private sector collaboration for increased digital participation and inclusion in the community, and promoting digital inclusion by design in Singapore’s digital ecosystem so that the impediments preventing people from using digital products and services are overcome.\(^7\)

Singapore’s success in developing its ICT industry is apparent. As of 2017, total ICT industry revenue reached S$199.2 billion.\(^8\) The number of ICT professionals has also increased year on year, with over 28,500 new ICT professionals projected to be required by the sector from 2018 to 2020.\(^9\) The ICT sector is believed to contribute to approximately 8 per cent of Singapore’s gross domestic product.\(^10\) Singapore was placed first in the World Economic Forum’s Global Information Technology Report 2016, which ranks countries in terms of their ability to leverage ICT as an enabler of sustainable, long-term economic growth.


\(^8\) [https://www2.imda.gov.sg/infocomm-media-landscape/research-and-statistics/infocomm-industry#1](https://www2.imda.gov.sg/infocomm-media-landscape/research-and-statistics/infocomm-industry#1).


\(^10\) [https://www.todayonline.com/singapore/42000-ict-professionals-needed-over-next-3-years-yaacob](https://www.todayonline.com/singapore/42000-ict-professionals-needed-over-next-3-years-yaacob).
As of June 2019, the number of fixed-line subscribers remained steady at approximately 2,004,600, representing a 35.6 per cent penetration. Further, as of May 2019, the amount of mobile subscribers was approximately 8.69 million (up from 8.34 million the previous year). Mobile population penetration as of May 2019 sits at 154.1 per cent, and there remained 5,500 dial-up internet subscribers (0.1 per cent penetration) in Singapore as at December 2018. Broadband internet subscriber figures decreased slightly, with approximately 12.0 million subscribers (94.7 per cent penetration by household for wired broadband and 185.6 per cent penetration for wireless broadband). By comparison, the figures on 1 April 2000 (at the start of liberalisation) were 1.876 million fixed-line subscribers, 1.63 million mobile subscribers and 1.711 million dial-up internet subscribers (no broadband services were available at that time).

II REGULATION

i The regulators

In the late 1980s, the government announced plans to privatise the telecommunication and postal services then being provided by the Telecommunication Authority of Singapore. Singapore Telecommunications Pte Ltd and Singapore Post Pte Ltd were subsequently incorporated in Singapore on 28 March 1992, and acquired all the necessary properties, assets and liabilities held by the Telecommunication Authority of Singapore in connection with the provision of such services.

The Singapore Broadcasting Authority was set up as a statutory board under the former Ministry of Information and the Arts – currently Ministry of Communications and Information (MCI) – in 1994. Formed in response to the privatisation of Singapore’s broadcasting industry, the Singapore Broadcasting Authority played a central role in the regulation and promotion of the broadcasting industry in Singapore. The Singapore Broadcasting Authority worked closely with the Economic Development Board, the National Computer Board and the Telecommunication Authority of Singapore to develop Singapore as a regional broadcasting hub. To provide a single agency for integrated planning, policy formulation, regulation and industry development of the IT and telecommunications sectors, a new Info-communications Development Authority of Singapore (IDA) was formed as a result of the merger between the Telecommunication Authority of Singapore and the National Computer Board in 1999. The Media Development Authority (MDA) was formed on 1 January 2003 by the merger of the Singapore Broadcasting Authority, the Films and Publications Department and the Singapore Film Commission to champion the development of a vibrant media sector in Singapore. The MDA regulates content delivery across various platforms, including television, radio, videos, internet and publications.

As part of the Infocomm Media 2025 plan, the government announced on 18 January 2016 that the IDA, MDA and Personal Data Protection Commission (PDPC)

---


12 The MCI was previously known as the Ministry of Information, Communications and the Arts, but was renamed with effect from November 2012 with the formation of a new Ministry of Culture, Community and Youth.
would be restructured by the end of 2016 into two new statutory boards, the Infocomm Media Development Authority of Singapore (IMDA) and GovTech, both of which were formed on 1 October 2016.

On 16 August 2016, the Parliament passed the Government Technology Agency Bill (GovTech Bill) and Info-communications Media Development Authority Bill (IMDA Bill). The GovTech Bill legislates the creation of GovTech, while the IMDA Bill establishes the IMDA and officially merges certain functions of the IDA with the MDA.

The new IMDA develops and regulates the converging infoComm and media sectors in a holistic way, and implements the Infocomm Media 2025 plan for Singapore. The new IMDA also deepens regulatory capabilities for a converged infoComm media sector, safeguarding the interests of consumers and fostering pro-enterprise regulations. The IMDA takes over the regulatory framework previously overseen by the IDA and MDA, such as the Telecommunications Act (Telecoms Act), the Postal Service Act, the Broadcasting Act and the Films Act. The PDPC will form part of the IMDA, and will continue to oversee personal data protection regulation in Singapore.

GovTech was established at the end of 2016 to lead digital technological transformation in the public sector. From 1 May 2017, GovTech has reported to the new Smart Nation and Digital Government Group under the auspices of the Prime Minister’s Office. GovTech has been tasked with building a more intuitive and anticipatory government through digital service delivery with technologies and ensure that people are always at the heart of digital service transformation for the public sector. As the nexus of technology and engineering capability within the government, GovTech is well-placed to help government agencies capitalise on the speed of innovation and new technology trends such as robotics, artificial intelligence, IoT and big data. The new organisation plays a vital role in supporting Singapore’s Smart Nation vision, especially in delivering the SNP and Smart Nation applications. GovTech also focuses on developing new technology capabilities as well as attracting and nurturing ICT engineering talent that will provide a strong foundation for Singapore’s Smart Nation ambitions.

ii Regulated activities

The Telecoms Act gives the IMDA monopoly powers to operate and provide telecommunications systems and services. The IMDA’s key functions include:

- exercising licensing and regulatory functions in respect of telecommunication systems and services in Singapore;
- the allocation and use of satellite orbits and RF spectrum;
- exercising regulatory functions in respect of determinations;
- approval of prices, tariffs and charges; and
- the provision of telecommunication and other related services.

The IMDA is empowered to grant, modify or suspend the licences of telecommunication operators, and to sanction offences under the Telecoms Act. There is a general prohibition on the running of telecommunication services in Singapore unless they have been licensed by the IMDA under Section 5 of the Telecoms Act.

---

The IMDA uses a two-tiered framework for the licensing of telecommunication operators. An operator who intends to deploy or operate any form of telecommunication network, systems or facilities for the purpose of providing telecommunication or broadcasting services outside its own property boundaries to third parties (who may include other licensed telecommunication operators, business consumers or the general public) is required to possess an FBO licence. On the other hand, an operator who intends to lease telecommunication network elements (such as transmission capacity and switching services) from any FBO licensee so as to provide its own telecommunication services, or to resell or promote the telecommunication services of FBO licensees to third parties, is required to apply for a SBO licence. An SBO licence is also required to deploy telecommunication networks, systems and facilities within the operator's own property boundaries in order to offer telecommunications services to third parties resident within their property boundaries.

The IMDA may also formulate and develop infocomm-related policies, as well as standards, codes of practices and advisory guidelines – all of which it can enforce – pertaining to issues such as licensing, interconnection, resource, assignment of spectrum rights and competition management. Mergers and acquisitions of telecommunication licensees are regulated under the Code of Practice for Competition in the Provision of Telecommunication Services 2012 (Telecoms Competition Code), which is enforced by the IMDA. Under this Code, all licensees are also required to interconnect with each other, whether directly or indirectly, to ensure seamless any-to-any communications throughout Singapore. The IMDA may grant exemptions from specific provisions of the Code where good cause is shown. The Telecoms Competition Code has also been amended for the purposes of alignment with the Singapore Personal Data Protection Act 2012 (PDPA), the key data protection provisions of which came into effect on 2 July 2014.

The IMDA is also empowered to grant licences in respect of broadcasting services and broadcasting apparatuses. No person is allowed to provide any of the licensable broadcasting services set out in the Second Schedule of the Broadcasting Act without a valid broadcasting licence issued by the IMDA. These services include free-to-air television or radio services (localised, nationwide or international), subscription television or radio services (localised, nationwide or international), special-interest television or radio services, audiotext, videotext or teletext services, VOD services, broadcast data services and online computer services. Some of the licensable broadcasting services (including audiotext, videotext and teletext services, broadcast data services and online computer services) are class-licensed by the IMDA under the Broadcasting (Class Licence) Notification (Notification).

The Code of Practice for Market Conduct in the Provision of Mass Media Services (MMCC) was issued by the then MDA in 2003 to promote fair market conduct and effective competition in the broadcasting and print sectors. The MMCC was significantly revised in 2010 to, inter alia, impose obligations around the cross-carriage of exclusive content in the pay-TV market, and further revisions were made to enhance consumer protection in the pay-TV sector in early 2016.

Unfair methods of competition and anticompetitive practices are expressly dealt with in the MMCC. These regulations also ensure that media players do not unfairly leverage their own or their affiliates' significant market power in a media or non-media market.

Mergers of any dominant media player with another media player (whether dominant or not) would require the IMDA's approval for consolidation. As such, this will assist in addressing potential anticompetitive issues arising from convergence and merging of portfolios of various players in the market.
In the event a particular media resource is declared to be an essential resource by the IMDA (i.e., the resource must be used by another media licensee, but such resource cannot be created within the foreseeable future or cannot be obtained from a third party at a cost to allow it to compete efficiently), access to such essential resource must be provided on reasonable and non-discriminatory prices, terms and conditions.

iii Ownership and market access restrictions

Full market competition in the telecommunications sector was introduced in April 2000. Direct and indirect foreign equity limits for all public telecommunications services licences were removed, and licensees were free to decide on the types of networks, systems, facilities and preferred technology platform to offer their services. The limits on the number or type of licences were also removed, except when there are physical or resource constraints.

In general, there are no foreign ownership restrictions on FBO or SBO licensees. However, an FBO licensee will be required to be a company incorporated under the Singapore Companies Act. An SBO (individual) licensee may be a company incorporated or a foreign company registered under the Companies Act, while an SBO (class) licensee may (in addition) be a limited liability partnership or limited partnership.

The Broadcasting Act regulates the ownership of broadcasting companies in Singapore. A broadcasting company is a company (or a holding company) incorporated or registered under the Companies Act that holds a free-to-air licence; any broadcasting licence under which a subscription broadcasting service may be provided (in each case where such licence permits broadcast that is capable of being received in 50,000 dwelling houses or more, but does not include a class licence); or any other broadcasting licence as the Minister of Communications and Information may from time to time specify in the public interest, or in the interest of public security or order or national defence.

There are also controls on the shareholding and voting power of broadcasting companies. For example, substantial shareholdings (i.e., an aggregate of more than 5 per cent of the nominal amount of all voting shares) in a broadcasting company and other forms of controlling shareholdings are subject to the Minister’s approval. Broadcasting companies in Singapore must also ensure that at least half of their directors are citizens of Singapore, unless the IMDA approves otherwise. The IMDA also has the right to approve the chief executive officer of a broadcasting company, as well as its directors and chair.

Further, there are media cross-ownership restrictions that provide that no regulated person shall be merged or consolidated with, or taken over by, any other regulated person, or any other person (not being a regulated person) carrying on business in any media industry, without the prior written approval of the IMDA.

iv Transfers of control and assignments

Generally, licences cannot be transferred from a licensee to a third party. For telecommunication licensees, the IMDA’s approval is required for any consolidation involving an FBO or SBO licensee that the IMDA has declared to be a designated telecommunication licensee pursuant to Section 32A(2) of the Telecoms Act that would result in an entity holding an ownership interest in the licensee of 12 per cent or more. For acquisitions of between 5 and 12 per cent, the IMDA is required to be notified, unless such acquisitions occur by virtue of certain prescribed transactions set out in the Telecommunications (Prescribed Transactions) Order 2012.
A consolidation application needs to be filed either separately or jointly by both parties, together with a competitive impact and public interest statement. The short-form consolidation application procedure, with an abbreviated statement, may be used if the consolidation is a horizontal consolidation that will not result in the post-consolidation entity having more than a 15 per cent share in the telecommunication market in Singapore; or if the consolidation is a non-horizontal consolidation in which none of the applicants has more than a 25 per cent share of any telecommunications market, whether in Singapore or elsewhere, in which it participates.

The IMDA will not approve a consolidation application where it determines that the consolidation is likely to substantially lessen competition in any telecommunications market in Singapore or harm the public interest. The IMDA may approve the consolidation application with or without conditions.

The IMDA will ordinarily complete its consolidation review within 30 days of the start of the consolidation review period. In any case in which the IMDA determines that a consolidation application raises novel or complex issues, it may extend the review period by up to 90 days, to a maximum of 120 days. Where appropriate, the IMDA will provide the public with an opportunity to comment on a request or a consolidation application.

For media licensees, the IMDA’s prior written approval is required for any consolidation between regulated entities, including broadcasting licensees.

For the purposes of the MMCC, a consolidation means a merger, acquisition, takeover or other similar transaction that results in two entities that were previously independent economic entities becoming – as a practical matter – a single economic entity, including by way of an asset purchase or the setting up of a new joint-venture vehicle into which significant assets of the entities will be transferred. Part 8 of the MMCC requires all regulated persons seeking to enter into a consolidation with another regulated person or any other person (not being a regulated person) that provides mass media services or ancillary media services to submit a consolidation application within 30 days of the day on which they entered into a consolidation agreement.

Both entities must jointly submit a consolidation application with a statement that provides a clear, accurate and comprehensive description of the proposed consolidation, a good-faith assessment of the likely impact of the proposed consolidation on competition in any mass media services market and a discussion of why approval of the proposed consolidation would serve the public interest.

As the IMDA may make statements available to the public, applicants should put proprietary or commercially sensitive information in a separate appendix and request its confidential treatment. The consolidation agreement (and any public statement regarding the proposed consolidation) must include language expressly stating that the consolidation will not be consummated unless and until such time as the IMDA grants written approval. The IMDA will ordinarily complete its review of the consolidation application within 30 days of the start of the consolidation review period (i.e., when the applicants submit a consolidation application that contains all materials required pursuant to Part 8 of the MMCC), but this can be extended up to a maximum of 120 days where novel or complex issues are raised, and 180 days in extraordinary cases.

There is a short-form application procedure for cases in which a proposed consolidation is unlikely to raise significant competitive issues. The IMDA will generally grant approval for any application that is eligible for this procedure without significant review based on the applicant’s abbreviated description, competitive impact and public interest statement. The
two cases when this procedure can be used are when the proposed consolidation is unlikely to result in the post-consolidation entity having a market share of 40 per cent or more of any media market in Singapore; or a market share of between 20 and 40 per cent of any media market in Singapore, and the post-consolidation combined market share of the largest three regulated persons or ancillary media service providers, or a combination thereof, is 70 per cent or more of any media market in Singapore.

The IMDA can impose structural and behavioural conditions as part of its approval.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

The IMDA regulates the carriage of internet and IP-based services and the content delivered on these various platforms. For example, if one were to deploy a telecommunication network or system to provide internet or IP-based services, one would have to apply to the IMDA for an FBO licence. For provision of internet or IP-based services over leased telecommunication network elements, an SBO licence will be required.

Provision of IP telephony services in particular requires an SBO (individual) licence. Licensees must likewise adhere to the National Numbering Plan provided by the IMDA, which sets out rules and guidelines for the use and assignment of numbers to telephone services delivered over the PSTN radio network (collectively, the paging network, cellular mobile network and trunked radio network) and the internet or other IP-based network. In general, numbers beginning with ‘3’ are reserved for use in the IP telephony service, while numbers beginning with ‘6’ are reserved for use in PSTN and IP telephony services.

ii Universal service

Since 2000, the government has rolled out the Singapore ONE project to provide nationwide broadband access over ADSL and cable to households in Singapore, and subsequently over fibre through the Next Generation National Broadband Network project. With full market liberalisation over recent years, the broadband household penetration rate has risen steadily from 7 per cent in December 2000 to a residential wired broadband household penetration rate of 94.7 per cent (residential wired broadband penetration rate only) in May 2019.14

In the area of wireless broadband access, the government appointed three operators to launch a nationwide wireless broadband programme called Wireless@SG in December 2006. This service aims to extend free wireless broadband access to the public in high human-traffic areas, and is available at about 7,500 hotspots around the island. Access speeds were doubled to 1Mb/s from 512kb/s from 1 September 2009 to allow users to enjoy better access to media-rich and interactive websites and bandwidth-intensive services. The most recent phase of this free Wi-Fi service (from 1 April 2013 to 31 March 2019) is offered by the three mobile operators, Y5Zone Singapore Pte Ltd and MyRepublic.15 Interoperable SIM-based authentication for automatic log-in to the network has been implemented from 1 April 2014 to supplement the web-based and seamless secure access login methods. On 29 April 2017, it

was announced that Wireless@SG would allow automatic login to non-SIM devices, which will eliminate the need to log in using usernames and passwords. Further, having identified Wireless@SG as a key enabler of Singapore’s Smart Nation initiative, the government has announced that the IMDA is on track to double its network of hotspots to 20,000 by 2018, reaching more locations such as public hospitals, hawker centres and government service centres. This is an increase from the 10,000 hotspots running at 5Mbps in 2017.

The government has also invested about S$1 billion to fund the deployment of the Next Gen National Broadband Network (NBN), a nationwide FTTH network. The Next Gen NBN is designed to be an open access network, and comprises three key industry layers. The network company (NetCo) designs, builds and operates the passive infrastructure layer, while the operating company (OpCo) designs, builds and operates the active network components to provide wholesale bandwidth connectivity to retail service providers. The NetCo must be structurally separated from the other industry layers, while operational separation is imposed on the OpCo.

It is envisioned that the Next Gen NBN will provide nationwide ultra-high-speed broadband access of 1Gb/s and beyond to all physical addresses, including homes, schools, government buildings, businesses and hospitals. The deployment of the Next Gen NBN commenced in 2009, and commercial services on the new fibre-optic network have been launched by all major telecommunication service providers. With the levelling of the playing field, a number of smaller ISPs, including MyRepublic, ViewQwest, OSINet and LGA Telecom, has joined the three existing operators in offering new high-speed packages to commercial and residential broadband subscribers. The coverage of the Next Gen NBN has reached over 95 per cent, with more than 560,000 subscribers signed up to services from approximately 15 retail service providers.

iii Restrictions on the provision of service

Dominant licensees are subject to tariff-filing requirements in respect of certain services, such as standardised services designed for residential customers, standardised services designed for business customers, services designed for specific customers, promotional services, and certain resale and wholesale services. The IMDA will determine whether a proposed tariff is just and reasonable. Non-dominant licensees are not subject to the tariff-filing requirements. Dominant licensees are also required to provide services on non-discriminatory terms.

There is a duty imposed on FBO and SBO licensees that use switching or routing equipment to provide services to the public to interconnect with other licensees. There is also a duty on public telecommunication licensees to provide a basic telephone service to any person in Singapore who requests the provision of such service. Otherwise, licensees have the latitude to choose the customers and the content they carry. There are no specific network neutrality obligations currently imposed on licensees, albeit ISPs must meet the minimum broadband quality-of-service standards to ensure a reasonable broadband internet experience for end users. ISPs are allowed to implement reasonable network management practices and

offer niche or differentiated internet service offerings provided that they satisfy the IMDA's requirements on information transparency and fair competition, and do not amount to blocking of legitimate internet content.

Network operators must take reasonable measures to prevent the unauthorised use of end user service information (EUSI). Network operators may intercept messages for the purpose of providing assistance to law enforcement, judicial or other government agencies.

iv Security

Regulatory and legislative policies governing the internet and IP sector as well as national security issues have evolved in tandem to adapt to the changes on each side.

Unauthorised access to, or modification of, computer material would constitute offences under the Computer Misuse and Cybersecurity Act (CMCA). Unauthorised use or interception of computer services would also constitute offences, and enhanced punishment is provided for offences involving protected computers (e.g., computers used in connection with national security or defence, law enforcement, public key infrastructure, and essential emergency and public safety services). The CMCA was amended in January 2013 and further amended in April 2017 to provide the government with greater powers to implement countermeasures against cyberattacks on critical infrastructure. In particular, where the relevant minister is satisfied that it is necessary for the purposes of preventing, detecting or countering any threat to the national security, essential services, defence or foreign relations of Singapore, that minister may authorise or direct any person or organisation to take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer service, or any class of computers or computer services. The definition of essential services was also widened to include services relating to land transport infrastructure, aviation, shipping and health services. The amended CMCA now criminalises the dealing in personal data obtained via a cybercrime without a legitimate purpose (e.g., journalistic reporting) as well as dealing in hacking tools with the intention of committing or facilitating the commission of a computer offence.

Apart from the offences provided for under the CMCA, the government has launched the National Cyber Security Masterplan 2018 (NCSM2018) to enhance Singapore’s resilience against cyberthreats. The NCSM2018 aims to reinforce Singapore’s cybersecurity by intensifying efforts in the government and critical infocomm infrastructure as well as the wider infocomm ecosystem, which includes businesses and individuals. Complementary to the NCSM2018 is the National Trust Framework, which was conceptualised as part of the iN2015 Masterplan to provide a national framework that provides greater assurance and trust. One of the key initiatives is establishing a national authentication framework, which will enhance the security of online transactions through the deployment of a nationwide-strong authentication platform.

A National Cyberthreat Monitoring Centre has also been established to provide the government with the capability for early detection of potentially devastating cyberattacks and the ability to respond to cybersecurity incidents in real time. Further, a major initiative launched in April 2015 was the new Cyber Security Agency (Agency), Singapore’s apex cybersecurity watchdog created to develop national cybersecurity strategy and policy, and to coordinate cyber-related operations between the multiple government agencies and departments. The need for the Agency has only grown as the number of cybersecurity incidents in Singapore continue to increase, with notable cyberattacks such as the hacking of the Prime Minister’s Office website in 2013, and the illegal accessing of over 1,000 SingPass accounts, which store crucial citizen information and provide access to important government websites, in 2014,
breaches of the IT systems of the National University of Singapore, Nanyang Technological University and Singapore Armed Forces over separate incidents in 2017, and, most recently, the theft of the personal data of 1.5 million patients of SingHealth (Singapore’s largest group of healthcare institutions), including that of the Prime Minister, on July 2018. Concurrently with the aim of increasing the strength of Singapore’s cybersecurity, the Economic Development Board and the Defence Science and Technology Agency have also stepped up efforts to recruit talent for the cybersecurity industry, with the latter conducting outreach to young Singaporeans through its Cyber Defenders Discovery Camp. The Agency carried out its first cybersecurity tabletop exercise for the banking and finance sectors, test-driving responses to hypothetical cyber incidents, in May 2015.

The Singapore Common Criteria Evaluation and Certification Scheme (SCCS), which was established in May 2005 as part of the iN2015 Masterplan, also aims to enhance cybersecurity. The SCCS allows infocomm companies to evaluate and certify their security products against the common criteria (CC) standard (ISO/IEC 15408) in Singapore. The framework of the CC is based on the Common Criteria Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, a set of publicly available standards that define the criteria for evaluating IT security properties.

Material that has a subversive tendency or compromises national interests, public order or security may be prohibited under the Internal Security Act. This includes material that:

- contains any incitement to violence;
- counsels disobedience regarding the law or any lawful order;
- is calculated or likely to lead to a breach of the peace, or to promote feelings of hostility between different races or classes of the population; or
- is prejudicial to the national interest, public order or security of Singapore.

The transmission of false threats of terrorist acts (e.g., bomb hoaxes) is also penalised under Regulation 8(1) of the United Nations (Anti-Terrorism Measures) Regulations, read with Section 5(1) of the United Nations Act. In some cases, such offences are prosecuted under Section 45 of the Telecoms Act, which contains a general prohibition against the transmission of a false or fabricated message through the telecommunications system.

The Sedition Act has also been used against persons who post racist or other incendiary remarks on the internet. The Sedition Act makes it an offence for a person to:

- commit or attempt to commit any act that has or that would have a seditious tendency;
- utter any seditious words;
- print, publish, sell, offer for sale, distribute or reproduce any seditious publications; or
- import any seditious publications.

Material that may potentially fall foul of the Sedition Act includes material that excites disaffection against the government or the administration of justice in Singapore, or excites hatred or contempt against it, and material that promotes feelings of ill will and hostility between different races or classes of the population of Singapore.

Under the Internet Code of Practice (the Internet Code), prohibited material is not allowed to be provided on the internet by any licensee under a class licence. The term prohibited material includes material that is objectionable on public interest, public morality, public order, public security and national harmony grounds. Similarly, the various television content codes provide that content provided on television should not undermine public security interests or public confidence in the law and its enforcement in Singapore.
The IMDA has worked with three ISPs in Singapore to provide family access networks (FANs) or filtering services that parents can subscribe to for their children. FANs assist parents who may be unfamiliar with standalone filtering software by filtering out pornographic and other undesirable sites. Parents can contact their respective ISPs to subscribe to the filtering services or can otherwise opt to purchase other internet-filtering software from the market.

The IMDA has also mandated that ISPs in Singapore are required to promote the use of internet filters, including filters for mobile devices, at the point of sale and upon renewal of the subscription agreement. It is hoped that this move will raise the awareness of parents and encourage the use of such filters to protect the young from inappropriate content. The first internet filtering service for mobile devices such as smartphones and tablets has been introduced by one of the major telecommunications service providers in Singapore.

v   Data protection and privacy
On 15 October 2012, the Parliament passed the PDPA, which establishes a baseline data protection framework that applies to all organisations in the private sector. Inter alia, it establishes notification and consent requirements for the use, collection and disclosure of personal data, establishes restrictions on the transfer of personal data abroad and places protection obligations on the private sector. The PDPA also establishes a do-not-call registry, which aims to provide individuals with a simple and efficient way to opt out of receiving unsolicited marketing messages.

On 2 July 2014, the Personal Data Protection Regulations (PDPR) came into force. The PDPR expand on, inter alia, the PDPA’s Access and Correction Obligation and Transfer Obligation. In particular, the PDPR require organisations to respond to each access request as accurately and completely as necessary, and as reasonably possible, within 30 days of such request being made. However, if an organisation is unable to comply with this requirement, it must (within the 30-day period) inform the applicant in writing of the date by which it will respond to the request.

Further, the PDPR require an organisation transferring personal data outside Singapore to take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore is bound by legally enforceable obligations to provide for the transferred personal data a standard of protection that is at least comparable with the protection under the PDPA.

Under the Telecoms Competition Code, there is a prohibition on all FBO and SBO licensees from unauthorised use of any EUSI. EUSI consists of all information that the licensee obtains as a result of an end user’s use of its telecommunication services, and includes the end user’s usage patterns, services used, telephone number and network configuration, location information as well as the billing name, address and credit history. Thus, unless the end user has provided prior consent, a licensee must not use EUSI for any purpose other than that as provided for in the Telecoms Competition Code.

vi   Spam control
The Spam Control Act (SCA) seeks to regulate the sending of spam (i.e., unsolicited commercial communications sent in bulk) by prescribing requirements that must be met before such communications may be sent. Such requirements include the provision of an unsubscribe facility and compliance with labelling and other requirements. The SCA applies to emails and mobile messages (i.e., text or multimedia messages sent via a mobile telephone) originating from or sent to a device located in Singapore, or where the sender or receiver of
the message is an individual or entity either physically present, or carrying on business or other activities, in Singapore. Sending of spam to electronic addresses obtained by way of a dictionary attack or address-harvesting software is prohibited under the SCA.

IV SPECTRUM POLICY

i Development

The IMDA is the regulatory body responsible for the utilisation of RF spectrum. It constantly monitors trends in and developments of new wireless technology, and reviews the frequency allocations whenever there is a demand for spectrum. In the past, spectrum was administratively allocated; however, the IMDA has recognised that in a liberalised environment, administrative allocation may not be the most objective, efficient or transparent means of ensuring that spectrum is effectively used. As such, the IMDA has moved towards a market-based approach by adopting an auction process where competing services in common bands cannot effectively share the same spectrum. For example, the IMDA has adopted the auction process for allocating spectrum for 3G services, 4G and wireless broadband access.

ii Flexible spectrum use

The spectrum of RFs in the VHF and UHF bands currently allocated for use, on a primary basis, for the provision of terrestrial broadcast services in Singapore are not all in use at any given time. Within this spectrum, there are interleaved and contiguous spectrum blocks that are not used to provide broadcast services. Such unused spectrum (white spaces) are situated below 1GHz, and radio signals within such spectrum have propagation characteristics that allow the signals to travel long distances and penetrate buildings easily. As such, the IMDA has invited interested parties to conduct trials to explore the various spectrum environments and regimes that white space technology can operate in, yet at the same time ensuring continued protection of licensed services in Singapore from possible interference during the trial period. One of the key objectives of the cognitive radio venues (CRAVE) trials is to examine how best to make use of the white space spectrum for the benefit of consumers and businesses. In April 2012, several organisations (I2R, StarHub and Microsoft) confirmed that they would lead the formation of a Singapore White Spaces Pilot Group to leverage on the CRAVE trials to establish Singapore as an innovation zone for white space technology. The pilot group intends to undertake commercial pilot deployments to explore how white space technology could supplement the existing wireless infrastructures and develop innovative consumer and business applications.

On 16 June 2014, the then-IDA issued its decision on the regulatory framework for the use of TV white space (TVWS) technology in Singapore after holding a public consultation. The then-IDA decision set out, inter alia, the inclusion of 700MHz band for TVWS deployment in the future, the adoption of the geolocation database approach as the mandated method for white space devices to access TVWS spectrum space and the implementation of unique white space devices identifiers.

In mid-2014, the then-IDA concluded a public consultation that sought to canvass industry views on the allocation of long-term rights in the 3.5GHz band, and planned services and target market segments for use of these bands. However, no further information from the IMDA has been forthcoming about the results of this consultation exercise.
Broadband and next-generation mobile spectrum use

To address the growing need for spectrum for broadband services and next-generation mobile services, apart from the white space trials, the IMDA is also reviewing current spectrum allocations to ensure the most efficient use. For example, it has identified certain spectrums for the future expansion of 3G services. In relation to the evolution of 4G spectrum bands, the IMDA is also aware of the necessity to ensure that there is adequate lead time for existing services to migrate to alternative modes of reception where necessary. With respect to 5G networks, which are expected to be up to 20 times faster than 4G networks, the IMDA is looking for a rollout of 5G network by 2020. In relation to wireless broadband services, the IMDA is looking into opening more spectrum for wireless broadband services, and has identified a certain bandwidth for mobile or wireless services.

One step that the IMDA has taken to expand 3G and 4G services is the closure of the 2G mobile network in April 2017, with the spectrum previously assigned to the 2G network being reallocated to provide faster and more advanced 3G and 4G services. These 2G users have had to upgrade to the 3G or 4G networks. The IMDA stopped accepting registrations of 2G-only mobile equipment in September 2015, and consumers have been advised not to purchase such equipment.

The government indicated in July 2010 that it would go ahead with a proposed auction of a fourth lot of spectrum in the 3G band (i.e., the 1,900/2,100MHz frequency band). This fourth lot of spectrum was left unallocated during the last round of auctions in 2001, when three lots of 3G spectrum were allocated to the three mobile operators in Singapore.

Pursuant to a public consultation process leading to this decision, respondents submitted feedback indicating that they generally agreed with the allocation of the remaining spectrum. However, three out of the four respondents (namely the existing mobile operators in Singapore) objected to the market allocation (i.e., allocation by way of auction) of the spectrum lots. The mobile operators instead suggested that the then-IDA allocate the spectrum administratively to them equally as a more cost-effective approach. Nonetheless, the then-IDA took the view that the auction mechanism ensured that scarce spectrum resources would be allocated in the most efficient and transparent manner.

However, only three applications were received from the existing mobile operators during the auction process. As such, the then-IDA allocated each of the available 3G spectrum lots to the respective bidders for the reserve price of S$20 million.

Where 4G spectrum is concerned, the then-IDA issued a public consultation paper in April 2012 on the proposed framework for the reallocation of spectrum for 4G telecommunication systems and services. Following the public consultation, the then-IDA announced on 16 January 2013 that it was putting up a total of 270MHz of 4G spectrum for auction, comprising 150MHz of spectrum in the 1,800MHz band and 120MHz of spectrum in the 2.5GHz band. The three mobile operators submitted initial offers for the spectrum, but the total amount of spectrum that they bid for did not exceed the amount available in each of the spectrum bands mentioned above.

As such, on 28 June 2013, the then-IDA provisionally awarded the 4G spectrum rights to the three mobile operators. M1 obtained 80MHz of spectrum, SingTel obtained 100MHz of spectrum and StarHub obtained 90MHz of spectrum. The placement of the spectrum lots acquired by the mobile operators will be determined in the next stage of the process (the assignment stage). These spectrum rights commenced on 1 July 2015 for spectrum in
the 2.5GHz band and on 1 April 2017 for spectrum in the 1,800MHz band, upon the expiration of the existing spectrum rights. The mobile operators may continue to provide mobile services (including 4G services) over their existing spectrum rights until then.

The mobile operators were required to provide nationwide 4G street level coverage by 30 June 2016, and coverage for Mass Rapid Transit underground stations and lines and road tunnels by 30 June 2018.

An additional total of 235MHz of spectrum was made available for auction for mobile services in the second half of 2016.

In 2017, the IMDA issued public consultations on key 5G technology developments and spectrum requirements. In mid-2019, the IMDA called for interested telcos to submit proposals of their 5G deployment plans, and the IMDA intends to assign 5G airwaves to two winning submissions. The Singapore government also announced an investment of S$40 million for 5G innovation. Application for the 5G Innovation Grant for use cases in four strategic clusters (Maritimes Operations, Urban Mobility, Smart Estates and Industry 4.0) is opened from June 2019 to May 2020. To facilitate the trials of 5G technology by industry, the IMDA is waiving frequency fees for certain frequency bands for technical trials and market trials for interested companies starting 31 December 2019.

Singapore is expected to benefit significantly from 5G networks and be the forerunner for 5G technology in ASEAN, with an expected penetration rate of 56.9 per cent by 2025. Reports by Cisco and A.T. Kearney also predict that the revenues of Singapore telco companies could increase by up to US$510 million by 2025 as a result of 5G mobile technology.

### Spectrum auctions and fees

The IMDA typically uses two schemes to charge users for access to the radio spectrum: market-based charging (auctions) or cost-based charging. Auctions are used to set a market-based charge for use in frequency bands in scarce supply. In frequency bands that are congested or potentially congested, the IMDA will set fees according to the opportunity cost of the spectrum. Cost-based charges are set to recover costs incurred in administering the use of the spectrum, such as frequency coordination, radio monitoring, interference investigations and frequency database management. In any event, the IMDA has moved away from administrative allocation, where feasible, to a market-based allocation approach using auctions, especially when assigning highly contested spectrum, so as to allow market forces to set the price.

The IMDA has also decided to use a new auction format after holding a public consultation on the reallocation of 4G spectrum. In the consultation paper, the IMDA proposed the use of a clock plus auction format, which is a variant of the simultaneous multiple round action and combinatorial clock auction formats commonly used in 4G communication.

---

18[https://www.straitstimes.com/singapore/singapore-aims-to-have-first-5g-applications-next-year-no-auction-for-airwaves-imda](https://www.straitstimes.com/singapore/singapore-aims-to-have-first-5g-applications-next-year-no-auction-for-airwaves-imda).


20[https://www2.imda.gov.sg/programme-listing/5G-Innovation/5G-Grant](https://www2.imda.gov.sg/programme-listing/5G-Innovation/5G-Grant).


auctions in other jurisdictions. Under the clock plus auction format that the IMDA has
decided to use for the main auction, bidders will specify demand for quantities of lots within
specified lot categories, subject to the relevant spectrum caps. In each round, there is a single
common price for all lots within a category, and this price ticks up over successive rounds
until there is no longer any excess demand.

v TPG Telecom wins IMDA’s spectrum auction to become Singapore’s fourth
mobile telecom company24

In an effort to encourage a fourth mobile telecom company to enter the Singapore market,
the IMDA held a highly anticipated new entrant spectrum auction (NESA) in the fourth
quarter of 2016. The NESA was first open only to interested pre-qualified parties that did
not operate a nationwide mobile network in Singapore, and offered a lower starting bid price
of S$35 million for the 60MHz of spectrum up for auction. A general spectrum auction
for additional spectrum followed thereafter at a higher reserve price, and was open to the
three incumbent mobile telecoms companies as well as any aspiring new entrants. Although
previous attempts to lure a fourth mobile operator into the market have been unsuccessful,
on 14 December 2016, the IMDA announced that TPG Telecom made a winning bid of
S$105 million in the NESA. The spectrum rights commenced in April 2017, and TPG
was required to utilise the allocated spectrum to provide nationwide street level coverage
for 4G within 18 months from the start of the new spectrum rights, with road tunnels
and in-building service coverage within 30 months.25 TPG achieved nationwide outdoor
coverage by the end of 2018. The entry of a new MNO is expected to enhance innovation
and competition in the mobile market.

vi Mobile virtual network operators

Since TPG’s entry, a number of telcos, including mobile virtual network operators (MVNOs)
have entered the Singapore market. As of mid-2019, there are now 11 telcos in Singapore,
including MVNOs. Unlike traditional telcos, MVNOs do not own and operate network
infrastructure and are required to lease capacity from Singtel, Starhub or M1.

MVNOs use technology to automate telco systems and cut operational costs and, as a
result, are able to offer more competitive pricings for consumers.

V MEDIA

i Restrictions on the provision of service

Broadcasters licensed by the IMDA are required to comply with various codes issued by the
IMDA under the Broadcasting Act, including the Free-to-air Television Programme Code,
Subscription Television Programme Code, Free-to-air Radio Programme Code (collectively,
Programme Codes), Television Advertising Code, Radio Advertising Code (collectively,
Advertising Codes) and Television Programme Sponsorship Code (Sponsorship Code).

in-new-entrant-spectrum-auction.
7642648.
The Programme Codes seek to impose guidelines that are congruent with national interests in upholding racial and religious harmony, observing societal and moral standards, and promoting positive family values. However, it is recognised in the Programme Codes that standards may vary according to the time of the telecast and the target audience (the watershed time for television is 10pm), as well as the accessibility or otherwise of the programme (e.g., premium channels for subscription television). The Programme Codes also require broadcasters to maintain high standards of language and speech in the four official languages of Singapore, and to refrain from using localised English or other dialects.

The Advertising Codes seek to ensure that the interests of viewers and listeners as consumers are protected. Therefore, the Advertising Codes prescribe that advertisements on television and radio must be truthful and lawful, and should not contain any claims that may be misleading. All claims and comparisons must be capable of substantiation, and should not in any way deceive or mislead. Advertisements should respect public tastes and interests, and uphold moral and social mores. In addition, the Advertising Codes stipulate that broadcasters should exercise discretion when scheduling advertisements and trailers to ensure that they are appropriate for the target audience.

The Sponsorship Code is concerned with aspects of television programme services that entail advertiser involvement in programming and promotional (rather than advertising) time. Besides exercising social responsibility, broadcasters are required to maintain editorial integrity and programming independence, and should not be influenced by the sponsor regarding either the content or acquisition of a programme.

In addition, the Broadcasting Act provides that the Minister of Communications and Information may, by an order published in the Gazette, declare any foreign broadcasting service rebroadcast in Singapore on any relevant licensable broadcasting service to be a foreign broadcasting service engaging in the domestic politics of Singapore. Currently, the nationwide subscription television services provided by StarHub Cable Vision Ltd and SingNet Pte Ltd have been designated as relevant licensable broadcasting services. Prior approval for the inclusion of such declared foreign broadcasting service would need to be sought from the Minister, who may make the approval conditional upon restrictions being imposed on the number of persons capable of receiving such declared foreign broadcasting service. The Minister may also impose conditions requiring that the rebroadcast be suspended for such period as the Minister may, from time to time, direct.

ISPs and ICPs licensed under the Notification are required to comply with the conditions of the class licence set out in the Schedule of the Notification. These conditions stipulate, inter alia, that the licensee shall:

a. ensure that its service is not used for, or in furtherance of, games and lotteries, the conduct of which is an offence under the Common Gaming Houses Act unless the licensee is exempted from the provisions of that Act;

b. avoid the broadcast of horse-racing analyses, commentaries or tips, other than horse-racing results, for the purpose of gambling;

c. ensure that its service is not used to advertise, provide or otherwise promote astrology, geomancy, palmistry or any other type of fortune-telling device;

d. ensure that its service is not used for soliciting or for any other immoral activity;

e. ensure that any professional advice or any specialist consultancy service offered on its service is offered by persons with qualifications recognised by the relevant professional bodies in Singapore;
in the case of the broadcast of sound recordings, ensure that only sound recordings that are acceptable to the censorship section of the MDA are broadcast; and

g in the case of the broadcast of films or video recordings, ensure that only films and video recordings that are approved by the Board of Film Censors are broadcast, unless the film or video recording is one to which the Films Act does not apply or is one that is exempted from the provisions of that Act.

Class licensees are also subject to the Internet Code, which seeks to set out other obligations and duties of licensees. Generally speaking, the Internet Code requires all licensees to ensure that no prohibited materials (i.e., material that is objectionable on the grounds of public interest, public morality, public order, public security or national harmony, or is otherwise prohibited by applicable Singapore laws) is broadcast via the internet to users in Singapore. In considering what material should be prohibited, the factors listed below are relevant:

- whether the material depicts nudity or genitalia in a manner calculated to titillate;
- whether the material promotes sexual violence or sexual activity involving coercion or non-consent of any kind;
- whether the material depicts a person or persons clearly engaged in explicit sexual activity;
- whether the material depicts a person who is, or appears to be, under 16 years of age engaged in sexual activity, in a sexually provocative manner or in any other offensive manner;
- whether the material advocates homosexuality or lesbianism, or depicts or promotes incest, paedophilia, bestiality and necrophilia;
- whether the material depicts detailed or relished acts of extreme violence or cruelty;
- whether the material glorifies, incites or endorses ethnic, racial or religious hatred, strife or intolerance; and
- whether the material has intrinsic medical, scientific, artistic or educational value.

The IMDA has the power to order the removal of objectionable content under the Notification, and if a licensee breaches such order, the IMDA has the discretion to cancel or suspend the class licence in respect of such licensee for such period as it thinks fit, or to require the payment of a fine of such amount as it thinks fit. However, the IMDA generally applies a light-touch approach towards regulating services on the internet, and a licensee found to be in breach of the foregoing regulations will generally be given a chance to rectify the same.

The IMDA implemented a new licensing regime for certain online news websites that have been subject to an individual licensing regime from 1 June 2013 to place them on more consistent regulatory footing with traditional news platforms. This new licensing requirement applies to websites that regularly report on issues relating to Singapore (on average at least one article per week on Singapore news and current affairs over a period of two months) and have significant reach (at least 50,000 unique IP addresses from Singapore per month over a period of two months). Since the implementation of the new licensing regime, the IMDA has assessed that 11 local news websites fall under the new licensing regime, including nine from the main newspaper publishers and broadcasters in Singapore (Singapore Press Holdings and MediaCorp), and one operated by Yahoo! News. The latest addition to the list is the current affairs site Mothership.sg.

Instead of being automatically class-licensed under the Notification (as is currently the case), the news websites subject to the new licensing regime will need to be individually
licensed, and have to put up a performance bond of S$50,000 with the IMDA. While it is expected that the prevailing content regulation requirements will not change, the new licence will also provide greater clarity on what the IMDA would consider prohibited content, and impose a requirement for licensees to comply with the IMDA’s direction to remove infringing content within 24 hours.

The new licensing framework invited a considerable amount of criticism from political and social activists, as well as ordinary members of the public. The IMDA is currently discussing details of the licensing regime with the three affected companies. It remains to be seen whether the IMDA would be forced to address such criticisms in the implementation of the regime.

ii Internet-delivered video content
Given the widespread availability of broadband access in Singapore, internet-delivered or OTT video content has gained much popularity as compared with broadcast video distribution. The increasing number of consumers accessing internet video content, along with other new media-rich content and applications, has led to an increased demand for bandwidth in Singapore.

There is a general consensus among network operators in Singapore that the demand for bandwidth, including over mobile broadband, will continue to grow steadily. Network operators are still grappling with business models that would allow them to monetise such transmission or otherwise allow them to recoup the investment sunk into infrastructure upgrading to meet such increased bandwidth demand.

iii Mobile services
The growing demand for mobile media services and media-rich services has fuelled the need for mobile broadband access in Singapore. An advanced communications infrastructure (Heterogenous Network) is recognised as a key pillar of one of the strategic thrusts set out in Infocomm Media 2025, building upon one of the key objectives of the iN2015, which was to increase the availability of wired and wireless broadband infrastructure in Singapore (see the Wireless@SG and Next Gen NBN initiatives discussed above).

Despite the higher costs per minute of mobile calls to fixed-line calls, mobile phone subscriptions have been increasing at a steady rate and have far surpassed the number of fixed-line subscriptions. The decrease in fixed-line penetration rates since July 2002 suggests that households may have replaced their fixed lines with their mobile phone lines.

The IMDA continues to recognise that certain spectrums may require review to address the growing need for spectrum for broadband services and next-generation mobile services.

VI THE YEAR IN REVIEW
i Singapore’s law on fake news regulates false online information
Singapore’s Protection from Online Falsehoods and Manipulation Bill, which passed in May 2019 and came into effect on 2 October 2019, is aimed at regulating false information that is spreading on the internet. Under the new law, a minister may decide whether to act
against a piece of fake news on the internet and has the authority to order such fake news to be taken down or corrected. Individuals and technology companies that do not comply with these orders may be subject to criminal sanctions.26

ii The MAS and the SAL launches a new programme to help payments industry comply with legal requirements

In September of 2019, the Monetary Authority of Singapore (MAS) and the Singapore Academy of Law (SAL) launched a new programme called the Payments Regulatory Evaluation Programme (PREP) to provide the payments industry with a list of lawyers specialising in payment services. The aim of PREP is to help payments companies meet their compliance needs. Under PREP, payment firms can be assured that regulatory assessment conducted by a legal provider on the list will be sufficiently comprehensive in scope and meets industry standards.27 Seven local and international legal service providers are participating in the two-month pilot programme. After the pilot programme, the MAS and SAL will take feedback from the participants and modify the regulatory programme if necessary.28

iii The MAS launches a new regulatory sandbox for faster testing of fintech products

On 7 August 2019, the MAS launched the Sandbox Express for firms carrying on certain activities to have a faster option to test new financial products and services on the market. Unlike the existing FinTech Regulatory Sandbox, eligible firms may begin market testing within 21 days of the day the MAS receives a complete application. At its initiation, the Sandbox Express is only available to insurance brokers, recognised markets operators and remittance businesses. Experiments in the Sandbox Express may be for up to nine months.29 The Sandbox Express is aimed to speed up innovation in the financial products and services industry, which aligns with the government’s initiative to promote fintech in Singapore and regionally. There are now over 600 fintech start-ups in Singapore and the sector is creating 1,000 fintech jobs every year.30

iv New masterplan on cybersecurity to protect critical sectors

Following the SingHealth data breach in July 2018 where the personal details of 1.5 million patients were stolen, the Singapore authorities and the public in general has heeded more attention to the importance of data protection. The operational technology (OT) Cybersecurity Masterplan, announced by Senior Minister Teo Chee Hean on 1 October 2019 at the fourth Singapore International Cyber Week, will promote development of capabilities to secure and mitigate cyber threats to OT systems. OT systems are defined as those operating critical infrastructure services using interconnected devices and computers, including those

in energy, transport, water and media. The OT Cybersecurity Masterplan, developed by the Cyber Security Agency of Singapore (CSA), will increase defence against cyber attacks in Singapore by fostering a local talent pool and facilitating information exchange between the government and private sectors. The CSA will further set up a new OT Cybersecurity Information Sharing and Analysis Centre.

Stricter rules on the collection of NRIC numbers
From 1 September 2019, under new Advisory Guidelines on the PDPA for NRIC and Other National Identification Numbers, it is illegal for organisations to collect, use or disclose NRIC numbers or make copies of the NRIC. Prior to this rule taking effect, there were many circumstances under which organisations were permitted to collect an individual’s NRIC number, including for allowing visitors to enter into the premise of a building, purchasing movie tickets or for lucky draws at the mall. Under the new rule, organisations are only allowed to collect, use and disclose NRIC numbers if the collection, use or disclosure is required by law or it is necessary to establish or verify an individual’s identity to a high degree of accuracy. Further, organisations must be able to provide justification on collection, use or disclosure of an NRIC number on request to individuals and to the PDPC. Organisations that have already collected and are holding NRIC numbers are encouraged to assess whether they need to keep these numbers and to dispose of them responsibly if there is no proper reason to retain them. In circumstances where the collection, use or disclosure of NRIC numbers is permitted, organisations must ensure that there are adequate protection measures in place to protect an individual’s personal data that are in compliance with the PDPA.

Alibaba’s artificial intelligence research centre in Singapore
On 28 February 2018, Chinese e-commerce giant Alibaba opened an artificial intelligence (AI) research institute in Singapore in collaboration with Nanyang Technological University (NTU), a local university. This will be Alibaba’s first joint research centre located outside mainland China. The institute will carry out research on AI technology for an initial five years with a pool of 50 researchers from both organisations, and aims to develop technologies to help in caring for the elderly, such as developing robot companions and sensors to detect problems. It has since managed to obtain an AI patent in Singapore in just three months, which is a world record.

PDPC contemplates mandating that organisations must report any breaches of personal data
As part of the revisions to the Personal Data Protection Act, tougher breach reporting rules have been proposed to be imposed on organisations. The proposed revisions to the PDPA will require individuals affected by a breach to be notified as soon as practicable, and the PDPC to be notified no later than 72 hours after an eligible breach is identified. The PDPC, in recognising that organisations may need time to determine the veracity of suspected breaches,

will give organisations up to 30 days to assess if breaches are eligible for reporting, and the 72-hours notification period will kick in after that. These changes follow the steps of mature jurisdictions such as the United States, Canada and Australia.³⁴

viii  New AI Governance Framework
The PDPC published a Model AI Governance Framework to frame the discussion around using AI responsibly. The Model Framework is not binding on organisations that adopt and deploy AI technology, but is rather a compliance and governance framework that organisations are encouraged to adopt. The Model Framework translates ethical principles into practical measures that organisations adopting and deploying AI solutions may implement. The guiding principles of the Model Framework are that (1) decisions made by AI should be explainable, transparent and fair; and (2) AI systems should be human-centric. The four key areas of governance proposed in the Model Framework are internal governance structures and measures, risk management in autonomous decision-making, operations management and customer relationship management.

ix  New Resource Sustainability Act targets management of electronic waste
The new Resource Sustainability Act, which is a part of Singapore’s larger strategy to manage electronic, food and packaging waste, passed its third reading in Parliament on 4 September 2019. The Resource Sustainability Act will require producers and retailers of electrical and electronic products to provide waste management solutions, including joining producer responsibility schemes and offering services for collection and disposal of electronic waste. Non-compliance with the Act may subject a violator to monetary fines of up to S$50,000 and up to three months’ imprisonment.³⁵

x  Singapore considering data portability requirement
Currently, Singapore’s data protection laws do not include a data portability rights for individuals. The PDPC issued a public consultation from 22 May to 3 July 2019 on proposed data portability obligation for organisations. The proposed data portability obligation will allow individuals to have more control over their personal data. Individuals will be able to request an organisation to provide to another organisation with information relating to the individual in a commonly used machine-readable format. The proposed data portability obligation only applies to data held in electronic form that is (1) provided by the individual to an organisation; or (2) generated by the individual’s activities in using the organisation’s product or service. Data that is not held in electronic form (e.g., paper forms) is not subject to the Data Portability Obligation. Derived data is also excluded. The PDPC continues to consider issues around data portability limits and the format, standards, security and protection of data to be transferred.

xi  IMDA introduces new niche television service licence
According to a new IMDA web page, service providers offering television services targeting niche market segments and OTT television services in or from Singapore will need to apply for a niche television service licence. Application can be done online, and according to the


© 2019 Law Business Research Ltd
IMDA web page, there is no licence fee. Content offered under this licence must comply with the Content Code for Over-the-Top, Video-on-Demand and Niche Services. While there is not much information available online on the requirements and procedures for this licence, this shows that the IMDA continues to be active in the OTT space.

VII CONCLUSIONS AND OUTLOOK

As can be seen from the foregoing, Singapore’s key strength lies in its foresight and strategic planning capabilities. Among other factors, the restructured IMDA is expected to strengthen and develop regulatory capabilities for a converged infocomm and media sector in a holistic manner, and further Singapore’s goal of establishing a value-creating economy that is well-positioned to leverage growing opportunities in the convergent telecommunications, media and technology sphere. As a small island nation, Singapore has also effectively leveraged on its size, and has successfully implemented and continued to improve a number of ambitious nationwide projects, such as Wireless@SG and the Next Gen NBN initiatives.

The ubiquity of ultra-high-speed broadband access, coupled with the drive to promote next-generation interactive multimedia applications and services delivered through the IPTV platform, heralds an exciting period of transition into a new generation of services for both businesses and consumers. This can be seen from the steadily increasing take-up rate of total fibre-optic broadband, which as at May 2018 stood at approximately 1.44 million subscribers.36

For Singapore to compete effectively at the global level, the government recognises that seamless, trusted and intelligent infocomm infrastructure will be crucial. The government has continued to encourage the development of new green data centre technologies, and has supported the establishment of a data centre park in Singapore so as to attract multinational corporations and other premium data centre operations to Singapore, and to strengthen its position as an economic hub. The government has also devoted increasing resources, effort and attention to its cybersecurity efforts with the continued development of resilient infrastructure, such as:

- the launch of the Defence Cyber Organisation and planned launch of the Government Security Operations Centre;
- the strengthening of the legislative tools it has to combat cyberthreats with the new cybersecurity bill;
- the development of a vibrant cybersecurity ecosystem through public–private partnerships such as the Alliance of Public–Private Cybercrime Stakeholders, and strong government support for Honeywell’s industrial cybersecurity centre and the National Cybersecurity R&D Laboratories;
- equipping Singapore citizens for digital access, literacy and participation as part of the Digital Readiness initiative.

Adopting a new mindset that it is not whether a significant cyber-threat will occur, but rather when, Singapore had also taken the controversial step to ring-fence or air-gap key government systems from the internet and unauthorised devices. This has proven particularly prescient given the significant increase of cyberattacks (both successful and thwarted) that Singapore

---

Singapore has faced over the past few years. This is only likely to worsen as Singapore’s increased reliance on ITC technologies as it achieves its goal of becoming a Smart Nation makes Singapore a more vulnerable and prominent target. Singapore continues to intensify its efforts to defend against and prepare to respond to cyberattacks, and by adopting a risk-based approach to cybersecurity and building in sufficient flexibility and redundancies, it has made itself significantly more prepared for any cyberattack and the new digital landscape than most nations. The Prime Minister’s Office has also set up a Smart Nation Programme Office that aims to bring citizens, the government and industry players together to identify issues, co-develop solutions, prototype ideas and deploy them effectively to transform Singapore into a Smart Nation. This initiative focuses on the development of infocomm-based integrated networks, capabilities and solutions for urban environments with a systems-of-systems approach that enables synergies within the whole government, and integrated insights that will contribute to the optimisation of key national resources across interdependent and inter-related city systems. The Smart Nation vision aims to harness ICT, networks and data to support better living and stronger communities, and to create more opportunities.

Further, Singapore has enacted an overarching data protection law in the form of the PDPA, which should help to strengthen and enhance Singapore’s position as a trusted data hub. We believe that the PDPA strikes the right balance in protecting the interests of consumers against the need for businesses to collect, use and disclose personal data. The PDPC continues to update and release new advisory guidelines to guide and inform organisations and individuals on data privacy, use, collection and disclosure. The PDPC also continues to look at further amending the PDPA to keep it updated and enable Singapore to continue exploiting growing opportunities in the world of big data, and allow businesses to harness value from information, arguably the most precious commodity in this era.

Finally, Singapore is forward looking, as seen from efforts to address and prepare for issues that may arise in the continued adoption of financial and AI technologies. The Sandbox Express allows certain financial institutions to fast-track the testing and adoption of their fintech products on the market. The AI Model Framework provides practical guidance to organisations employing AI technologies. Singapore recognises that these are key industries and is proactively learning about these industries to ensure that Singapore has in place laws and policies that strike a balance between being conducive to the growth of these industries and the protection of individual rights.
Chapter 17

SPAIN

Pablo González-Espejo and Nerea Sanjuan

I OVERVIEW

This chapter provides a general overview of the electronic communications, audiovisual and internet access regulations in Spain. Given the complexity and constant evolution of these sectors, this summary is not intended to be comprehensive, but simply to outline the main aspects of the regulations, as well as recent news and trends.

Electronic communications

Following the consolidation process of the electronic communications market in Spain through mergers and acquisitions, which resulted in the convergence of fixed and mobile operators (e.g., Orange and Jazztel, Vodafone and ONO, Yoigo, Pepephone and Másmóvil), and broadband and pay-TV operators (e.g., Telefónica and DTS), the Spanish market has continued a process of deep transformation due to the convergence of technologies, devices and platforms. On top of that, OTT services have significantly increased their market share, as evidenced by:

a a new European regulation on the protection of natural persons with regard to the processing of personal data that applies, inter alia, to OTT and IoT services addressed to end users in the European Union (EU); and

b a new Directive to amend the Audiovisual Media Services Directive which, among other things, establishes specific rules that, inter alia, are intended to create a level playing field with the traditional linear and non-linear audiovisual services, as alternative audiovisual platforms are growing fast, replacing traditional means of accessing content (e.g., Netflix, HBO, Amazon, Sky, Huawei and Apple’s audiovisual platforms have entered the Spanish market since 2015).

As regards the regulatory framework, although the General Telecommunications Law, which has been the main piece of legislation governing the telecoms sector since 2014, provided for the development of its own ancillary regulations, most of the former Law’s ancillary regulations are still in force. As an exception, in February 2017 the government passed Royal Decree 123/2017, of 24 February, on the regulation of the use of the radio spectrum, which

---

1 Pablo González-Espejo is a partner and Nerea Sanjuan is a senior attorney at Uría Menéndez.
3 Law 9/2014.
sets out the general regime for the use of spectrum and repealed the 2008 Royal Decree in this regard. Additionally, Royal Decree 381/2015 on measures against unauthorised traffic and irregular traffic for fraudulent purposes, and Royal Decree 330/2016, which implements Directive 2014/61/EU on measures to reduce the cost of deploying high-speed ECNs,4 were issued in 2016.

Additionally, the approval of Directive (EU) 2018/1972 of the European Parliament and of the Council, of 11 December 2018, establishing the European Electronic Communications Code, which repeals most of the EU prior regulation on this matter (EECC) will surely cause a revision of the Spanish electronic communications regulations as a whole.5

In compliance with its periodic duty to analyse the electronic communications markets, the National Markets and Competition Commission (NMCC) has followed the deregulation tendency of other European countries and begun its fourth review and analysis of the electronic communications markets. In particular, in January 2017 the NMCC issued a resolution on Markets 1/2007 and 2/2007 (Markets 1 and 2), lifting Telefónica’s obligations as a holder of significant market power on the retail market for access to fixed telephony as the requirements to be a relevant market subject to ex ante regulation are no longer being met. However, regarding the wholesale market for call origination in the fixed network, the NMCC still considers that the wholesale market is not really competitive and imposes certain obligations on Telefónica (including providing separate accounts, non-discrimination and transparency measures, etc.). In addition, in April 2017 the NMCC issued a resolution to deregulate access to mobile network markets (Market 15), lifting the obligation on the main three network operators (Telefónica, Vodafone and Orange) to provide virtual mobile operators (OMVs) with reasonable access to their mobile infrastructure on the basis that, according to the NMCC, this market is already competitive. In addition, throughout 2017, the NMCC reviewed Telefónica’s main reference offers and prices as an operator designated as having significant market power, including disaggregated virtual access to the fibre optic loop, the new broadband ethernet service, the wholesale offer for access to manholes and conduits, and the reference offer for leased lines.

In the context of its duties as referred to above, the NMCC has also issued several recent resolutions regarding the regulation of the telecommunications market:

- Resolution ANME/DTSA/002/17/M2-2014 approving the definition and analysis of the market of termination of vocal calls in individual mobile networks (Market 2/2014);
- Resolution ANME/DTSA/001/17 approving the definition and analysis of the wholesale leased trunk line market;
- Resolution ANME/DTSA/002/18 listing the operators who shall be considered as principal in the fixed and mobile telephone services in the national market;
- Resolution ANME/DTSA/001/18/M18-2003, approving the definition and analysis of the wholesale market for the television broadcasting transmission service; and
- Resolution ANME/DTSA/003/18/M1-2014 approving the definition and analysis of the wholesale market of termination of calls in individual public telephone networks available at a fixed location.

---

4 This Royal Decree has been further developed by Order ECE/529/2019, of 26 April, setting up the Unique Point of Information therein established for the purpose of reducing the cost of deploying high-speed ECNs.

5 Transposition of the EECC to national regimes is due by 21 December 2020.
Since the publication of the Spanish Digital Agenda in February 2013, the Ministry of Economy and Enterprise (MINEE) has published several reports that keep the original agenda up to date and address final users of telecommunication services. In August 2017, the MINEE opened a public consultation to obtain feedback on the drafting of a Digital Strategy for an Intelligent Spain, the preliminary results of which were released in November 2017.

In compliance with the European mandate regarding the liberalisation of the 800MHz band (the first digital dividend), in March 2015 the MINEE announced the conclusion of the liberalisation process in favour of telecom operators for the provision of LTE and 4G services. Additionally, in May 2017, Decision (EU) 2019/899 on the use of the 470–790MHz band in the EU was enacted, seeking to promote the development of a 5G network and the improvement of mobile connections (the second digital dividend).

Following this decision, on 29 June 2018, the Spanish government published its national roadmap for the liberalisation of the second digital dividend and, on 21 June 2019, it passed Royal Decree 391/2019 approving the new National Technical Plan for DTT and the regulation of certain aspects of the liberalisation of the second digital dividend (Royal Decree 391/2019). Among others, this Royal Decree regulates how the 700MHz band will be liberalised and how the radio-electric channels and the new digital MUXs will be distributed among the Spanish Public Radio and Television Corporation and other licence holders.

ii Audiovisual

In September 2014, a new technical plan for DTTV was passed regulating the new allocation of spectrum to DTTV services and certain aspects of the release of frequencies of the digital dividend to telecom operators. As a result of a public tender called during the first half of 2015, the government allocated six new DTTV channel licences (three SD and three HD) in October 2015 that were launched in April 2016. Those licences were challenged in court, but they were finally confirmed by the Spanish Supreme Court in a decision issued in January 2018.

In November 2015, the NMCC also passed a proposal that recommends introducing certain flexibility to the spectrum cap of high bandwidths if certain conditions are met.

Finally, the imminent implementation of the New Audiovisual Media Services Directive will require the amendment of the current national regulation on audiovisual media services dated 2010.6

iii Internet

Following a ruling of the Grand Chamber of the European Court of Justice (CJEU) dated 12 May 2014 on case C131/12, which involved Google and the Spanish Data Protection Agency (AEPD),7 consultations and proceedings on the right to be forgotten have spread, and the AEPD has published a subsection on this right on its website. Furthermore, as a consequence of such ruling, the right to be forgotten has been included in the recently adopted EU Regulation on the protection of natural persons with regards to the processing of personal data.

6 The deadline for implementation is 19 September 2020.

7 Google Spain, SL and Google Inc v. the Spanish Data Protection Agency and Mario Costeja González.
of personal data\(^8\) (GDPR). Further legal development of the right to be forgotten has been approved for Spain in the recent Spanish Basic Law 2/2018 on Protection of Personal Data and Guarantee of Digital Rights (the Data Protection Law).

Since its creation in December 2013, the Spanish National Institute of Cybersecurity (INCIBE) has been quite active in building digital confidence in the Spanish market, particularly and in cooperation with the AEPD, with regards to the protection of privacy and cybersecurity.

Additionally, Spain has recently transposed the NIS Directive\(^9\) into the Spanish legal system through Royal Decree-Law 12/2018, of 7 September.

II REGULATION

i The main sources of regulation

The main sources of regulation applicable to the TMT sector in Spain are:

\(a\) the General Telecommunications Law;
\(b\) the General Audiovisual Law;
\(c\) the e-Commerce Law;
\(d\) the GDPR and the Data Protection Law;
\(e\) the Data Retention Law;
\(f\) the National Markets and Competition Commission Law; and
\(g\) Royal Decree-Law 12/2018, of 7 September, transposing the NIS Directive.

There have also been several administrative orders, instructions, recommendations and guidelines issued by the government, the relevant ministries and the NRAs that develop these laws.

ii The NRAs

The NMCC is an independent public body in charge of supervising market competition in Spain, as well as certain relevant markets including the electronic communications and audiovisual markets. Its main functions as regards the electronic communications market are to establish and supervise the fulfilment by operators of their obligations, to promote fair competition and the plurality of the offer of ECSs, and the resolution of disputes between operators. The NMCC has, inter alia, the power to define the relevant electronic communications markets, to advise on the regulation of the electronic communications market, and to exercise certain supervisory and sanctioning powers. Among its functions regarding audiovisual matters, the NMCC is in charge of monitoring compliance by TV service providers with the quota and financing obligations set out in the General Audiovisual Law as well as with advertising restrictions.

The State Secretariat for Digital Progress (SEAD), which is part of the MINEE, holds certain powers regarding electronic communication, audiovisual and other TMT matters, and is responsible, inter alia, for:

---

proposing general policies and regulations on the electronic communications and information society;

b the promotion and development of TMT infrastructure and services;

c the management of domain names under the Spanish country code (.es);

d the management and control of TMT scarce resources (such as spectrum), including the processing and granting of licences for private spectrum use; and

e keeping the Spanish National Registry of Audiovisual Operators.

As regards certain matters included in the TMT laws that relate specifically to personal data protection, such as the use of cookies and the submission of commercial electronic communications, some control and sanctioning powers have been granted to the AEPD, which is the independent authority responsible for the enforcement of data protection regulations. The AEPD has the power to hear claims concerning personal data protection and to exercise sanctioning powers for infringements under the data protection, e-commerce and electronic communications regulations. In addition, some autonomous regions (Catalonia and the Basque Country) have set up regional authorities whose functions are limited to the processing of personal data by regional public entities.

iii Regulated activities

Electronic communications

According to the General Telecommunications Law, telecommunications are services of general interest to be provided under conditions of free competition regardless of the imposition of certain public service obligations on operators. Under the General Telecommunications Law, no licence is required for the provision of ECSs and the operation of networks, but formal notice must be provided to the MINEE before these activities can begin. The prior notice must include corporate and identification data and documentation, a declaration of compliance with the applicable laws, a description of the services that are to be provided or of the networks that are to be exploited, and an approximate date of when the activity is expected to start. The MINEE has 15 days to reject a notification if it does not comply with the requirements established in the General Telecommunications Law and its ancillary regulations. If the requirements are met, the MINEE will automatically register the notifying party with the General Operators Registry. Every three years, operators must notify the MINEE of their intention to continue or discontinue providing electronic communication services.

An administrative authorisation or concession is required to make private use of the radio electric spectrum in Spain. The procedure to obtain an authorisation or concession for spectrum use is set out in Royal Decree 123/2017,10 which distinguishes between general authorisations, individual authorisations and public concessions. According to Royal Decree 123/2017, operators must submit a spectrum use application together with a technical proposal to the MINEE (through the SEAD), in response to which the SEAD must issue a resolution granting or rejecting the application. As a general rule, as a prerequisite for obtaining a spectrum concession, applicants must prove their status as registered electronic communications operators; however, the SEAD may limit the concessions in certain frequency bands in order to guarantee the efficient use of spectrum or when demand for the spectrum exceeds the offer. In those cases, the relevant concessions will be awarded through public tender processes.

10 As modified by Royal Decree 391/2019.
In addition, operators interested in obtaining numbering use rights must submit an application to the MINEE, which will decide whether to grant or refuse these rights according to the National Numbering Plan and other regulations within three or six weeks (in the case of competitive selection procedures) following the submission of the application.

**Audiovisual communications**

The provision of audiovisual communication services is only subject to a prior notification to the relevant administrative body, be it national or regional, depending on the coverage of the service. Exceptionally, DTTV services and any other audiovisual services (including radio) that require the use of terrestrial radio waves must obtain a licence through a public tender process called by the government (for nationwide broadcasting) or by the regional governments (for regional and local broadcasting). Licences are granted for 15-year terms and are subject to subsequent 15-year term renewals if the audiovisual service provider meets all the required conditions.

If the provision of audiovisual services requires spectrum use, such use is subject to the prior reservation of the corresponding spectrum pursuant to a public resolution by the SEAD.

**iv Ownership and market access restrictions**

**Electronic communications**

Under the General Telecommunications Law, there are no limitations – even for foreign entities – on ownership. The only limitation is imposed not on ownership but on the provision of direct ECSs by foreign (non-EU) entities in Spain, with such provision requiring a reciprocal treaty.

Royal Decree-Law 6/2000, of 23 June, on urgent measures to improve competition in the goods and services markets, provides for certain restrictions on the ownership of certain types of telecommunications service providers. Individuals and legal entities holding, directly and indirectly, 3 per cent or more of the total share capital or voting rights of two or more principal operators in, inter alia, the fixed-line and mobile telephony markets cannot exercise their voting rights in excess of 3 per cent of the total in more than one operator without the prior authorisation of the NMCC. Furthermore, no individual or legal entity may appoint, directly or indirectly, members of the management body of more than one principal operator in, inter alia, the fixed-line or mobile telephony markets without the prior authorisation of the NMCC. Additionally, individuals or legal entities considered principal operators may not exercise more than 3 per cent of the voting rights of another principal operator or appoint, directly or indirectly, members of the management body of any principal operator without the prior authorisation of the NMCC.

Finally, Royal-Decree 458/2011, as amended by Ministerial Orders ITC/2499/2011 and IET/173/2014, establishes certain thresholds on the holding of frequencies by each operator (spectrum cap), and some temporary restrictions on the transfer or assignment of spectrum in certain frequency bands.

According to Royal Decree 123/2017, certain restrictions exist preventing anticompetitive hoarding from restricting the total amount of frequencies to be used by the same operator or group of operators, or providing time limits on the utilisation of the rights of use.
Audiovisual communications

According to the General Audiovisual Law, the following requirements must be met to be granted a TV or radio licence that uses the spectrum as a means of transmission.

Natural persons and legal persons must be citizens of a country within the European Economic Area (EEA) or a country that allows Spanish citizens to hold equivalent licences, and they must have a legal representative domiciled in Spain. For legal persons, any foreign (non-EEA) stake in their capital must also comply with the reciprocity principle, and the individual stake of any non-EEA natural or legal person cannot directly or indirectly exceed 25 per cent of the share capital, while the total non-EEA stake must be below 50 per cent of the share capital.

In addition, there are some constraints on aggregate holdings in TV and radio service providers that are intended to guarantee pluralism in those markets. In relation to TV service providers, individuals and legal entities are forbidden from holding a significant stake\textsuperscript{11} in more than one operator providing national television audiovisual communication services if the average number of viewers of the television channels broadcast by the audiovisual communication service providers in question exceeds 27 per cent of the total viewers in the past 12 consecutive months. Individuals and legal entities are not allowed to acquire a significant stake or voting rights in more than one provider of television audiovisual communication services when national providers, in aggregate, hold rights to use the spectrum exceeding the technical capacity corresponding to two multiplex channels; and regional providers, in aggregate, hold rights to use the spectrum exceeding the technical capacity corresponding to one multiplex channel.

Moreover, individuals or legal entities holding a stake in a national provider of television audiovisual communication services cannot acquire a significant stake or voting rights in another provider of the same service if the acquisition prevents the existence of at least three different private providers of national television audiovisual communication services so as to ensure pluralism in the media.

With regard to radio licences, no individual or legal entity may control, directly or indirectly, more than 50 per cent of the private licences for the terrestrial radio services within the same coverage area. Furthermore, no individual or legal entity may control, directly or indirectly, more than five of these licences within the same coverage area. In addition, no person is allowed to control more than 40 per cent of the total licences in an autonomous community where there is only one licence per licence area. Nor is any person allowed to control more than one-third of the licences with total or partial nationwide coverage.

Transfers of control and assignments

Electronic communications

There is no express regulation on the transfer of control of an operator or of its telecoms business to a third party. When a telecoms business is assigned to a third party, the latter must ensure that it has previously notified the MINEE of its intention to provide the services in question or operate the relevant network.

\textsuperscript{11} That is, a direct or indirect holding of 5 per cent of the share capital or 30 per cent of the voting rights, or a lower percentage if such percentage is to be used to appoint, within 24 months following the acquisition, a number of members to the board of directors representing more than half of the total.
The transfer of authorisations or concessions or the assignment of rights to use the spectrum are regulated under Royal Decree 123/2017, and require the prior authorisation of the MINEE or the SEAD. In particular, no transfer or assignment of the spectrum can take place if it is proven that it will restrict market competition or if restrictions to prevent anticompetitive hoarding would be exceeded. The authorisation procedure differs somewhat for transfers and assignments of certain spectrum use rights (particularly, rights on the special use of public spectrum granted by general and individual authorisations or those granted as public concessions cannot be transferred). There are also different formalities that apply depending on whether the relevant title over the private use right is transferred or the right assigned.

Regarding numbering use rights, the holders of these rights may assign them (including the management or marketing of the numbers) to other telecommunications operators with the prior authorisation of the MINEE and provided that the application specifies the intended use of the numbering rights being assigned.

Audiovisual

The General Audiovisual Law repealed the notification procedure for transfers of interests in companies holding a TV licence that use the spectrum as a means of transmission. In addition, for the first time it allows and regulates legal transactions involving audiovisual communication licences. Under this regulation, these transactions require the prior authorisation of the relevant public authority (once the applicant has provided evidence of compliance with all applicable legal conditions) and the payment of a fee.

Finally, it should be noted that mergers within the TMT sector may be subject to the authorisation of the NMCC or the European Commission if the thresholds set out in the competition regulations are exceeded.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

IP-based services are not subject to a separate regulatory structure, but are regulated under the traditional electronic communications regulation, the General Telecommunications Law and its ancillary regulations.

Internet services that do not qualify as ECSs or the operation of telecom networks, such as the provision of mere content services, are excluded from the scope of the General Telecommunications Law and its ancillary regulations, and are regulated by the e-Commerce Law.

ii Universal service

The General Telecommunications Law establishes that electronic communications operators may be requested to provide certain universal services that cover a range of ECSs that must be provided to all users at a reasonable price and be of a certain quality, regardless of their geographical location.

According to the General Telecommunications Law, the availability of functional access to the internet, allowing bandwidth communications at a downlink speed of at least 1Mb/s, is part of the universal service. The Law has empowered the government to review this speed taking into account the market conditions as well as the social, economic and technological developments.
To reinforce the development and use in Spain of internet and broadband services, the government and the old Telecommunication Market Commission (CMT) issued certain decisions with the aim of encouraging the provision of broadband services (e.g., restructuring the wholesale price offering) and the deployment of NGA networks by alternative operators, improving the technical conditions for the deployment of networks by using the main operator’s infrastructure. Among these decisions, a new plan developing the Spanish Digital Agenda was approved by the government in February 2013, and a plan with specific measures for the development of ultra-fast networks was published in June 2013. By the same token, the Digital Agenda 2016 Annual Report insists on the significance of the promotion of high-speed networks, focused in high-speed networks (30Mb/s), ultra-fast networks (100Mb/s) and 4G, and remarks that the objectives set for 2015 by the Digital Agenda as regards the ultra-fast networks were achieved.

Additionally, in August 2017 the MINEE opened a public consultation to obtain feedback on the drafting of a Digital Strategy for an Intelligent Spain based on the results obtained from the implementation of the Digital Agenda, which preliminary results were published in November 2017. According to those results, a majority of the population (52 per cent) considered that the strategy planned by the government was accurate because it covered the areas that most concern the citizens. Finally, in the context of the above-mentioned Digital Agenda, the MINEE recently published Order ECE/1016/2018, of 28 September, establishing the rules for the granting of subsidies to pilots on 5G technology.12

iii  Restrictions on the provision of service

Regarding restrictions on pricing, the only regulated retail price that was in place in 2012 (i.e., the maintenance fee for telephone line rental) was liberalised as a result of the review of the market for access to the public telephone network at a fixed location carried out by the CMT in December 2012. After 2016, Telefónica ended the freezing and such retail price was fully liberalised. The NMCC has also imposed restrictions on wholesaler prices charged by Telefónica to the alternative operators for the use of its infrastructure and networks.

For operators with significant market power, the NMCC may impose additional obligations to ensure transparency regarding interconnection and access, non-discrimination (i.e., the operator applies equivalent conditions to operators providing equivalent services) and wholesale price control. In this regard, Telefónica has issued, inter alia, price and service level offers validated by the NMCC and available to other operators, including:

- a reference interconnection offer (time-division multiplexing over IP);
- a reference offer for leased lines;
- disaggregated virtual access to the fibre optic loop;
- the new broadband ethernet service; and
- the wholesale offer for access to manholes and conduits.

In addition, all operators must respect end users’ rights, which are established in the General Telecommunications Law, and developed by Royal Decree 899/2009 and the Improvement of the Telecommunication Users Support Plan published in May 2015 by the NMCC, which aims to improve the current regulations on these matters and the quality-oriented culture when providing electronic communication services and to develop the inspection

12 This initiative is framed in the Spanish 5G National Plan launched by the SEAD for the period running from 2018 to 2020.
plans for 2015 to 2016 (the plans for 2017 and 2018 were successively published by the MINEE following the requirements set forth in the General Telecommunications Law and its implementing regulations). Ministerial Order IET/1090/2014 regarding the quality of services of electronic service providers was also issued in June 2014.

The limits on unsolicited calls, emails and texts are scattered mainly among the General Telecommunications Law and its ancillary regulation (Royal Decree 424/2005), the e-Commerce Law, the GDPR and the Data Protection Law (regarding individuals), and the Consumers and Users Defence Law.

As a general rule, direct marketing activities require the subject’s prior and informed consent. This consent must be explicit if the direct marketing is sent by e-communication means, fax or email, or through automated calling systems.

Regarding unsolicited calls for commercial purposes, when not carried out through fax, email or through automated calling systems, these may be carried out provided that recipients have not objected to them (e.g., upon the collection of the data, when the recipients have avoided appearing in telephone directories or are not registered in anti-marketing lists) and that they are offered a simple and free-of-charge objection procedure.

iv Security

Spanish legislation recognises general principles such as homeland security, law enforcement, network security, and freedom of access to information and self-expression either as inspiring principles or in specific rules. They are also measured and applied by the rulings of Spanish courts.

In particular, operators that provide public ECSs or networks must guarantee the secrecy of communications, which is a fundamental right under the Spanish Constitution. The protection of personal data and privacy is mainly regulated by the GDPR and the Data Protection Law, although all the other TMT rules referred to in this chapter also contain specific provisions to ensure the applicability of data protection in the relevant sectors. The Data Protection Law was passed in December 2018 and contains not only rules on data protection that are compatible with the GDPR but has also approved a new set of digital rights for citizens in Spain. Some of these new digital rights have a significant impact on the TMT sector, such as those limiting the use of monitoring technologies, such as geolocation or CCTV, within the workplace, or those imposing additional duties on TMT companies regarding the new right to a digital will, rectification rights on digital contents or those reinforcing the scope of the right to be forgotten.

Electronic communications operators also have the obligation to retain certain electronic communications data (traffic and locational data, and data that enables the identification of users) pursuant to the Data Retention Law.

With regard to cybersecurity, the NIS Directive has been implemented in Spain by Royal Decree-Law 12/2018, of 7 September, and it includes the appointment of competent authorities (most likely, the already developed INCIBE, which is the Spanish public entity in charge of cybersecurity) and computer security incident response teams. Further legal development of this law, by means of a regulation, is expected in the following months. Cybersecurity concerns in Spain were readdressed by a reform of the Spanish Criminal Code in March 2015 (effectively in force since July 2015) and a reform of the Criminal Procedure

13 Modified by Royal Decree 1517/2018, of 28 December.
Code in October 2015. Among other developments, these amendments provide for the possibility of police officers disguising themselves on the internet to obtain evidence of remote registrations of computer hardware and for the regulation of technological investigation measures in criminal proceedings.

Finally, INCIBE has been quite active in building digital confidence by, among other activities, publishing various guidelines and reports since June 2015 (the most recent guidelines were published in May 2018) regarding, inter alia:

a the secure storage of information, digital identities and online reputation;

b how to manage an information leak;

c cybersecurity in e-commerce;

d secure deletion of data; and

e how to manage risks related to security measures.

IV SPECTRUM POLICY

i Development

The radio spectrum is a public domain commodity that is owned, managed and controlled by the state (through the MINEE). The general rules and principles on the regulation of the spectrum are set out in the General Telecommunications Law.

Royal Decree 123/2017, inter alia, is intended to make spectrum use and its assignment more flexible, as well as to promote services and technological neutrality. Particularly, it clarifies the different types of use of spectrum (i.e., common, special and private) and titles granting the use of spectrum depending on said types. This Royal Decree is aimed at adapting regulations regarding the use of the radio spectrum to the General Telecommunications Law. Royal Decree 123/2017 also foresees the possibility of sharing the right of use over the radio spectrum among various titleholders in the same geographical area and seeks to simplify certain administrative procedures that, along with the mutualisation of exclusive rights of use, aim to make use of the spectrum more efficient and flexible.

Another key piece of legislation is the National Chart of Frequency Attribution (last updated in 2018), which allocates frequency bands to the different categories of services in accordance with technical characteristics.

Additionally, as further described below, Royal Decree 391/2019 regulates a subsequent liberalisation of spectrum and how the radio-electric channels and the new digital MUXs will be distributed.

ii Flexible spectrum use

Several measures have been implemented in Spain to make the use of the spectrum more flexible and to accommodate such use to the current and new uses of technology. Following the European Commission’s recommendations, the government announced in 2009 its intention to reserve the 800MHz band (the first digital dividend), previously reserved for TV services broadcasted through the former analogue system, for ECSs (particularly for mobile broadband services). This release became possible as a consequence of the digital switchover, which was completed in April 2010 and was intended to enable a more efficient use of the spectrum according to the current spectrum uses. As set out on Section I.i, in March 2015 the MINEE announced the conclusion of this liberalisation process.
Along the same lines, Royal Decree 458/2011 of 1 April on actions related to the spectrum for the development of the digital society imposes certain measures as regards the 900MHz and 1,800MHz bands, such as the technology neutrality principle. Royal Decree 805/2014 approved a new technical plan for digital television, reallocating bandwidth for DTTV services and electronic communication services in accordance with EU recommendations. In November 2015, the NMCC approved a proposal that recommends introducing certain flexibility to the spectrum cap currently applicable in high bandwidths if certain conditions are met.

Also, as set out in Section III.ii, a new plan developing the Spanish Digital Agenda was approved by the government in February 2013, whose specific plans were updated in June 2014. This plan highlights the need to optimise spectrum use in Spain. To achieve this goal, the plan proposes certain measures:

- to increase the flexibility in its use, such as access to ultra-fast mobile broadband;
- to facilitate and simplify the regulation of the management and use of the spectrum by encouraging, for instance, the secondary market;
- to review the current use of spectrum to identify those frequency bands that are underused; or
- to evaluate the spectrum needs for an effective development of the NGA networks.

As mentioned in Section I.i above, in May 2017, Decision (EU) 2019/899 on the use of the 470–790MHz band in the EU was enacted seeking to promote the development of a 5G network and the improvement of mobile connections (the second digital dividend). Following this decision, Royal Decree 391/2019 further regulates a subsequent liberalisation of spectrum and how the radio-electric channels and the new digital MUXs will be distributed among the Spanish Public Radio and Television Corporation and other licence holders, obligations of minimum range of reception and the technical specifications that the television services have to meet. The current number of MUXs (and their coverages) on the sub-700MHz band will be maintained, as well as the offer of DTT channels. This Royal Decree also states that the DTT service will be offered in the sub-700MHz band and that the 700MHz band shall not be used by audiovisual communication service providers after 30 June 2020, in order to make it available for the 5G mobile services from that date onwards. The Royal Decree further establishes that the sub-700MHz band will continue to be used for television broadcasting until, at least, 2030. On the same date, the Spanish government approved Royal Decree 392/2019, which regulates the direct granting of subsidies to compensate the costs in the reception of or access to television audiovisual communication services in buildings, as a consequence of the liberalisation of frequency bands in the 694–790MHz range (the second digital dividend).

Royal Decree 579/2019, dated 11 October 2019, further establishes subsidies for public audiovisual communication service providers to compensate costs for the simultaneous and transitory distribution of their television channels during the liberalisation of frequencies in the 694–790MHz range.

### iii Broadband and next-generation mobile spectrum use

The growing need for spectrum for broadband services and next-generation mobile services is being addressed within the new spectrum reorganisation and assignation process explained above.
iv Spectrum auctions and fees
As explained above, whenever the efficient use of spectrum needs to be guaranteed and demand for the spectrum exceeds the offer, spectrum use licences are granted through public tenders.

In addition to other fees applicable to electronic communications operators, the reservation of spectrum use for private purposes is subject to the payment of an annual fee, as set out in Annex I of the General Telecommunications Law. The amount of this reservation fee is calculated according to the number of spectrum reservation units multiplied by the value assigned to each unit, following certain parameters set out annually in the relevant law.

The amount of the fee will mainly depend on the type of service to be provided, the category of band reserved, the equipment and technology used, the level of use and congestion of the bands, the geographical areas, the market value of the reserved frequency and the revenue that the beneficiary may obtain.

V MEDIA
i Restrictions on the provision of service
As a general rule, audiovisual service providers enjoy programming freedom; however, the General Audiovisual Law establishes certain service obligations and restrictions to protect other general interests such as those of consumers, children’s rights, cultural and linguistic diversity, and political pluralism in the news.

This regulation will be modified as per the implementation in Spain of the New Audiovisual Media Services Directive, as it addresses some of these issues.

The main restrictions and obligations at present imposed on TV service providers are as follows.

Quota obligations
At least 51 per cent of annual broadcasting time (excluding, inter alia, news, sports events and advertisements) of each channel or set of channels must be reserved for European works. Moreover, 50 per cent of that quota must be reserved for European works in any of the official Spanish languages. Regarding annual broadcasting time, 10 per cent must be reserved for independent producers of European works, and half of this 10 per cent must have been produced in the past five years. With respect to non-linear audiovisual services over which a service provider has editorial responsibility, 30 per cent of the catalogue of programmes must be reserved for European audiovisual productions, and half of that 30 per cent for European audiovisual productions must be in any of the official Spanish languages.

Financing obligations
TV service providers whose programming includes full-length feature films, television films and series, documentaries, animated series or short films produced less than seven years ago must contribute, on a yearly basis, 5 per cent of the total income from the previous fiscal year (6 per cent for public broadcasters), according to their accounts, to the pre-financing of the production of certain audiovisual works such as full-length feature films, television films and series, documentaries, animated series and short films. Judgments of the Spanish Constitutional Court in case STC 035/2016 dated 3 March 2016, and of the Supreme Court in case STS 1665/2016 dated 7 July 2016 have confirmed the legality of this obligation on the grounds that it does not violate the principle of freedom of individual enterprise.
The General Audiovisual Law has been developed by Royal Decree 988/2015 and Royal Decree 241/2019 of 5 April, which regulate the legal regime applicable to this financing obligation for European audiovisual works.

This regulation will be subject to review as per the implementation in Spain of the New Audiovisual Media Services Directive, as it addresses some of these issues.

**Payment obligation**

According to the RTVE Financing Law\(^\text{14}\) and Royal Decree 1004/2010, since September 2009 private audiovisual communication services operators must pay 1.5 per cent (for pay-TV) and 3 per cent (for free-to-air TV) of their television and other audiovisual communication services revenue on a yearly basis for the financing of the public broadcaster RTVE, since advertising has been banned from RTVE’s broadcasting. This obligation was challenged by one of the Spanish audiovisual operators (DTS Distribuidora de Televisión Digital, SA) before the CJEU. By a decision dated 10 November 2016, the CJEU confirmed that the European Commission’s authorisation of such financing obligation is compliant with EU legislation (case C-449/14 P).

**Advertising restrictions**

While there are no specific advertising restrictions on radio services (other than those set out in the General Advertising Law),\(^\text{15}\) TV service providers must fulfil certain advertising-related obligations, which for linear services include the obligation to broadcast a maximum of 12 minutes of commercials per hour. The General Audiovisual Law has been developed by Royal Decree 1624/2011 on certain aspects of television commercial communication (self-promotion, telepromotion and sponsorship).

This regulation will likely be modified as per the implementation in Spain of the New Audiovisual Media Services Directive, as it addresses some of these issues.

**Other content-related restrictions and obligations**

There are also specific content-related restrictions, including those intended for the protection of children, that are of the utmost importance. First, audiovisual services providers must not use children’s voices and images without their consent or that of their parents or legal guardians. Secondly, the broadcasting of content that may seriously impair the development of minors (e.g., pornography or gratuitous acts of violence) is forbidden, and other content that may also be harmful for minors (such as gambling) may only be broadcast within certain time slots. The law also establishes reinforced protection for certain time slots that are considered to be accessible by children. Furthermore, to facilitate parental control, all audiovisual service providers must use digital encryption to classify their content, and TV service providers must use an age rating system according to the guidelines issued by the relevant authorities. In July 2015, the NMCC published the Guiding Criteria for the Classification of Audiovisual Content, which indicate content that is harmful, and on the other hand beneficial, to minors. Under the Criteria, and depending on the content of a programme, a grade is given that ranges from ‘for all audiences’ to ‘not suitable for minors under 18 years old’.


\(^\text{15}\) Law 34/1988 of 11 November on advertising.

© 2019 Law Business Research Ltd
With regards to sports content, additionally to the provisions of the General Audiovisual Law with regards to exclusivity agreements for the broadcasting of relevant sport events, Royal Decree-Law 5/2015 sets out the rules for the commercialisation of certain Spanish football content, and establishes the criteria to distribute the relevant income among organisers and participants in various competitions.

The NMCC also supervises the enforcement of these content restrictions in the audiovisual communication market. In fulfilling this duty, it has been exercising its sanctioning powers very intensively since 2016 and up to the present date against TV services providers for breaching the Advertising Law and the Guiding Criteria for the Classification of Audiovisual Content.

**Disabled persons**

There are further obligations (i.e., subtitling, audio-description and deaf sign language quotas) aimed at guaranteeing disabled people access to TV services, which will also be reviewed as per the implementation of the New Audiovisual Media Services Directive.

**ii Non-linear services**

Stand-alone non-linear services (e.g., VOD streaming services) in 2018 are fully consolidated among Spanish users and the market as a whole. In some cases, these services operate independently, while in others they operate through market arrangements with telecom companies.

The consolidation of web-based streaming services has opened a debate regarding the law applicable to providers that operate in Spain under the EU freedom to provide services rules, as for some issues the General Audiovisual Law will apply, while others may be subject to the e-Commerce Law. Thus far, the NMCC has not issued any specific instructions in this regard. The European Commission took the lead on this issue by launching the Proposal for a Directive that led to the passing of the New Audiovisual Media Services Directive, which establishes specific rules addressing these kinds of services. This new Directive also sets up some ruling with regard to video-sharing platforms, mostly as to the protection of minors and the public interest.

**iii Mobile services**

The provision of mobile television audiovisual services and other ancillary services has been specifically regulated in the General Audiovisual Law. According to this regulation, the provision of mobile television services requires operators to obtain a licence on the same terms as those set out for general audiovisual services as detailed in Section II.iii.

**VI THE YEAR IN REVIEW**

The most significant development in electronic communications over the past few years has been the approval of the General Telecommunications Law.

Regarding the audiovisual sector, although no major laws have been passed in recent months, the allocation of six DTTV channels (three SD and three HD) in October 2015, which commenced broadcasting in April 2016, has entailed a significant change in the competitive private television landscape. This year has also been marked by the NMCC’s continuous intense sanctioning activity in the audiovisual sector, which has mainly been for breaches of advertising-related obligations.
While the consolidation process reached its peak in 2016, the sector is far from being calm, as the main operators reacted against OTT, requesting further regulation of these services in line with that applied to traditional telecom operators to try to safeguard their competitive position; those requests led to the approval of the New Audiovisual Media Services Directive, which sets up certain new rules that will apply both to OTTs and traditional telecom operators and it established further separate regulation for video-sharing platforms.

As regards OMVs, the NMCC has deregulated their market on the basis that it has already achieved a reasonable level of competitiveness. The deregulation involves the removal of the obligation for the main three network operators (Telefónica, Vodafone and Orange) to provide OMVs with reasonable access to their mobile infrastructure.

VII CONCLUSIONS AND OUTLOOK

Looking ahead, and despite the apparent state of calm in the market (at least in terms of legislative activity), there are certain events that have had a significant impact on the Spanish TMT market, such as the implementation of the NIS Directive through Royal Decree-Law 12/2018, of 7 September, and the execution of the GDPR, the move towards regulation of OTTs and the development of further regulations on e-commerce. Additionally, the approval of the New Audiovisual Media Services Directive points to the European authorities’ existing preoccupation with OTT services providers and IoT services addressed to end users in the EU.

Furthermore, the NMCC’s structure is currently under review, and whether the NMCC should again segregate into sector-specific NRAs is under discussion. No laws have been enacted yet in this regard, but this could entail bringing back the former CMT or the creation of a similar NRA.

Finally, the intense consolidation process in the telecoms and audiovisual market experienced in recent years has reduced significantly the number of players in the market. As a result of these transactions, it is expected that the already consolidated operators will use their joint efforts to bring about fast technological developments in a context where the division between platforms and content is becoming increasingly unclear.
I OVERVIEW

With the trend of convergence between telecommunications and media, Taiwan’s existing regulatory regime is out of date, and even hinders the sound development of the TMT sector. To achieve the policy goals of deregulation and fostering market competition, the competent authority, the National Communications Commission (NCC), has formulated a set of policies and proposed amendments of mainly applicable laws to encourage new entrants and eliminate the hurdles for conducting TMT businesses.

Nevertheless, in the wake of emerging OTT services, which are not regulated under the current TMT regulatory regime, the difference in regulation level between the traditional telecom and broadcasting operators and OTT service providers has been raised by the former operators, and they are striving for the introduction of a policy wherein ‘the same legal requirements should apply to services with the same nature’. In this context, the NCC is now also considering how to reach a balance in terms of deregulation and fairness of competition.

II REGULATION

i The regulators

Prior to 22 February 2006, the telecom and broadcasting sectors in Taiwan were regulated by the Directorate General of Telecommunications, the Ministry of Transportation and Communications (MOTC) and the Government Information Office, Executive Yuan, respectively. With the trend of convergence, in the spring of 2006 the two authorities were consolidated into a new independent regulatory agency, the NCC, which is composed of seven full-time commissioners who are appointed by the Premier of the Executive Yuan with the consent of the Legislative Yuan (i.e., the Congress). These seven commissioners serve a four-year term, and may be reappointed for a second consecutive term.

The NCC’s principal duties include, inter alia:

a developing relevant regulations and policies;

b processing applications for licences;

c overseeing the telecom and broadcasting industry;

d allocation of radio frequency spectrum;

e setting information security standards and technical specifications; and

f regulating the content of broadcasting.

1 Patrick Marros Chu is a partner, Vick Chien is a senior attorney and Sam Huang is an attorney at Lee and Li, Attorneys-at-Law.
Main sources of law

The Telecommunications Act (TA) is the main source of law for the telecom sector in Taiwan. Under the authorisation of the TA, the NCC enacts a variety of regulations for different types of telecom services, including without limitation:

- the Administrative Rules on Fixed Network Telecommunications Businesses;
- the Administrative Rules on Third Generation Mobile Communications Businesses;
- the Administrative Rules on Mobile Broadband Businesses;
- the Administrative Rules on Satellite Communications Businesses; and
- the Administrative Rules on Type II Telecommunications Businesses (the Type II Regulations).

For the broadcasting sector, the main source of law is the ‘Three Broadcast Laws’: the Radio and Television Act (RTA), the Cable Radio and Television Act (CRTA) and the Satellite Broadcasting Act (SBA).

Regulated activities

To operate telecom and broadcasting businesses, business operators have to apply for an operating licence from the NCC in accordance with the applicable laws and regulations.

According to the TA, telecom businesses can be divided into two categories: Type I telecom businesses (Type I telecom operators) and Type II telecom businesses (Type II telecom operators). Pursuant to Article 11 of the TA, a Type I telecom operator means an enterprise that installs telecommunications line facilities and equipment to provide telecom services. The aforementioned telecommunications line facilities and equipment refer to network transmission facilities connecting the sending and receiving terminals, the switching facilities installed to be integrated with the network transmission facilities and the auxiliary facilities of both. A Type II telecom operator means a telecom operator other than any Type I telecom operator. Type I telecom operators are generally perceived as facility-based telecom operators, while Type II telecom operators are generally perceived as service-based telecom operators.

The service categories of Type I telecom businesses include:

- integrated network services, local network services, long-distance network services, international network services and leased-circuit services;
- 3G mobile communications services;
- mobile broadband access services; and
- satellite communications services, including satellite fixed network communications services, satellite mobile network communications services and satellite TV programme uplink services.

According to the Type II Regulations, Type II telecom businesses can be further divided into two categories: ordinary Type II services and special Type II services. Special Type II services refer to international simple resales (including domestic long distance calls and international calls), VoIP services, international communication services provided to non-specific persons by leasing international circuits and other telecom services designated by the NCC. Ordinary Type II services are Type II services other than special Type II services.

A Type I telecom operator shall be a company limited by shares and incorporated under the Taiwan Company Act, and the chairperson of the board of a Type I telecom operator shall be a Taiwanese citizen. In addition, Type I telecom operators are subject to the minimum capital requirements.
Generally speaking, the process for obtaining licences includes two stages: first, an applicant must file a written application, business plan and other required documents with the NCC for the establishment permit; second, the applicant has to complete its corporate registration and other statutory requirements (e.g., establishing a network system) so as to submit the relevant documents to the NCC for a business licence within six months of obtaining the establishment permit.

With regard to broadcasting business, the NCC’s prior approval is also required for conducting any of the following activities: providing radio and television broadcasting services; providing cable television (CATV) services; and providing satellite broadcasting services.

iv Ownership and market access restrictions

For a Type I telecom operator, the total direct shareholding by foreigners shall not exceed 49 per cent, and the sum of direct and indirect shareholding by foreigners shall not exceed 60 per cent. Nonetheless, there is no restriction on foreign investments in a Type II telecom operator. Therefore, foreigner investors may acquire a 100 per cent equity interest in a Type II telecom operator.

Foreign investment in a radio or television broadcasting business operator is prohibited. A foreign natural person is not allowed to be a direct shareholder of a CATV operator, and the total direct shareholding thereof by foreign legal persons shall not exceed 20 per cent, and the sum of direct and indirect shareholding thereof by foreigners shall not exceed 60 per cent. Direct foreign investment in a satellite broadcasting business operator shall be less than 50 per cent of the total issued shares. On the other hand, an offshore satellite broadcasting business operator may offer programmes in Taiwan by setting up a branch office or appointing a distributor, provided that the NCC has granted broadcasting approval.

v Transfers of control and assignments

In principle, all licences issued by the NCC are non-transferrable and the assignment of business by telecom or broadcasting operators is not allowed.

If a Type I telecom operator would like to assign all or a substantial part of its business or assets, make investments in other Type I telecom operators or merge with other Type I telecom operators, a prior approval from the NCC would be required. On the other hand, if a Type II telecom operator is merged into other Type II telecom operator or other company, the Type II telecom operator also needs to file a consolidated business plan with the NCC for approval in advance.

The NCC’s approval would be required as well for transferring shares of a radio or television broadcasting business operator. If a CATV operator intends to assign its business, merge with other CATV operators or make investments in other CATV operators, the CATV operator has to file a written re-application and an updated business plan with the NCC for approval. Additionally, neither CATV operators nor satellite broadcasting business operators shall commission the operation of broadcasting business to a third party.

Cross-ownership among broadcasting business operators is subject to general competition laws. In addition, the CRTA stipulates that the total number of subscribers of a CATV operator as well as its affiliates and directly or indirectly controlled CATV operators, shall not exceed one-third of the total number of subscribers in Taiwan. Last but not least, on 12 July 2017, the NCC published a bill of the Anti-Media Monopoly Act (the Anti-Monopoly Bill) to solicit public comments. The Anti-Monopoly Bill aims to set a cap
for mergers or acquisitions among broadcasting businesses and national daily newspapers. However, as this is very controversial, we do not expect that the Anti-Monopoly Bill will be enacted in the near future.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

Purely internet-based services are not deemed by the NCC as telecom services; hence, no telecom licence is required. However, some of the communications services using both IP and traditional telecom networks are still regulated under the TA or the Type II Regulations. For instance, under the Type II Regulations, VoIP services are defined as voice services received and transmitted through the internet. Although this definition is very broad, based on market practice, the NCC holds the view that providing voice communication services through an internet platform or software would not be deemed as a telecom service, and thus would not be subject to the Type II Regulations as long as there is no connection to the traditional telecommunications network (such as PSTN).

For the VoIP services that fall into categories of telecom services, these can be further divided into two types: E.164 internet telephony service and non-E.164 internet telephony service. The former refers to the internet telephony service run by E.164 numbers allocated by the NCC in accordance with the ITU-T Recommendations, while the latter refers to the internet telephony service that is provided without an E.164 number.

Another relevant issue regarding IP regulation that raises industry concerns is whether an OTT service should be regulated as a traditional broadcasting service. Currently, there is no law that specifically regulates online video programme distribution services. Therefore, the provision of pure OTT services in Taiwan would not trigger any licence requirements such as those under the RTA, CRTA or SBA. Nonetheless, if an OTT service is provided in the name of a fixed network telecom operator (e.g., Chunghwa Telecom) by using the PSTN rather than the internet, and the content therein is linear programming, this service would still be deemed a value-added telecom service, and a telecom licence is required. It is worth noting that on 31 May 2019, the Acting Chairperson of the NCC indicated that the NCC is considering proposing a bill of the Audio-Visual Convergence Act to regulate OTT media services by the end of 2019, requiring OTT streaming platforms to report the number of subscribers, fee schemes and other consumer protection-related matters to the NCC.

ii Universal service

In accordance with Article 5 of the Fundamental Communications Act (‘Communications and disseminations should safeguard human dignity, respect the rights of minorities and advance balanced development of cultural diversity’), the NCC is active in promoting universal service. The scope of universal service includes voice service and access to data communications. The former refers to the provision of uneconomic public payphone services and telephone services in uneconomic areas. The latter refers to the provision of access to data communications in uneconomic areas and to elementary and secondary schools and public libraries at a preferential rate. Since mobile broadband has become a fundamental part of the information society, besides traditional voice services and internet access services, providing
ubiquitous wireless broadband access has become a key issue of universal service. In light of
the foregoing, in 2019, the NCC revised the universal service regulation to extend the scope
of universal service to offering mobile broadband services in uneconomic areas.

iii Restrictions on the provision of service

Telecom sector

Due to their nature as common carriers, telecom operators are required to provide telecom
services in a fair and non-discriminatory manner, unless stipulated otherwise in the TA.
However, in the wake of OTT’s development, the issue regarding net neutrality has also been
brought to the NCC’s attention. Accordingly, in the bill of the Digital Communications and
Broadcasting Act (the DCBA Bill), which has been submitted to the Legislative Yuan for
its review and approval, digital communication or broadcasting service providers (including
current telecom and broadcasting operators) should not impose any obviously unfair
restriction on communications protocols and internet traffic control, and such restriction,
if any, should be imposed based on the purposes of facilitating the optimisation of network
transfer and access. However, whether and when the DCBA Bill will be enacted is still not
clear.

With regard to price control, only a Type I telecom operator’s primary tariff (such as
fees for internet access or mobile communications service and wholesale price of the items
designated by the NCC) is subject to a price cap. The currently effective price cap provides
that the aggregate price increases of a Type I telecom operator during any given year shall
not exceed ‘ΔCPI-X’,2 where X is a coefficient set by the NCC. As the NCC has realised that
decreases in retail prices may lead to a price-squeezing effect, it has recently focused on the
tariffs of the more competitive retail telecom services to intermediate and wholesale telecom
services so as to facilitate competition on the retail telecom service markets.

Broadcasting sector

Similar to telecom businesses, CATV operators are deemed by the regulator to be
quasi-common carriers. Therefore, Article 49 of the CRTA provides that CATV operators
shall not reject, without justification, requests from the local populace to subscribe to a
CATV service.

Under the current regulatory regime, a price cap of NT$600 per month per household
for CATV services was set by the NCC, which has never been adjusted since the 1990s even
though the CPI has risen substantially in the past 20 years. In addition, CATV operators are
required to report the subscription tariff to local government agencies within a month after 1
August every year. The local government will examine and decide the actual subscription tariffs
within the price cap (i.e., NT$600) enacted by the NCC, and then make an announcement
of its decision on subscription tariffs accordingly. Currently, the subscription tariffs of CATV
operators are between NT$495 and NT$590. To offer multiple options for subscribers, the
NCC has proposed a bill of multiple subscription tariff schemes for CATV services, which
requires CATV operators to adopt a tiered scheme and provide subscribers with different

2 ‘ΔCPI’ refers to the most current annual rate of increase of the consumer price index (CPI) in Taiwan, as
announced by the competent authority prior to each year of implementation.
packages which contain different combinations of channels. Under the bill, the price cap of NT$600 remains unchanged; however, CATV operators may be exempted therefrom under some circumstances.

iv Privacy and data security
A telecom operator is entitled to refuse to provide telecom services only when the content conveyed through telecommunications appears to endanger national security or public order. In addition, to protect network security, telecom operators are required to regularly conduct self-inspection in accordance with the NCC’s guidelines. Among other measures, telecom operators should set up an information security task force for establishing an information security management mechanism. Information security should be divided into levels A, B and C, and the operator should select a suitable security baseline according to the rating.

With regard to CATV services, the CRTA provides that foreign investments in CATV services shall not affect national security, impair overall industrial developments, hinder fair competition or restrict market competition. It is worth noting that in some recent cases regarding mergers of CATV operators, the NCC held the view that national security may be jeopardised if the source of funds for investments comes from or is related to Mainland China.

The Personal Data Protection Act (PDPA) is a general law regulating the collection, processing and use of personal data in Taiwan. The PDPA requires data controllers to have in place appropriate measures to prevent personal data from being stolen, altered, damaged, destroyed, lost or disclosed. The Enforcement Rules of the PDPA further provide certain technical and organisational measures that data controllers may consider adopting based on the principle of proportionality (i.e., based on the quality and quantity of the personal data involved). Moreover, pursuant to Article 21 of the PDPA, the central competent authority has the power, in its discretion, to prohibit cross-border transfers of personal data if, inter alia, it will prejudice any material national interest. To date, the NCC is the only government agency that has issued a ruling to prohibit telecom and broadcasting operators from transmitting their subscribers’ personal data to Mainland China.

Pursuant to the Communication Protection and Surveillance Act (CPSA), telecom operators must enable the law enforcement authority to conduct monitoring and interception of communications on their systems. Such an obligation is imposed on all Type I telecom operators and certain Type II telecom operators. Pursuant to the CPSA, if there is sufficient evidence that the accused or the suspect is involved in certain material crimes explicitly listed under the CPSA and there is reasonable belief that the content of his or her communications is relevant to the case being investigated, and it is difficult or there are no other methods to collect or investigate the evidence, an interception warrant may be issued. The CPSA also provides that when it is necessary to conduct surveillance on certain communications in order to collect intelligence on foreign forces or hostile foreign forces to protect national security, the head of the competent authority overseeing national intelligence may issue an interception warrant.
IV SPECTRUM POLICY

i Development

Pursuant to the TA, spectrum is allocated by the NCC to various mobile telecom service operators in accordance with the telecom licences they obtain and the Table of Radio Frequency Allocation of Republic of China (Taiwan) promulgated by the MOTC.

The use of spectrum is still highly regulated in Taiwan. Mobile telecom service operators that are entitled to use spectrum should first apply for the NCC’s prior approval if there is any change of their use of the spectrum allocated to them (including the equipment, station or network involved) as indicated in their business plan, which is a required document when applying for a telecom licence. Furthermore, unless stipulated in other regulations (such as the 4G Regulations allowing the transfer of the right to use spectrum between 4G telecom operators with the NCC’s involvement), the right to use spectrum is not allowed to be leased, transferred, lent or split. Accordingly, the value of spectrum is underestimated because of the current restrictions, and the NCC has conducted several studies on the issue of opening a secondary market for spectrum.

In the Telecommunications Management Act (TMA), which was passed by the Legislative Yuan on 31 May 2019, with the effective date to be further determined by the Executive Yuan, the NCC deregulates the use of spectrum so as to have the spectrum used efficiently. Article 58 of the TMA provides that a telecom operator is allowed to transfer part of the spectrum allocated to it to another telecom operator, provided that it first submits the application and the agreement between the two parties to the NCC for its approval. The TMA also authorises the NCC to further promulgate relevant regulations in terms of the scope of the spectrum that may be transferred, the usage of spectrum after transfer, the qualification of the transferee(s), restriction and other management matters.

It is widely recognised that the above-mentioned development would help to establish the secondary market for spectrum in Taiwan after the TMA takes effect. The TMA and other bills proposed by the NCC will substantially change the current regulatory regime of the telecom industry.

ii Flexible spectrum use

With the promising development of IoT services, the NCC notes that IoT services combined with the 5G service may substantially change the telecom industry and everyday life in Taiwan. To facilitate the development of IoT services, the NCC, according to the frequency band used and the quality of service required, divides IoT services into telecommunications grade IoT services (using Narrowband IoT, LTE for machines and massive machine-type communication for future 5G services) and non-telecommunications grade IoT services (using Bluetooth, LoRa, Sigfox, Wi-Fi, Zigbee, etc.).

With regard to non-telecommunications grade IoT services, the original spectrum used was the 922–928MHz, 2.4GHz and 5GHz frequency bands, and a telecom licence is not required. On 22 February 2017, the NCC announced that the 920MHz–925MHz frequency band had also became available for low-power IoT services. On 27 July 2018, the NCC further announced that 839MHz–847MHz in the 800MHz frequency band have also became available for advanced metering infrastructure. As for telecommunications grade IoT services, these are deemed telecom services, and the spectrum they use would be the same as that obtained from the mobile service operators via auctions. The spectrum used in this regard is expected to be the frequency bands below 1GHz.
iii Broadband and next-generation mobile spectrum use

Currently, the radio spectrums must be allocated along with telecom licences and used within certain business scopes. For the purposes of increasing spectrum use efficiency, the TMA allows the NCC to set a spectrum sharing mechanism, free-to-use terms, etc. in advance while it releases spectrums so as to respond to the needs of innovative technologies and services. A telecom operator that has obtained spectrum may file an application with the NCC to provide the spectrum or part thereof to other telecom operators for their use by dividing the spectrum into different subbands, time slots or subregions. Telecom operators may even combine and use their spectrums together, which is expected to bring about dramatic changes to the competition in the relevant markets. In addition, a telecom operator that has obtained spectrum may also file an application with the NCC to return the spectrum after the Executive Yuan makes a public announcement. The NCC will re-auction and re-allocate the spectrum to another telecom operator, and the winning bidder would not be subject to the original usage restrictions.

iv Spectrum auctions and fees

The NCC held the spectrum auctions for 4G services in November 2013 (700MHz, 900MHz and 1,800MHz frequency bands), December 2015 (2,500MHz and 2,600MHz frequency bands) and November 2017 (1,800MHz and 2,100MHz frequency bands). A total of 610MHz bandwidth has been taken by five 4G operators in Taiwan, and as of March 2018, 4G subscription accounts for approximately 82.21 per cent of total mobile communications, which is around 23.5 million subscribers.

To avoid the spectrum being held by a small number of operators, and thus affecting the development of the telecom industry, the bandwidth that each 4G operator can hold is capped at one-third of the total 4G bandwidth and one-third of the total 2,100MHz bandwidth.

In terms of the spectrum usage fees, currently, the annual fee payable is NT$10.675 million per MHz (applicable to 2G, 3G and 4G services) multiplied by the applicable bandwidth and applicable territory factor (e.g., if the mobile service is launched nationwide, the factor would be 1). To encourage 4G operators to construct mobile broadband networks in remote areas, the NCC has revised the Charging Standards for the Radio Frequency Usage Fees by providing a 5 to 15 per cent discount if the coverage rate in remote areas reaches 85 to 95 per cent.

In August 2019, the NCC announced the spectrum that it plans to release for 5G services, including 270MHz in the 3.5GHz frequency band, 2,500MHz in the 28GHz frequency band, and 20MHz in the 1,800MHz frequency band (2,790MHz of bandwidth in total). The total floor price for the 5G spectrum auction to be held at the end of 2019 would be NT$30 billion. The 5G spectrum auction would be conducted in two phases: the first would be a multiple-round auction to determine the amount of bandwidth each bidder can receive; the second would be an auction to determine each bidder's location on the spectrum.
V MEDIA

i Regulation on media distribution generally

The RTA and the SBA require a radio or television broadcasting business operator or a satellite broadcasting business operator to classify the programmes that it broadcasts in accordance with the Regulations Governing TV Programming Rating promulgated by the NCC, and that the programmes are easily identifiable and distinguishable from advertisements.

Radio and television broadcasting business operators and satellite broadcasting business operators are prohibited from broadcasting any programmes or advertisements invested in or produced by the government and related to a certain candidate in elections. If radio and television broadcasting business operators and satellite broadcasting business operators accept sponsorship, they shall clearly disclose the information concerning the sponsors before and after broadcasting programmes.

To develop local cultural industries, the RTA stipulates that locally produced programmes shall not be less than 70 per cent of the total programmes, and locally produced drama programmes broadcast in the time slots from 8pm to 10pm shall not be less than 50 per cent of the total drama programmes. If a satellite broadcasting programme supplier broadcasts dramas, films (including documentaries), variety shows or children’s programmes in specific time slots designated by the NCC, the ratio of locally produced programmes to the total broadcasted programmes shall not be less than 25 per cent and the ratio of premier programmes thereto shall not be less than 40 per cent (decreased to 20 per cent in the case of broadcasting films).

The SBA also requires satellite broadcasting business operators not to broadcast any programmes containing embedded marketing placed by the government, or any programmes invested, produced, sponsored or subsidised by the government without disclosure of relevant information. Furthermore, placing embedded marketing in news-related or children’s programmes is not allowed. When placing embedded marketing in other programmes, satellite broadcasting business operators shall not deliberately affect the content of such programmes, or directly encourage viewers to purchase specific products or services, or exaggerate the effect of such products; and shall disclose the information about the business operator who placed the embedded marketing before and after the programmes.

ii Internet-delivered video content

With the development of technology and communications, OTT services that are being provided via the internet have not only gradually impacted the existing industries, but have also brought various challenges for regulatory bodies. It is noted that at present, the NCC does not regulate OTT TV being provided online, but has drafted the DCBA Bill as the basic principles of the internet, which introduces the spirit of internet governance and light touch as a positive response to the needs of the times.

It is worth noting that at this stage, the business scale of Taiwan OTT TV service is still not substantial, and operators are still testing the water and trying to find a profitable business model. On the other hand, as some of the TV programme content delivered through OTT TV services may raise piracy concerns, content owners are also urging the NCC to take anti-piracy measures such as revising relevant laws requiring telecom operators to block illegal websites where piracy content came from. Nevertheless, the NCC has yet to decide on adopting such an approach due to freedom of speech concerns.
VI THE YEAR IN REVIEW

On 31 May 2019, the TMA was passed by the Legislative Yuan, with the effective date to be further determined by the Executive Yuan. The TMA will result in major structural changes to the regulatory environment and the telecom industry. The TA divides the telecom industry into various types of businesses based on whether business operators own relevant telecom facilities, thereby adopting a vertical regulatory regime, and a telecom service provider that does not have prior approval from the NCC would be subject to criminal sanctions and severe administrative penalties. However, the TMA adopts a horizontal regime, which separates the telecom industry into three levels: the infrastructure level (telecom networks), the operation level (telecom services), and the content/application services level. Moreover, to encourage new entrants to enter the market and to give them the flexibility to conduct business operations, the TMA has changed the mechanism of market participation to voluntary registration. Telecom service providers that choose not to register as telecom operators may still provide telecom services to consumers. Nonetheless, if a telecom service provider intends to obtain certain rights or resources conferred by the TMA (e.g., applying for allocation of radio frequency), it would still need to register as a telecom operator.

In furtherance of establishing telecom infrastructure, the TMA has removed the punishment of unauthorised telecom networks under the TA, which means that entities may establish their own telecom networks according to their needs without obtaining prior approval from the NCC. Furthermore, entities may organise telecom networks by means of leasing others’ telecom networks or using network slicing technologies instead of establishing their own telecom network. For the purposes of increasing spectrum utilisation efficiency, the TMA allows the NCC to set a spectrum sharing mechanism, free-to-use terms, etc., in advance when it releases spectrums so as to respond to the needs of innovative technologies and services. In addition, the TMA also authorises the NCC to ban the purchase and use of certain telecom equipment for national security reasons.

VII CONCLUSIONS AND OUTLOOK

i Telecoms sector

The current TA was promulgated 60 years ago. Although it has been revised several times, the regulatory structure therein obviously cannot meet market changes caused by evolving IT technologies and the convergence of the telecom and broadcasting sectors. In response to emerging OTT services and formulating a fair market competition environment, the NCC has taken the lead by drawing up and promoting the TMA and DCBA Bill under a converged legal framework. On 31 May 2019, the TMA was passed by the Legislative Yuan, with the effective date to be further determined by the Executive Yuan. Under the TMA, the concept of Type I and Type II telecom businesses would be abandoned, and only those intending to provide telecom services by using frequencies, numbers or rights-of-way would be required to register in advance with the NCC. In addition, current telecom operators with significant market power (SMPs) would not necessarily be SMPs under the TMA, which situation would be assessed by several market parameters, such as the maturity of such SMP’s services and technologies, the geographical regions it covers, and issues in supply and demand.

On the other hand, the DCBA Bill is in essence a guide or code of practice that has no mandatory effect on market players. The DCBA Bill stresses self-discipline by providers and users of internet services, and collaboration between the private sector and the public sector, as well as minimal use of government regulation.
ii Media sector

Owing to the restriction whereby the government cannot invest in the broadcasting sector (including CATV business), any entity, so long as any of its share is held by the government or a government-owned fund, would not be allowed to acquire a broadcasting business. Such prohibitions have prevented a number of proposed buyouts by listed Taiwan companies, as almost all of Taiwan’s major listed companies have some portion of their shares purchased by government-owned funds.

The NCC has been aware of that unreasonable restriction, and has proposed amendments to fix this hurdle for the acquisition of broadcasting businesses. Nevertheless, as the issue of how large a percentage of shares of a broadcasting business could be held by an investment involved with government funds is quite politically sensitive, the political parties so far have not yet reached a consensus. As a result, recently several acquisition cases have been rejected by the NCC merely because of such unreasonable restriction, even where the NCC itself is of the opinion that the market would benefit from such acquisition. Without doubt, the zero-government fund restriction is a critical hurdle that the NCC has to fix for the sound development of the media sector in Taiwan.

It is worth noting that on 31 May 2019, the Acting Chairperson of the NCC indicated that the NCC is considering proposing a bill of the Audio-Visual Convergence Act to regulate OTT media services by the end of 2019, requiring OTT streaming platforms to report the number of subscribers, fee schemes and other consumer protection-related matters to the NCC. Currently, however, it is still at an early stage to predict how the bill would regulate OTT media services, but this development is certainly worthy of being noted.
Chapter 19

UNITED ARAB EMIRATES

David Bintliff, Lena El-Malak, Christopher Eklund, Mayowa Olusola, and Ayah Abdin

I OVERVIEW

As the UAE prepares to welcome the world in 2020 as the first country in the Middle East, Africa and South Asia to host Expo, the country continues to be a beacon for technology and innovation. As a country that has achieved global recognition for its transformation and diversification, the UAE shows no sign of standing still.

On 25 September 2019, the UAE launched its first astronaut programme, sending Hazaa Al Mansouri into space. The UAE plans to send an unmanned spacecraft to Mars 2021 as part of the Hope Mars Mission. If successful, that would be the Arab world’s first mission to Mars.

Smart Dubai 2021 aims to move to a 100 per cent digital future within four years leading to the Dubai government issuing its last paper transaction by 2021. Government planning extends to the year 2071 across a programme that includes the following objectives: (1) fortifying the country’s reputation; (2) diversifying imports and exports by relying less on oil; (3) investing in education focusing on advanced technology; (4) building Emirati values and ethics for the future generations; (5) raising productivity of the national economy; and (5) enhancing society’s cohesion. Technological change sits at the heart of this agenda.

While the UAE’s regulatory schemes continue to develop, the government is also actively addressing the natural tension between regulation and innovation. The country has been keen to incorporate best of breed learnings from successful innovation hubs such as Silicon Valley. The Dubai Future Accelerators initiative, for example, brings together top international companies and entrepreneurs to address seven key ‘21st century opportunities’. This includes the application of cutting-edge technologies such as AI and robotics, genomics, 3D printing, distributed ledgers, biomimicry and biotechnology, as well as new business models and ways of working. In March 2019, Abu Dhabi government launched Hub71, a 1 billion dirham mega hub that aims to bring together start-ups, innovators and global and regional leaders in technology and venture capital, such as Microsoft and Mubadala.

At a regulatory level, we expect significant changes in the near future in areas such as data privacy and healthcare. We understand that the Telecommunications Regulatory Authority (TRA) is looking at implementing a federal level data privacy law, as part of the UAE National Cybersecurity Strategy, which, if enacted, will have a significant impact on companies that collect, process, host and transmit data within the UAE.

---

1 David Bintliff is a partner, Lena El-Malak, Chris Eklund and Mayowa Olusola are associates, and Ayah Abdin is a trainee associate at Bird & Bird.
II REGULATION

i The regulators

Formed in 1971, the United Arab Emirates is a constitutional federation of seven emirates, each with their own laws and each subject to federal laws. Free zones within emirates may issue their own laws, applicable within the relevant free zone, but are subject to the Federal Penal Code. The free zones are often referred to as offshore while the rest of the UAE is referred to as onshore.

The regulatory framework for the TMT sector in the UAE is divided into two sub-sectors: telecommunications and technology, and media, although convergence has led to a degree of overlap. In addition, as other sectors continue to digitally transform their everyday operations, there might be sector-specific considerations and legislations relating to technology outside the TMT sector in the UAE, such as in healthcare, banking or litigation.\(^2\) These sector-specific considerations are not covered as part of this chapter.

Telecommunications and technology

The principal regulator of the telecommunications and technology sector is the TRA, which was established under the law regarding the Organisation of the Telecommunications Sector (the Telecoms Law).\(^3\)

The TRA has two stated focuses: regulating the telecommunications sector and enabling government entities in the field of smart transformation.\(^4\)

It is responsible under the Telecoms Law for a range of functions, including ensuring telecommunications services provided throughout the UAE sufficiently satisfy public demands and enhancing the level of service provided by the telecommunications sector.\(^5\)

In addition to the Telecoms Law, the TRA is also bound to act in accordance with the Executive Order,\(^6\) the Licensing Framework Resolution\(^7\) and the National Agenda.\(^8\)

Media

The National Media Council (NMC) is the federal authority tasked with supervising media activities in the UAE. It is mandated to:

\(a\) develop the UAE’s media policy;
\(b\) draft media legislation and ensure its execution;
\(c\) coordinate media policy between the emirates; and

\(^3\) Federal Decree Law No. 3 of 2003 as amended by Federal Law No. 1 of 2005 and Federal Law No. 5 of 2008 (the Telecoms Law).
\(^5\) Article 13, Telecoms Law.
\(^6\) The Decision of the Supreme Committee for the Supervision of the telecommunications Sector No. (3) of 2004 issuing the Executive Order of the Telecoms Law.
\(^7\) TRA Resolution No. (6) of 2008 regarding the Licensing Framework.
d issue operating licences to media companies.\textsuperscript{9}

Federal Law No. 15\textsuperscript{10} (the Media Law) regulates printing and publishing licensing activities in the UAE and applies to traditional media content such as newspapers, magazines and television broadcasting. A 2010 Chairman's Resolution extended the application of the Media Law to all audio, visual, print and digital media institutions in the UAE.\textsuperscript{11}

In March 2018, the NMC established a new system to govern electronic and digital media activities in the UAE. Under Cabinet Decision No. (23) of 2017 Concerning Media Content (the EM Regulations), any individual or company carrying on electronic media activities\textsuperscript{12} in the UAE must obtain a licence from the NMC. The websites of licensed traditional media (i.e., television, radio, newspapers and magazines) already fall under the provisions of the EM Regulations and, as such, are not required to secure new licences.

In addition to the federal laws referenced above, some free zones in the UAE also regulate broadcasters and publishers operating within the parameters of their jurisdictions.\textsuperscript{13}

\textbf{ii Regulated activities}

\textit{Telecommunications and technology}

Under the Telecoms Law, any sale, provision or operation of a telecommunication service requires a licence.\textsuperscript{14}

Telecommunication services are defined as transmitting, broadcasting, switching or receiving by means of a telecommunications network. This includes, for example, wired and wireless telecommunications; voice, music and other audio material; and visual images.

The provision of internet services to subscribers also requires a licence,\textsuperscript{15} as clarified in Article 66 of the Executive Order.

There are two types of licences:\textsuperscript{16} individual licences for services that require substantial regulatory supervision or usage of scarce resources (e.g., spectrum); and class licences\textsuperscript{17} where there is no need to use scarce resources of spectrum and numbers or less regulatory supervision is required.\textsuperscript{18} Both licences are issued for 10-year periods.

\textsuperscript{9} UAE Federal Law No. 1 of 1972 on the competencies of ministries and powers of ministers, and concerning the establishment of the National Media Council as amended by Federal Decree Law No. 1 of 2006.
\textsuperscript{10} Federal Law No. 15 of 1980 concerning Printing and Publishing and its amendments (the Media Law). An amendment to the Media Law was proposed in 2009, but not signed into law.
\textsuperscript{11} Chairman of the NMC Resolution No. 20 of 2010 Concerning Media Content Standards.
\textsuperscript{12} All online activities including e-commerce, publishing and selling of print, video and audio material ‘even if practiced on social media’.
\textsuperscript{13} For example, Dubai Media City, regulated by Dubai Creative Clusters Authority, and Two Four Fifty Four, the media free zone in Abu Dhabi.
\textsuperscript{14} Article 37, Telecoms Law.
\textsuperscript{15} Except in the case of internet service provided onboard aircraft, which can be provided without a licence above 10,000 feet. See Aeronautical Radio Systems Regulation issued by the TRA on 14 March 2018.
\textsuperscript{16} TRA Resolution No. (6) of 2008 regarding the Licensing Framework (the Licensing Framework Resolution).
\textsuperscript{17} Not to be confused with class licences granting a general authorisation to provide certain telecommunication services to a number of service providers providing the same class of service as used in the UK regulatory regime and other jurisdictions.
\textsuperscript{18} Article 4(2)(b) of the Licensing Framework Resolution.
There are currently two licensed providers of public telecommunications services in the UAE: Etisalat and du.

The telecommunications sector is currently excluded from the scope of the most recently enacted competition law in the UAE. 19

**Media**

Under the Media Law, certain activities require a licence, including operating a printing press or publishing house; circulating, selling or distributing printed material; and the publication of newspapers. 20

Applications must be filed online via the NMC’s website, and the fees payable depend on the type of licence sought.

As noted previously, any individual or company carrying on electronic media activities is required to obtain a licence from the NMC. 21

Restrictions apply under the Media Law and the EM Regulations in respect of the types of individuals and entities that can apply for a licence.

**Internet of things**

The UAE has an ambitious internet of things (IoT) strategy. Through projects such as the ‘Dubai Internet of Things Strategy’, the UAE seeks to build the world’s most advanced IoT ecosystem. As part of this, the TRA has published policy and regulatory procedures regulating the internet of things (IoT Policies). 22 These IoT Policies give the TRA regulatory powers in relation to IoT services in the UAE and set forth certain principles with respect to the associated data. The IoT Policies apply broadly and will be relevant to individuals, companies, public authorities and other legal entities concerned with IoT in the UAE (including foreign IoT providers that provide IoT services remotely into the UAE). An overview of the principal requirements includes the need to register with the TRA and to obtain a registration certificate. To obtain a registration certificate a UAE presence or appointed UAE representative is required by the TRA. In addition, there are various data-focused requirements such as data storage requirements and purpose limitation requirements. In the absence of any additional grace periods IoT suppliers need to be compliant with the IoT Policies at the time of writing.

**Future technology**

The UAE government has issued new legislation under which a temporary licence can be granted for projects that use modern technologies (including the use of artificial intelligence) which are not currently governed by legislation in the UAE. 23 This temporary licence may be granted as a temporary measure while appropriate legislation regulating the project or technology is prepared.

19 Federal Law No. 4 of 2012 on the Regulation of Competition. However, a sector may be listed as exempt due to another law or regulation regulating competition in that sector; for example, the TRA has authority to regulate competition in the sector.

20 Articles 3, 17, 24, 49, 54, 66 and 67 of the Media Law.

21 Refer to the EM Regulations.


23 Federal Decree-Law No. 24/2018 on Futuristic Projects; Cabinet Decision No. 14/2019 on the Regulation of Issuance of Temporary Licences for Futuristic Innovative Projects
iii Ownership and market access restrictions

General foreign ownership restrictions

Currently, foreign companies can only operate onshore in the UAE by partnering with a UAE national or wholly owned UAE entity, with the UAE national or entity having 51 per cent ownership.24 Companies established in the free zones are exempt from this restriction, and may have 100 per cent foreign ownership.25 A limited liberalisation of the onshore position was introduced in September 2018 allowing foreign ownership of some companies operating in 13 sectors.26

Telecommunications and technology

Licence holders under the Telecoms Law (individual and class) must be a company established under the Commercial Companies Law27 whose shareholding accords with a resolution of the TRA Board.28

TRA Resolution No. 8 of 2009 restricts the foreign ownership of global mobile personal communications service licensees or public access mobile radio service licensees to 49 per cent.29

At the time of writing, there are no public constraints on aggregate holdings of spectrum and licences but, in the future, as the number of new entrants increase, there may be changes to help the TRA manage competing claims for spectrum.

Media

Article 2 of the Media Law (and subsequent resolutions issued by the NMC) provide that the owner of a media service must be a UAE national. This means that a media entity with foreign ownership must either partner with a UAE national or wholly owned UAE entity to set up an onshore entity or, as noted above, set up in a free zone that permits 100 per cent foreign ownership.

iv Transfers of control and assignments

Licence transfers require the written approval of the TRA.30

There is also an express obligation to obtain the prior written consent of the TRA in the event of a merger or acquisition, transaction, contract, reorganisation, sale or other corporate venture that results in the change of control of a licensee.31

24 Article 10, Federal Law No. 2 of 2015.
27 Federal Law No. 2 of 2015.
28 Articles 28 and 29 Telecoms Law; and Articles 2(1) and 3(1) NMC Resolution No. (7) of 2008.
29 Resolution No. 8 of 2009 Regarding the Approval of Acquisition Fees and Licensing Applications.
30 Under the Telecoms Law, the Executive Order and each licence. Note, the blanket prohibition on assigning spectrum authorisations under Article 5.5 of the Radiocommunications Policy.
31 Under each provider's licence, e.g., Article 3.4.2 of the Emirates Integrated (du) licence.
III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation
The Telecoms Law makes no regulatory distinction between internet and IP services and other telecommunications services. Such services fall within the definition of a regulated activity and thereby require a licence from the TRA. That said, certain specific policies cover the provision of internet and IP services in the UAE.

For example, it is TRA policy that the provision of VOIP services requires a licence.32 There are two exceptions: where the network is operated for the benefit of users within the same company or group; or where the network is operated for an educational purpose, research purposes or for the benefit of UAE government entities. Otherwise, the provision of consumer IP services is not permitted in the UAE, and access to a number of these services such as Skype consumer and Facetime are blocked.33

ii Universal service
As noted previously, the TRA is tasked with ensuring that telecommunication services provided in the UAE are sufficient to satisfy the public demands of those who wish to make use of such services.34 It also has the authority to create conditions on universal service in the UAE.35 To this end and, in addition to certain financial obligations for universal service funding in each telecoms licence, the TRA has issued a regulatory policy on the promotion of universal telecommunications services in the UAE (USO Policy).

Under the USO Policy, the TRA will designate one or more licensees as having an obligation to provide universal services in the UAE (a universal service provider (USP)). A USP must ensure that consumers in permanent accommodation have access to a service capable of delivering basic voice, TV services and high-speed data packages of at least 10Mbps. A USP may subcontract its USO to other licensees who are able to provide the services more efficiently provided that it obtains approval from the TRA.

At this stage, there are no official government subsidies for the construction of broadband infrastructure and innovative communications technologies. However, the government is heavily invested in telecommunication companies who in turn invest in deploying new broadband infrastructure. This differs from other countries and regions (including the European Union) where public funding is made directly available for broadband deployment.

iii Restrictions on the provision of service
Pricing regulation
The TRA has in place a regulatory policy on pricing36 that prohibits a licensee from pricing in a way that is anticompetitive, and that could restrict, distort or prevent competition in the

33 However, licence holders Etisalat and du have both recently introduced their own VOIP-based apps, BOTIM and C’ME as part of their unlimited voice and video call services. It is also important to note that Enterprise VoIP solutions, such as Microsoft’s Teams are not blocked when used within a closed network.
34 Article 13 of the Telecoms Law.
35 ibid., Article 14.

© 2019 Law Business Research Ltd
short term or in the long term; or restricts, distorts or prevents the growth and development of the telecommunication sector of the UAE, the exception being in the case of a public emergency.

The TRA recently published a new regulatory policy and procedure on price control, which provides that each licensee must request prior approval before implementing any change in price, including where there is a price promotion.

Interconnection

Licensees are required pursuant to the terms of their licence to permit interconnection with each other’s networks. There are regulations on interconnection pricing and corresponding fee schedules that either du or Etisalat may be required to comply with.

Net neutrality and monitoring

There is no net neutrality obligation in the UAE, and in the absence of one, licensees technically have the freedom to block or favour certain content over other content. Content is typically blocked on the grounds of public or political policy or as a result of TRA policies (i.e., the prohibition on VOIP services discussed above).

The network operators monitor content accessed through their network in order to assist with the enforcement of laws in the UAE.

Unsolicited communications

Under Article 5 of the Unsolicited Electronic Communications Regulations, telecommunication licensees must establish practical measures to minimise the transmission of spam having a UAE link across their telecommunications networks. If they become aware of such spam, they are under an obligation to take all practical measures to end its transmission or breach the regulations.

For those entities which are not telecommunications licensees, there is no express obligation under the privacy laws in onshore UAE to obtain consent for marketing communications, although in practice it is recommended to do so to align with best practice in other jurisdictions such as Europe. For those operating in free zones such as the Dubai

---

39 ibid., Article 4.1.
40 Public Telecommunication Licences No.1 of 2006 and No. 2 of 2006 respectively.
43 Whether they are required to comply depends on whether they have market power (as defined in the TRA’s Instructions on Cost Accounting, Accounting Separation and LRIC Modeling, Version 3.0 dated 14 July 2010).
44 In 2017, the principal reason why content was blocked was because it contradicted the ethics and morals of the UAE: https://www.tra.gov.ae/userfiles/assets/KK8LZJGR1.pdf.
45 Version 1.0 issued 30 December 2009.
46 ibid., Article 5.2.
International Financial Centre (DIFC)\textsuperscript{47} and Abu Dhabi Global Markets (ADGM),\textsuperscript{48} an individual must be notified and given the right to object to its data being used for direct marketing purposes.

\textbf{iv Security}

\textit{Protection of national interest and law enforcement}

National standards for content exist under the Media Law and NMC resolutions, including prohibitions on material that is harmful to the UAE’s interests or criticises the government or rulers of the UAE. These are discussed in further detail in Section V.

The telecommunication providers are required to assist the government with criminal enforcement. Article 8.2 of Etisalat’s licence requires that it complies with directions of the TRA or other competent authority that may be issued from time to time on public interest, safety or national security. It must also maintain call logs for its subscribers and install such equipment as the TRA needs to allow access to its network and the retrieval and storage of data for reasons of public interest, safety and national security. Likewise, satellite licensees must permit access to their premises for inspection by the TRA and otherwise comply with the directions of the TRA with regard to public interest, safety and national security.

Telecommunication licensees are required to register any mobile consumer who purchases a mobile sim card and mobile services, including obtaining and verifying their identification details and storing such information in a database.

The UAE legislature has taken steps to protect national interests under the Cyber Crimes Law,\textsuperscript{49} as described in Section IV.

\textit{Personal data and privacy protection}

There is no general data protection law in onshore UAE and no single national data protection regulator. An individual’s right to privacy is enshrined in the UAE Constitution\textsuperscript{50} and the UAE Penal Code. It is, however, worth mentioning that the TRA is looking at implementing a data privacy law, as part of the UAE National Cybersecurity Strategy. A draft of the law has yet to be made public. Likewise, the DIFC has amended its Data Protection Regulations to bring them more in line with GDPR and international best practices,\textsuperscript{51} and we understand that it is expected to issue a new data privacy law before the end of the year.

\begin{footnotesize}
\textsuperscript{47} Article 9 of DIFC Law No.1 of 2007 (the Data Protection Law) as amended by DIFC Laws Amendment Law, DIFC Law No. 1 of 2018.
\textsuperscript{48} Section 2 of ADGM Data Protection Regulations 2015.
\textsuperscript{49} Federal Decree-Law No. 5/2012 on combating cybercrimes as amended. On 13 August 2018, HH Shaikh Khalifa Bin Zayed Al Nahyan approved Decision No. 2 of 2018 with regard to the amendment and replacement of Articles 26, 28 and 42 of the Cyber Crimes Law. Not published at the time of writing, we understand that this decision will increase the fines and penalties of imprisonment for establishing, managing, running a website or publishing information in favour of a terrorist group or that affects national security.
\textsuperscript{50} Article 31 of the Constitution confirms the right to privacy of communications.
\end{footnotesize}
For example, under the Penal Code it is an offence to disclose the secret\(^{52}\) of another without their consent. A company must obtain consent from individuals before collecting personal details of individuals, whether that is a consumer or an employee.

When obtaining consent electronically, companies must ensure that individuals granting consent to the use of their personal information must signify consent through some form of positive act. Collecting an individual’s personal information without first obtaining consent has the potential to carry criminal liability.

More comprehensive data protection laws apply to companies incorporated in a free zone with its own data protection laws, such as the DIFC and ADGM.\(^{53}\)

Companies using tracking technologies such as cookies should be aware of the Cyber Crimes Law. Article 2, for example, creates an offence for anyone who gains access to, inter alia, a website, computer network or electronic information system without consent. The Cyber Crimes Law also carries criminal liability.

**Protection of children online**

To deal with an increase in crimes against children online, the UAE has established various child protection initiatives. A UAE based non-profit organisation called e-safe aims to create a safer online experience and to protect children from all types of exploitation.\(^{54}\)

In 2016, a child protection law\(^{55}\) was issued by the government. The law obliges telecommunication companies to notify the competent authorities or concerned entities of any child pornography being circulated on the internet.\(^{56}\)

**Cybersecurity in the UAE**

The Cyber Crimes Law was designed to prevent crimes online and promote a safer digital environment.\(^{57}\)

Offences include gaining access to an individual’s electronic system without permission,\(^{58}\) invading an individual’s privacy using electronic means and using a false internet protocol address for the purposes of concealing a criminal activity. Punishment for breach of the law can lead to imprisonment and fines.

The UAE established the UAE Computer Emergency Response Team to improve information security standards and practices and to protect IT infrastructure in the UAE.

---

\(^{52}\) Generally accepted to mean any personal information about an individual, including any photographs where an individual or their belongings are identifiable: Section 379.

\(^{53}\) Supra notes 41 and 42.


\(^{55}\) Federal Law No. 3 of 2016 on child rights (Wadeema’s Law).

\(^{56}\) ibid., Article 29.

\(^{57}\) Federal Decree-Law No.5 of 2012 on combatting IT crimes (the Cybercrimes Law), as amended by Federal Decree Law No. 2 of 2018 (the Amending Decree).

\(^{58}\) This would encompass the use of cookies and other tracking technologies without consent.
IV SPECTRUM POLICY

i Development

In common with other jurisdictions, the UAE operates a licensed spectrum regime, and the TRA has in place a spectrum allocation regulation and a spectrum fees regulation.

ii Flexible spectrum use

The UAE has implemented, and is in the process of implementing, a number of strategies with respect to spectrum licensing:

a. digital dividends, which will occur when spectrum is freed up as operators switch from analogue to digital transmissions;

b. LTE standards, which may utilise spectrum more efficiently than certain alternative technologies;

c. spectrum sharing: the TRA Regulations on Spectrum Allocation and Cordless Telephony allow for spectrum sharing, and place a special emphasis on reviews and audits of such proposed sharing to ensure there is no mutual harmful interference; and

d. mobile monitoring stations: the TRA has purchased a mobile monitoring station with the objective of monitoring frequencies and better managing spectrum.

iii Broadband and next-generation mobile spectrum use

Like many other jurisdictions, the demand for broadband services has increased in the UAE. To this end, and to encourage the deployment of the new 5G broadband technology, the TRA has created a steering committee with respect to the introduction and deployment of 5G technology. To manage UAE spectrum more efficiently in the provision of 5G services, the TRA supports the use of harmonised spectrum bands for 5G, and is considering the 40GHz for 5G technology beyond 2020.

Both du and Etisalat launched their 5G network in the Middle East and North Africa region (MENA) region in June 2019. Users can enjoy 5G service access on select smartphones only. The three devices that currently grant users access to the 5G network are ZTE Axon 10, the Huawei Mate 20X 5G and OPPO RENO 10X 5G. Technology analysts estimate 5G connectivity will boost the GCC economy by US$269 billion over 10 years with cheaper, faster internet access and connecting devices through the IoT.

To meet the growing demands for broadband services, the TRA has introduced exceptions to the blanket requirement for a spectrum authorisation for any use of spectrum in the UAE. For example, the provision of Wi-Fi services in public places (i.e., hotels, cafes) can be provided by any person without a formal spectrum authorisation from the TRA, provided certain conditions are met.

59 Spectrum Allocation and Assignment Regulations version 1.0 issued 30 December 2009.
60 Frequency Spectrum Fees version 3.0 issued 7 January 2016.
63 ibid., 57.
64 TRA press release: TRA Launches the 5G in the UAE, 23 December 2017.
66 Article 2.4 of the Spectrum Allocation and Assignment Regulations version 1.0 issued 30 December 2009.
67 See Article 2.2 of the TRA Regulations on the Use of 2.4GHz and 5.8GHz bands for WLAN and RLAN: version 1.0, issued on 5 August 2009 (WLAN Regulations).
Spectrum auctions and fees
There are currently no plans to auction spectrum in the UAE.

V MEDIA

i Restrictions on the provision of service

Telecommunications and technology
The TRA implements an internet access management (IAM) policy in the UAE, in coordination with the NMC and Etisalat and du, the licensed ISPs. The policy must be taken into consideration by the ISPs to ensure the security of the internet and to protect end users from harmful websites that are contrary to the UAE’s religious and ethical values. Restricted content under the IAM policy includes pornography, nudity, vice and offences against the UAE. The TRA also monitors online advertising in its enforcement of the IAM policy and has discretion to block online content if found contrary to the policy and other local legislation.

Media
The Media Law sets national standards for media content. Restrictions include prohibitions on material that is harmful to Islam or harms the UAE’s interests; material criticising the government or rulers of the emirates or the UAE; and publishing news, photographs or comments that invade the privacy of individuals and families or destroy reputations.

A 2010 Chairman’s Resolution extended the Media Law (including the content restrictions thereunder) to all audio, visual, print and digital media institutions in the UAE.

The EM Regulations 2017 reinforce the existing restrictions for media content and their extension in scope to include digital activities. The Regulations also create a Website Censorship Committee tasked with ensuring websites comply with the principles and standards of media content set out in the legislation, and recommending websites to be blocked and keywords to be banned on the internet.

NMC Chairman’s Decision No. 35 of 2013 regulates the content of advertising materials. Advertisements that are produced, placed or distributed within the UAE or imported into the UAE must abide by the national standards for media content and the Media Law.

Finally, the Penal Code includes specific provisions regarding defamatory content.

In addition to the federal laws above, some free zones in the UAE also regulate broadcasters and publishers operating within the parameters of their jurisdictions. Examples include Dubai Media City, regulated by the Dubai Development Authority, and Two Four Fifty Four, the media free zone in Abu Dhabi.

---

68 TRA Internet Access Management Regulatory Policy (Version 1.0) issued on 19 April 2017 (the IAM policy).
69 For statistics on blocked content, see www.tra.gov.ae/userfiles/assets/KK8LZjJGR1.pdf.
70 Comprising representatives from the Ministry of Interior, TRA and National Electronic Security Authority.
71 Article 372 deals with publicity that exposes the victim to public hatred or contempt and Article 373 deals with a false accusation that dishonours or discredits the victim in the public eye.
ii Internet delivered video content

Online video subscriptions across the MENA region exceeded 1 million in 2017, up 48 per cent from the previous year.\textsuperscript{72} Subscriptions are forecast to grow at a compound annual growth rate of 34.4 per cent over six years, reaching 5 million in 2022.\textsuperscript{73}

That growth is likely to be more pronounced in the UAE, a market with high internet and mobile penetration rates, government support for internet ubiquity and the presence of a significant youth population. Relative to the country’s high gross national income per capita, broadband is also affordable for many users.\textsuperscript{74} In the UAE, consumers spend an average of 4.7 hours weekly on smartphones watching online videos, and 71 per cent of internet users watch films online.\textsuperscript{75}

As in other jurisdictions, telecom operators in the UAE have suffered a decrease in revenues due to the emergence of OTT players in the market. That has led to a debate around the cost of network infrastructure rollout, OTTs’ contribution towards such costs, and whether network operators and OTTs operate on a level regulatory playing field.

VI THE YEAR IN REVIEW

On 6 February 2019, the President of the UAE issued Federal Law No. 2 of 2019 (the Health Data Law),\textsuperscript{76} which regulates the use of information and communications technology (ICT) in the healthcare sector. The law was introduced to increase the use of ICT in health fields, while ensuring the safety and security of health data and information. Some of the notable provisions of the law include Article 13, which imposes a data localisation requirement for the storage and transfer of health information and impacts the use of non-UAE based cloud service providers in the healthcare sector.

In March 2019, Uber announced plans to acquire the regional ride hailing app Careem for US$3.1 billion.\textsuperscript{77} While the acquisition, which is expected to close in 2020, was viewed as another success story for e-commerce startups in the UAE,\textsuperscript{78} it is still being challenged by the competition authority in Qatar.\textsuperscript{79}

Also in March 2019, the Abu Dhabi government launched Hub71, a 1 billion dirham mega hub that aims to bring together start-ups, innovators and global and regional

\textsuperscript{72} MENA Pay TV & Online Subscription Video Market Monitor, IHS Markit, 2018.
\textsuperscript{73} ibid.
\textsuperscript{75} Growth in Pay TV and OTT Video Services Paving Way for Hybrid TV Viewing, Frost & Sullivan, 2017.
\textsuperscript{76} Federal Law No.2 of 2019 On the Use of the Information and Communication Technology (ICT) in Health Fields, issued on 06 February 2019.
\textsuperscript{77} Forbes: Uber Acquires Careem for $3.1 Billion as the Middle East Startup Pushes to Become a Super App, https://www.forbes.com/sites/michellelevans1/2019/03/26/meet-careem-ubers-3-1-billion-new-acquisition-in-the-middle-east/#39f7f00c1e3c.
\textsuperscript{79} MenaBytes: Qatar blocks Uber’s acquisition of Careem in the country, https://www.menabytes.com/qatar-blocks-uber-careem-deal/.
leaders in technology and venture capital, like Microsoft and Mubadala, with the aim of accelerating Abu Dhabi’s economy and positioning the capital as a preferred destination for tech companies and start-ups.\(^{80}\)

In April 2019, the UAE launched a national strategy for artificial intelligence (AI) with the aim of employing artificial intelligence in vital areas in the UAE to improve customer services and increase living standards.\(^{81}\)

Tech giants Microsoft and AWS both announced the launch of data centres in the Middle East in a race to become the leading cloud service providers in the region. In June 2019, Microsoft announced the launch of two new data centres in the UAE.\(^{82}\) Amazon Web Services (AWS) closely followed suit in July by announcing the launch of a data centre in Bahrain.\(^{83}\)

VII CONCLUSIONS AND OUTLOOK

In 2019, the UAE continued to position itself as a regional hub for emerging technology and innovation, by introducing regulations governing the IoT, adopting a national strategy for AI and launching 5G.

In addition, the UAE is gearing up to host Expo 2020 between 20 October 2020 and 10 April 2021, under the slogan of ‘Connecting minds: Creating a better tomorrow’, which is likely to boost the economy and attract foreign investment in the country, particularly in the TMT sector.

We anticipate that the UAE’s ambitious plans for smart cities, autonomous transportation and blockchain technology will continue to cement the country’s position as a leader in this field.

Challenges still exist. The question regarding public and private data ownership is likely to be a source of future debate, particularly in light of the Dubai Data Law,\(^{84}\) which allows the government to require private sector entities to provide Dubai data\(^{85}\) for the purposes of making that information open data. The UAE may also consider revisiting its restrictions on VoIP services if it wants to stimulate the exchange of ideas and innovations across borders, and relax its localisation requirements for the storage of data to enable businesses to benefit from the agility and scalability that can only be achieved through the use of public cloud platforms.


\(^{84}\) Dubai Law No. 26 of 2015 on the Regulation of Data Dissemination and Exchange in the Emirate of Dubai.

\(^{85}\) Any data related to the Emirate of Dubai and available to data providers.
I  OVERVIEW

The Office of Communications (Ofcom) and the Communications Act 2003 (Act) regulate the UK communications landscape. Ofcom’s current priorities are set out in its 2019–20 Annual Plan. They include encouraging investment and improving broadband and mobile coverage across the UK, supporting UK broadcasting and supporting consumers and industry through Brexit. Twenty-eight European Commission (Commission) Digital Single Market (DSM) proposals have been finalised, which promise to make significant changes to the UK communications landscape, and subject to longer-term changes to national legislation as a result of Brexit.

European and national law and standards currently govern the UK data protection framework and impose compliance obligations on organisations that process personal data. These rules apply broadly to, inter alia, the collection, use, storage and disclosure of personal data. In general, personal data is defined as information relating to an identified or identifiable natural person who can be identified directly or indirectly from that data (e.g., names, contact information, or special categories of personal data such as health data).

These laws and regulations have undergone substantial change as a result of the General Data Protection Regulation (GDPR), which came into force on 25 May 2018 across Europe, and the UK government’s implementing legislation – the Data Protection Act 2018 (DPA) – which came into force on 23 May 2018. The legal landscape in this sector has also been impacted by the Network and Information Security Directive (NISD) (adopted by the European Parliament in July 2016 and implemented in the UK by the Network and Information Systems Regulations 2018 (NIS Regulation), effective as of 10 May 2018), which is the first EU-wide legislation on cybersecurity. The GDPR and NISD introduce significant fines based on a percentage of global turnover, similar to the regime imposed for antitrust violations. In relation to Brexit implications, both the GDPR and NISD have been implemented into UK national law, as a result of which equivalent standards for data protection and cybersecurity have already been established in the UK and will continue to
apply post-Brexit (at least in the short and medium terms). However, at the time of writing it is unclear exactly what type of arrangement the EU and UK will reach regarding the UK’s data protection regime in the post-Brexit period.

II REGULATION

i The regulators and key legislation

Ofcom is the independent communications regulator in the UK. The Department for Digital, Culture, Media and Sport (DCMS) remains responsible for certain high-level policy, but most key policy initiatives are constructed and pursued by Ofcom. Ofcom has largely delegated its duties in respect of advertising regulation to the Advertising Standards Authority (ASA). The Committee of Advertising Practice is responsible for writing and updating the Non-broadcast Code and the Broadcast Committee of Advertising Practice is responsible for the Broadcast Code. On 1 November 2014, Ofcom renewed its 10-year contract with the ASA for broadcast advertising regulation until 2024.5

Ofcom’s principal statutory duty (pursuant to the Act) is to further the interests of citizens in relation to communications matters and to further the interests of consumers in relevant markets, where appropriate by promoting competition.6 This is enshrined in Ofcom’s three main objectives: ‘to promote competition and ensure that markets work effectively for consumers;7 to secure standards and improve quality; and to protect consumers from harm’. The government published a draft statement of strategic priorities for consultation in February 2019, upon which Ofcom’s priorities have been based. The post-consultation policy paper entitled Statement of Strategic Priorities for telecommunications, the management of radio spectrum, and postal services has since been published, in July 2019.

Ofcom’s priorities and major work areas for 2019 and 2020 are set out below:8

a improving broadband and mobile connectivity for people across the UK:

• ensuring the universality of broadband services by designating broadband universal service provider(s) (USPs) and setting out the conditions that will apply to them;
• promoting investment in fibre networks;
• helping to improve mobile coverage, particularly in rural areas;
• improving opportunities for spectrum sharing; and
• preparing for the launch of 5G mobile services;

---

6 Section 3(1) of the Act.
7 Ofcom has concurrent powers to apply competition law along with the primary UK competition law authority, the Competition and Markets Authority (CMA). Enhanced concurrency arrangements came into effect on 1 April 2014 with the objective of increasing the enforcement of competition law in the regulated sectors by strengthening cooperation between the CMA and sector regulators, including Ofcom, referred to as concurrency. The most recent Annual Report on concurrency was published by the CMA on 10 April 2019, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811431/ACR_PV2406.pdf.
delivering a fair deal for consumers and protecting people from unfair and harmful pricing practices:

- improving pricing for mobile handset and airtime contracts;
- considering differential pricing practices;
- end-of-contract and best tariff notifications;
- implementation of the European Electronic Communications Code, particularly in respect of switching mobile service providers; and
- ensuring consumer data is available on availability, speeds and usage of communications services;

c supporting UK broadcasting:

- reviewing public service broadcasting;
- supporting future public service broadcasting;
- reviewing the BBC’s news and current affairs output;
- considering material changes to BBC public service activities (e.g., the BBC’s iPlayer proposals); and
- considering any material changes to the BBC’s commercial activities;

d raising awareness of online harms:

- developing an in-depth understanding of specific harms;
- working with external partners to develop a rounded view of online harms and potential solutions; and
- actively contributing to the international discussion about online harms and media literacy;

e supporting consumers and industry through Brexit:

- ensuring preparation for a range of potential Brexit outcomes;
- providing independent technical advice to the government on aspects of any negotiations about the UK’s future relationship with the EU; and
- engaging with the industry to better understand the concerns and post-Brexit plans;

f enabling strong, secure networks:

- monitoring potential security risks and working closely with the government, National Cyber Security Centre and industry;
- implementing the Network and Information Systems Regulations, placing legal obligations on providers to protect UK critical services; and
- launching a version of a threat intelligence-led penetration testing scheme that assesses how well a company stands up to a concerted attack based on the techniques known to be used by cyber criminals and hostile nation states;

g increasing diversity and inclusion by publishing:

- the Diversity and Inclusion at Ofcom report;
- an Equal Pay and Gender-ethnicity Pay audit;
- annual reports on diversity and equality opportunities in TV and radio; and
- an annual report on the BBC;

h sustaining the universal postal service:

- carrying out a review of Royal Mail’s efficiency; and
- seeking to understand the needs of postal users better;

i continuing to innovate Ofcom’s approach to regulation:

- enabling better use of data analytics;
- collaborating to protect vulnerable people; and
• assessing Ofcom’s existing duties and programmatic work in light of the shift towards delivering communications services online.

Ofcom’s main statutory duties fall into six areas:

1. ensuring the UK has a wide range of electronic communications services;
2. ensuring optimal use is made of the radio spectrum;
3. ensuring a wide range of high-quality television and radio programmes are provided by a range of different organisations, appealing to a range of tastes and interests;
4. ensuring people are protected from harmful or offensive material, unfair treatment and invasion of privacy on television and radio;
5. ensuring the BBC is held to account on its compliance with appropriate content standards, its performance against its mission and public purposes, and the impact of its activities on fair and effective competition; and
6. ensuring the universal service obligation on postal services is secured in the UK.

Following its overarching review of the UK’s digital communications over the course of 2015 and 2016, Ofcom’s strategy has focused on six fundamental measures intended to facilitate the development of the UK communications market:

1. universal availability of fixed and mobile services;
2. a strategic shift to large-scale full-fibre deployment;
3. a step change in the quality of service;
4. significantly strengthening the independence of Openreach;
5. empowering and protecting consumers; and
6. simplifying and removing unnecessary regulation.

The next steps set out in phase two of the review were to implement the proposed measures through the usual mechanism of regular reviews of individual markets and likewise to implement specific dedicated projects. Specific dedicated projects that have been envisaged or undertaken include:

1. Ofcom working with the government to introduce the new universal right to broadband. This culminated in the introduction of legislation for a broadband Universal Service Obligation in March 2018, which came into force on 23 April 2018 and which Ofcom is responsible for implementing. The USO provides a legal right to request a broadband connection of at least 10Mbps download speed (discussed further in Section III.ii). Ofcom has designated BT and KCOM9 to provide universal broadband service connections in the UK, and has set a deadline of March 2020 for the relevant infrastructure to be in place;
2. Ofcom continuing to provide accurate, comparable, accessible and increasingly granular coverage information, published in its annual Connected Nations reports, and launching an interactive data portal for Ofcom’s cross-sector communications market data;
3. Ofcom using its power to require operators to improve mobile coverage, for example by including increasingly demanding licence conditions on population and geographic coverage for new spectrum releases, including in relation to 5G. Ofcom intends to release 5G spectrum bands over the course of 2019 and 2020;

9 KCOM is the designated provider for Hull area only; BT is the designated provider for the rest of the UK.
Ofcom working with communications providers to minimise potential disruption in the migration to voice-over-IP services and possible switch-off of the PSTN in the future, including a review of relevant regulation and consumer safeguards.

Ofcom working with BT and industry to make BT’s underground duct system more easily accessible to competitors. Ofcom implemented these changes through the Civil Infrastructure Directive and UK transposition legislation, which came into effect on 31 July 2016. Ofcom has also made specific proposals for improving access in its Wholesale Local Access Market Review, including implementing regulated access and pricing policies to support investment in access networks. Ofcom envisages implementing a new approach to the regulation of wholesale access to broadband networks by April 2021, to be in place for at least five years;

Ofcom setting tough minimum standards for Openreach in the business market with rigorous enforcement and fines for underperformance. Ofcom fined Openreach £42 million in March 2017 for breaching contracts with telecoms providers;

Ofcom extending minimum standards and introducing rules to incentivise Openreach to go beyond minimum standards and deliver better service. These rules were introduced in 2016, and have been consulted on throughout Ofcom’s Wholesale Local Access Market Review, which took place from March 2017 until June 2017. The results of this Review were published on 28 March 2018, as modified, with new measures resulting from this taking effect in April 2018. Ofcom is planning a further, single review of business and residential full-fibre markets to be undertaken by April 2021 and which will supersede previous separate reviews including the Wholesale Local Access Market Review;

Ofcom consulting on and implementing an automatic compensation scheme for consumers and small businesses; this came into effect in April 2019;

Ofcom developed detailed proposals on Openreach independence and discussed these proposals with the Commission in 2016. In response to Ofcom’s competition concerns, BT agreed in 2017 to Ofcom’s requirements to make Openreach a distinct company with its own staff, management and strategy, and a legal purpose to serve all of its customers equally, and Openreach become a legally separate entity in October 2018. Ofcom established the Open Reach Monitoring Unit in 2018 to support the ongoing assessment of Openreach: an interim report was published in November 2018 and a full annual compliance report was released in July 2019;

Ofcom consulting on proposals to streamline and update the General Conditions throughout 2016 and 2017, and set out its conclusions in statements published in September 2017, March 2018 and July 2018. All of the revised conditions came into force on 1 October 2018. Ofcom will start a review and revision of the General
Conditions in the third quarter of 2019 to reflect requirements under the new European Electronic Communications Code (to be implemented into national law by 21 December 2020);

Ofcom working with the government and Information Commissioner’s Office (ICO) to develop a regulatory framework and communications plan around online harms. An initial product of this work is a joint research report published by Ofcom and the ICO in September 2018 on internet users’ experience of online harms; and

Ofcom working closely with the government, the National Cyber Security Centre and industry to monitor cybersecurity risks and improve network resilience, including implementation of the NIS Regulations and operation of the TBEST penetration testing scheme as part of the wider Security and Resilience Assurance Scheme launched in February 2019.

In terms of other regulators, the Body of European Regulators for Electronic Communications (BEREC), formed after the adoption of Regulation (EC) 1211/2009,10 is now playing an increasingly significant role at a European level. BEREC replaced the European Regulators Group, and acts as an exclusive forum and vehicle for cooperation between NRAs and between NRAs and the Commission.

The prevailing regulatory regime in the UK is contained primarily in the Act, which entered into force on 25 July 2003. Broadcasting is regulated under a separate part of the Act in conjunction with the Broadcasting Acts of 1990 and 1996. Other domestic and European legislation also affects this area, including:

- the Wireless Telegraphy Act 2006;
- the Digital Economy Act 2010;
- the GDPR and the Data Protection Act 2018;
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011);
- European Regulation 2017/003 (e-Privacy Regulation), once it takes effect;
- the NISD and the NIS Regulation;
- the Freedom of Information Act 2000;
- the Enterprise Act 2002;
- the Copyright, Designs and Patents Act 1988;
- the Digital Economy Act 2017 (DEA) (although some sections of the DEA are in force, the remainder are subject to staggered commencement dates);
- the Competition Act 1998;
- the European Electronic Communications Code Directive,11 establishing the European Electronic Communications Code; and

The European data protection regime has undergone wholesale reform with the introduction of the GDPR, which became applicable on 25 May 2018, and the UK implementing

legislation, the Data Protection Act 2018, which came into effect on 23 May 2018. This legislation replaces the previous Data Protection Directive\textsuperscript{12} and the corresponding UK implementing legislation, the Data Protection Act 1998, and introduces more stringent standards and an enhanced enforcement regime.

In July 2013, the DCMS published a policy paper titled ‘Connectivity, content and consumers – Britain’s digital platform for growth’ (Strategy Paper)\textsuperscript{13}. In line with the government’s view that a large-scale overhaul of the existing legislation was unnecessary, the Strategy Paper focused on specific and incremental legislative changes to a number of areas, including the following:

\begin{itemize}
\item[a] a consumer rights bill introducing a new category of digital content in consumer law, together with a set of statutory rights for the quality standards that this content should meet and the remedies available to consumers when digital content does not meet these standards;
\item[b] changes to improve spectrum management and amendments to the Wireless Telegraphy Act 2006; and
\item[c] amending the Electronic Communications Code (ECC), in line with the new European Electronic Communications Code, to make it easier for communications companies to use land for broadband infrastructure.
\end{itemize}

Following on from the above, the Consumer Rights Act 2015 introduced rights in respect of the quality of digital content and digital services. The Act received royal assent on 26 March 2015 and came into force in stages; it is now fully in force. The main provisions of the Act, including those relating to goods, services and digital content, came into force on 1 October 2015.

In April 2018, the government announced in the Modernising Consumer Markets Green Paper\textsuperscript{14} that it would review the regulatory model for providing various consumer-facing services, including utilities, telecoms and financial services, with a particular focus on ensuring that consumers benefit from new technology while ensuring that personal data is protected. It simultaneously launched a call for evidence on the review of competition law. The consultation closed on 4 July 2018. Following this, the UK government appointed an expert panel to examine competition in the data economy and explore what steps were possible to ensure that new technology markets support healthy competition. The panel ran from September 2018 to March 2019 and culminated in a final report of recommendations to the government (the Furman Report)\textsuperscript{15}. The recommendations in the Furman Report included:

\begin{itemize}
\item[a] the establishment of a digital markets unit, with three functions: developing a code of competitive conduct with the participation of stakeholders, enabling greater personal data mobility and systems with open standards, and advancing data openness. This unit would have links to the Competition and Markets Authority (CMA) and Ofcom and a strong relationship with the Information Commissioner’s Office (ICO);
\end{itemize}

\textsuperscript{12} Directive 95/46/EC.
b a revision of merger assessment in digital markets. The revisions would entail the CMA taking more frequent, and firmer, action on mergers that could be detrimental to consumer welfare through reducing future levels of innovation and competition;
c updates to the CMA’s enforcement tools against anticompetitive conduct to protect and promote competition in the digital economy. The Report notes that existing tools have been used infrequently in a digital markets context, and that cases have moved slowly;
d the government, the CMA and the Centre for Data Ethics and Innovation continuing to monitor how use of machine learning algorithms and artificial intelligence evolves to ensure it does not lead to anticompetitive activity or consumer detriment, in particular to vulnerable consumers;
e the CMA conducting a market study into the digital advertising market encompassing the entire value chain, using its investigatory powers to examine whether competition is working effectively and whether consumer harms are arising. On 3 July 2019, the CMA launched a market study into online platforms and the digital advertising with the aim of assessing three broad potential sources of harm to consumers in connection with the market for digital advertising: to what extent online platforms have market power in user-facing markets, and what impact this has on consumers; whether consumers are able and willing to control how data about them is used and collected by online platforms; and whether competition in the digital advertising market may be distorted by any market power held by platforms. The consultation on the CMA’s statement of scope for this market study closed on 30 July 2019 and further details and responses are available on the CMA’s case page;¹⁶ and
f the government engaging internationally on the recommendations it chooses to adopt, encouraging closer cross-border cooperation between competition authorities in sharing best practice and developing a common approach to issues across international digital markets.

The DCMS issued its spectrum management strategy in March 2014, recognising the need for, among other things:
a a uniform system for the valuation of spectrum to set licence fees;
b the government to work with Ofcom to encourage efficient use of spectrum, in particular in the release of spectrum, transfer of spectrum and assignment of spectrum to new users;
c encouragement of innovation; and
d a strategy to address increased demands on spectrum that will evolve from the growth of the IoT, M2M communication and 5G.

The DCMS’s strategy was followed in April 2014 by Ofcom’s spectrum management strategy, discussed in more detail below.

In August 2014, the DCMS issued a consultation paper seeking input on the goals and policies set out in a July 2013 report entitled ‘Connectivity, content and consumers – Britain’s digital platform for growth’, which was explored further within a framework published in February 2014. The results of this consultation were used to develop the government’s digital communications infrastructure strategy, which was published on 18 March 2015. For the past few years, the government has made commitments in relation to broadband infrastructure, in particular superfast broadband, connectivity in rural areas and the delivery of mobile broadband connectivity. One step towards this objective came in the form of the DEA, which received royal assent in April 2017. This provided the statutory basis for the development of the new broadband USO (discussed above).

The DEA, among other things, reformed the ECC by introducing a range of measures to make it easier for network operators to deploy infrastructure (phone masts, exchanges, etc.) on public and private land. Ofcom was obliged to publish a new Code of Practice to accompany the proposed changes, to create a number of templates to be used by Code operators and landowners or occupiers, and to create standard terms that may be used by Code operators and landowners or occupiers when negotiating agreements to confer Code rights. Ofcom published final versions of these documents on 15 December 2017.

ii Regulated activities

Ofcom oversees and administers the licensing for a range of activities, including, broadly speaking, mobile telecommunications and wireless broadband, broadcast TV and radio, postal services, and the use of radio spectrum.

The Act replaced the system of individual licences with a general authorisation regime for the provision of ECNs and ECSs. Operators of ECNs and ECSs are able to provide networks or services to the public without the need for prior authorisation from Ofcom where they have complied with the general conditions of entitlement. A revised version of the general conditions came into force on 1 October 2018. As well as the general conditions, individual ECN and ECS operators may also be subject to further conditions specifically addressed to them. These fall into four main categories: universal service conditions, access-related conditions, privileged supplier conditions, and conditions imposed as a result of a finding of significant market power (SMP) of an ECN or ECS operator in a relevant economic market.

Use of radio spectrum requires a licence from Ofcom under the Wireless Telegraphy Act 2006 (subject to certain exemptions).

Television and radio broadcasting requires a licence from Ofcom under the Broadcasting Act 1990 or 1996. Providers of on-demand programme services have to notify Ofcom of their services in advance.

iii Ownership and market access restrictions

No foreign ownership restrictions apply to authorisations to provide telecommunications services, although the Act directs that the Secretary of State for DCMS may require Ofcom to suspend or restrict any provider’s entitlement in the interests of national security.

In the context of media regulation, although the Act and the Broadcasting Acts impose restrictions on the persons that may own or control broadcast licences, there are no longer any rules that prohibit those not established or resident in the EEA from holding broadcast licences.

In March 2017, the Secretary of State intervened in connection with media plurality when it asked Ofcom to review the anticipated acquisition by Twenty-First Century Fox, Inc (21st Century Fox) of 100 per cent of the shares in Sky plc (Sky), a British pay-TV operator. The Secretary of State’s stated potential concerns were twofold: whether there would be sufficient plurality of persons with control of the media enterprises and whether the parties would have genuine commitment to the attainment of standard objectives in relation to broadcasting. Ofcom published its report in June 2017 and found that the anticipated transaction raised potential public interest concerns relating to media plurality due to a risk of increased influence by members of the Murdoch Family Trust over the UK news agenda and political process, with its unique presence on radio, television, in print and online.20 Ofcom recommended a reference by the Secretary of State to the CMA.

In January 2018, the CMA provisionally found that 21st Century Fox’s anticipated acquisition was not in the public interest due to media plurality concerns, but not due to a lack of commitment to meeting broadcasting standards. The CMA sent its final report to the DCMS in May 2018, following which the Secretary of State accepted the CMA’s recommendation that the anticipated acquisition was not in the public interest due to media plurality concerns and that the most effective and proportionate remedy would be for the Sky News channel to be divested to a suitable third party.21 21st Century Fox then agreed to divest Sky News to the Walt Disney Company.22 However, Comcast has since outbid Disney for a majority interest in Sky. The takeover of Sky by Comcast was completed in October 2018.23

iv Transfers of control and assignments

For transactions that do not fall within EU merger control jurisdiction, the UK operates a merger regime in which the parties to a transaction can choose whether to notify a transaction prior to closing. The UK CMA monitors transactions prior to closing and has the power to

---

23 See https://www.ft.com/content/b402969a-cbd5-11e8-b276-b9069bde0956.
intervene in un-notified transactions prior to closing or up to four months from the closing of a transaction being publicised. Where the CMA intervenes in a closed transaction it is policy to impose a hold-separate order.24

The administrative body currently responsible for UK merger control is the CMA. The CMA consults Ofcom when considering transactions in the broadcast, telecommunications and newspaper publishing markets.25

The Secretary of State also retains powers under the Enterprise Act 2002 to intervene in certain merger cases, which include those that involve public interest considerations. In the context of media mergers, such considerations include the need to ensure sufficient plurality of persons with control of media enterprises serving UK audiences; the need for the availability throughout the UK of high-quality broadcasting calculated to appeal to a broad variety of tastes and interests; and the need for accurate presentation of news, plurality of views and free expression in newspaper mergers. Importantly, the Secretary of State is subject to the same four-month time limit to intervene in un-notified transactions as the CMA, as recently confirmed by the Competition Appeal Tribunal.26 In such cases, the Secretary of State may require Ofcom to report on a merger’s potential impact on the public interest as it relates to ensuring the sufficiency of plurality of persons with control of media enterprises (as was the case, for example, in relation to the recent attempted acquisition of Sky by 21st Century Fox discussed in Section II.iii). Ofcom is also under a duty to satisfy itself as to whether a proposed acquirer of a licence holder would be fit and proper to hold a broadcasting licence pursuant to Section 3(3) of each of the 1990 and 1996 Broadcasting Acts.27

Following the 2017 National Security and Infrastructure Investment Review Green Paper,28 amendments to the UK’s merger control regime for transactions in the defence and technology sectors came into force on 11 June 2018. The aim of the amendments is to provide greater powers for the Secretary of State to intervene in transactions on public interest grounds. Among other changes, under the new rules, the target turnover threshold has been lowered from £70 million to £1 million for transactions between parties operating in either the design and maintenance of aspects of computing hardware or the development of quantum technology.29

24 Note, however, that changes in control of certain radio communications and TV and radio broadcast licences arising as a result of mergers and acquisitions may in certain circumstances require the consent of Ofcom.
27 There is also the power to take appropriate measures nationally to protect the plurality of the media under Article 21(4) of the EU Merger Regulations (Regulation 139/2004/EC).
29 The CMA’s guidance to the changes is available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715167/guidance_on_changes_to_the_jurisdictional_thresholds_for_uk_merger_control.pdf. A recent example where the Secretary of State decided to intervene under the new rules on the basis that the interests of national security (one of the specified public interest considerations) are relevant is the proposed acquisition of Inmarsat plc by Connect.
DSM: e-commerce, online platforms, geo-blocking and telecoms

Introduction

On 6 May 2015, the Commission published a Communication on a DSM Strategy for Europe. This Strategy aims to make the EU’s single market fit for the digital age through three pillars: better online access for consumers and businesses across Europe; creating the right conditions and a level playing field for advanced digital networks and innovative services; and maximising the growth potential of the digital economy. The Strategy includes legislative proposals in a range of areas with a view to make cross-border e-commerce easier, end unjustified geo-blocking, reform the copyright regime and reduce burdens due to different VAT regimes. Twenty-eight of these proposals have been agreed or finalised by the European Parliament and the Council of the European Union, and an update on progress was provided in a DSM factsheet published by the Commission in July 2019.30 For instance, a regulation on cross-border portability of online content services has applied across the EU since 1 April 2018 and allows EU consumers to access their online content services while travelling within the EU (discussed further in Section V.ii). This can be seen as complementary to the data roaming rules of June 2017, which enable EU consumers to use their domestic mobile data allowance and rates when roaming in other Member States.

In May 2017, the Commission published its mid-term review on the implementation of the DSM, which identifies three main areas where further EU action is needed: the development of the European data economy to its full potential; the protection of Europe’s assets by tackling cybersecurity challenges; and the promotion of online platforms as responsible players in a fair internet ecosystem.31 The mid-term review also clearly emphasised the necessity to rapidly adopt the proposals for the Electronic Communications Code, which has since occurred in December 2018. As a direct response to the challenges identified in the mid-term review, the Commission announced in April 2018 that revisions are being made to Directive 2003/98/EC, which governs the use of public sector information. The aim is to tap into the huge resource of data that is currently held in the public sector, thought to be worth approximately €52 billion, and reuse it to help address a range of different societal problems such as healthcare, public transport and even artificial intelligence.32

E-commerce

On 10 May 2017, the Commission published a report on the e-commerce sector enquiry. One of the main points the Commission raised was that, with the growth of e-commerce, business practices have emerged that may raise competition concerns, such as pricing restrictions and online marketplace (platform) bans. The Commission noted that it is important to avoid diverging interpretations of the EU competition rules in e-commerce markets, which may in turn create obstacles for companies to the detriment of a DSM. One significant development has been the abolition of retail roaming charges throughout the EU, effective from 15 June 2017, as part of the ongoing focus on promoting cross-border e-commerce.


31 Available at eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496330315823&uri=CELEX:52017DC0228.
Since the roaming charges developments, the Commission’s focus for e-commerce reforms has been preventing unjustified geo-blocking (discussed in more detail below), as well as revised general consumer protection rules.

**Online platforms**

The Commission has emphasised the role of online platforms, with one million businesses already selling goods and services via online platforms and more than 50 per cent of SMEs that operate through online marketplaces selling cross-border. In May 2016, it published a communication that proposed ways to foster development of such platforms and identified two specific issues for further investigation: safeguarding a fair and innovation-friendly business environment; and ensuring that illegal content online is timely and effectively removed, with proper checks and balances, from online platforms. In its mid-term review, the Commission identified online platforms as one of three emerging challenges, and proposed the implementation of actions to tackle these challenges. The result, announced by the Commission on 26 April 2018, was a proposed suite of new standards on transparency and fairness in relation to online platforms, which were agreed by the Commission, Parliament and Council in February 2019 and adopted on 14 June 2019. The aim of these new rules is to create a fair, transparent and predictable business environment for smaller businesses when using online platforms. The new Regulation (Regulation on promoting fairness and transparency for business users of online intermediary services) includes measures seeking to reduce unfair trading practices, increase transparency, resolve disputes more effectively as well as establishing an Online Platform Observatory to monitor the impact and implementation of the new rules. The new Regulation will apply from 20 June 2020, and will be subject to a review within 18 months of that date.

**Geo-blocking**

On 27 February 2018, the EU adopted the Geo-blocking Regulation, which will apply from 3 December 2018. The Regulation prohibits unjustified geo-blocking, and other forms of discrimination, based on customers’ nationality, place of residence or place of establishment. The Regulation tackles the concern that geo-blocking potentially limits online shopping and cross-border trade, and leads to undesirable geographical market segmentation. Importantly, electronically supplied services offering copyright-protected content are excluded from the Regulation: territorial exclusivity is essential for the creative industries to monetise and exploit their content, and the Commission argues that facilitating access to audiovisual

---

services across borders is part of other initiatives under the DSM Strategy.\textsuperscript{38} For this reason, the Regulation does not affect online television, films, streamed sports, music, e-books or games. However, the Commission will evaluate the Regulation’s impact two years after its entry into force to assess the possibility of an extension of the new rules to online services related to non-audiovisual copyright-protected content.

**Telecoms**

The current European Commission telecoms and connectivity proposals include:

\begin{itemize}
  \item[a] recasting the Framework, Authorisation, Access and Universal Services Directives as one directive, the European Electronic Communications Code;
  \item[b] upgrading BEREC to a fully fledged EU agency;
  \item[c] a 5G Action Plan for the development and deployment of 5G networks in Europe; and
  \item[d] a WiFi4EU initiative to aid European villages and cities roll out free public Wi-Fi.
\end{itemize}

In December 2018, the Commission adopted the European Electronic Communications Code (the Code) and a revised remit for the Body of European Regulators for Electronic Communication (BEREC). The Commission implemented these changes as a step towards modernising and improving connectivity.

The Code aims to address and harmonise spectrum policy and regulation, including spectrum auction timing, across the single market in part to stimulate competition and investment in 5G networks. It also tries to address new technologies and services that are not clearly contemplated by current legislation. In the UK, the rules and timelines for the spectrum auctions were announced by Ofcom in July 2017. The results of the principal bidding stage were announced on 5 April 2018.\textsuperscript{39}

OTT services would be classified a sub-class of ECS and subject to regulations concerning security (including security audits) and interconnectivity (among end users and to emergency services). Other amendments regarding number allocation have been made to address potential competition issues with the expected advent of the IoT and M2M communication: national regulators would be allowed (but not required) to assign numbers to undertakings other than providers of ECNs and services. The Code moves away from universal service access requirements to legacy technologies (e.g., public payphones) and replaces them with a requirement to ensure end users have access to affordable, functional internet and voice communication services, as defined by reference to a dynamic basket of basic online services delivered via broadband. In addition, the Code contains additional consumer protections via proposed regulations requiring telecoms providers to provide contract summaries and improved comparison tools.

The regulatory role of BEREC has been enhanced with a view to improving regulatory consistency across the single market. For example, decisions on spectrum assignment are subject to a peer review process whereby BEREC issues an opinion on whether a decision should be amended or withdrawn to ensure consistent spectrum assignment. BEREC can also issue an opinion on any remedy proposed by an NRA in relation to maintaining the Code’s objectives. BEREC has also been granted legally binding powers, including a double-lock system in relation to any draft remedy proposed by an NRA. New rules on cheaper intra-EU


calls are also intended to cap the retail price of mobile or fixed calls from the customer’s home Member State to another EU Member State. There will also be a cap for intra-EU text messages. The new caps started to apply as early as 15 May 2019.

In terms of policy proposals, the 5G Action Plan proposes to bring uninterrupted 5G coverage to all major European urban areas and transportation corridors by 2025, with several interim deadlines relating to, inter alia, spectrum assignment and development of global 5G standards (2019). In December 2017, Urve Palo, Minister of Entrepreneurship and Information Technology, set out the deployment road map and detailed commitments, for example to transpose the Code into national law by mid-2020. The specifics of the 5G Action Plan, such as the development of 5G standards, are still evolving. There is limited guidance on funding for the 5G Action Plan, although the Code itself has stimulated to an extent such investment, and the Commission has launched the European Broadband Fund (combining private and public investments) to support network deployment throughout the EU. The Commission has also committed to exploring a proposal by a telecoms industry group to provide a venture-financing facility (jointly funded by public and private sources) for start-ups developing 5G technologies and applications.

The WiFi4EU initiative intends to assist local authorities to offer free Wi-Fi connections in parks, libraries and other public spaces by providing local authorities with small grants of up to €60,000 (from a total initial budget of €120 million) for equipment and installation costs. In May 2017, the European Parliament, Council and Commission reached a political agreement on the initiative and its funding, and as of May 2018, local communities have been able to apply for WiFi4EU vouchers to set up free public Wi-Fi networks. There have been two calls for members of the public to apply for funding in connection with WiFi4EU (in November 2018 and April 2019 respectively). To date a combined total of €93 million has been allocated to implement free Wi-Fi across the EU. It is intended that this will develop into a more harmonised telecoms regulatory regime, with an advanced 5G network that could be in place by 2025.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation
As previously noted, the Act is technology-neutral, and as such there is no specific regulatory regime for internet services. ISPs are also ECNs or ECSs depending on whether they operate their own transmission systems, and are entitled to provide services under the Act in compliance with the general conditions and, where applicable, specific conditions.

VoIP and VoB are specifically subject to a number of general authorisation conditions under the Act, such as those related to emergency call numbers.

In the context of the net neutrality debate, the Revised EU Framework adopted a range of internet traffic management provisions allowing NRAs such as Ofcom to adopt measures to ensure minimum quality levels for network transmission services, and to require ECN and ECS operators to provide information about the presence of any traffic-shaping processes operated by ISPs. These provisions were implemented into UK law.

Prior to the Regulation on Open Internet Access coming into force in 2016, the Broadband Stakeholders’ Group published a voluntary industry code of practice on traffic management transparency in March 2011. In July 2012, major ISPs published the Open Internet Code of Practice, which commits ISPs to providing full and open internet access. The latest Open Internet Code was published on 8 June 2016. The Code preserves the concept of
an open internet while clarifying the context in which some innovative services, which could become more prevalent as the IoT becomes a reality, could be provided alongside the open internet. The Code added three new commitments: ISPs promise open and full access to the net across their range of products; firms cannot market a subscription package as including internet access if certain kinds of legal content or services are barred; and members must not target and degrade content or applications offered by a specific rival.40 Notably, Everything Everywhere (EE) opted out of signing the Code.

From April 2016, the Regulation on Open Internet Access41 put in place EU-wide rules for net neutrality, and granted end users rights to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of such end user's or provider's location (Article 3(1)). The aim is that users will have access to online content that is not subject to discrimination or interference. Likewise, companies may not pay for prioritisation, so access to an SME’s website will not be unjustly slowed down to allow access for larger companies. The requirement that all internet traffic be treated equally is subject to exceptions to:

a comply with EU or national legislation related to the lawfulness of content or with criminal law;

b preserve the security and integrity of the network such as to combat viruses;

c minimise network congestion that is temporary or exceptional; and

d filter spam (i.e., to filter unsolicited communications and allow parents to set up parental filters).

In terms of the latter, such measures need to be transparent, non-discriminatory and proportionate, and must not be maintained for longer than is necessary. Likewise, providers of internet access services must publish information on traffic-management measures in end user contracts, along with details on the privacy of end users and the protection of their personal data. Notably, NRAs are required to monitor and enforce the open internet rules, although it is for Member States to lay down rules on the penalties applicable for infringements of the net neutrality provisions. On 30 August 2016, BEREC published guidelines42 for NRAs on the implementation of net neutrality under the Regulation on Open Internet Access, in particular covering obligations to monitor closely and ensure compliance with the EU net neutrality rules to ensure equal treatment of traffic in the provision of internet access services and related end user rights. Ofcom published a statement on its approach to assessing compliance with the Regulation on Open Internet Access in May 2019.43 Ofcom’s report focuses on two primary areas: the practice of ‘zero-rating’ data traffic, and traffic management practices, and also concludes Ofcom’s initial enforcement programme started in December 2017 (though Ofcom will continue to monitor compliance with the Regulation on an ongoing basis).

---

41 Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN.
Universal service

Universal service is provided under the Act by way of the Universal Service Order. Effective from April 2018, the Secretary of State published an order for a minimum affordable broadband connection to be available throughout the UK providing, inter alia, a download sync speed of at least 10Mbps and the capability to allow data usage of at least 100GB per month. The Order in the UK covers ECNs and ECSs and activities in connection with these services. Ofcom designated BT and KCOM as universal service providers in the geographical areas they cover; in June 2019, Ofcom published a statement setting conditions for the delivery of Universal Service Order connections and services by the universal service providers. Consumers and businesses will be able to request connections from 20 March 2020.

In June 2015, Ofcom published a report setting out its assessment and recommendations on the provision and availability of communications services for SMEs in the UK. Ofcom found that the availability of superfast broadband to SMEs is significantly lower than to residential premises. In its annual review for 2017 to 2018, Ofcom noted that it was key to continue to help SMEs engage in the communications market, and in 2018 it identified a lack of ICT specialism within SMEs and adequate assistance from providers as contributing factors to this lack of engagement.

Access and interconnection are regulated in the UK by EU competition law and specific provisions in the Act aimed at increasing competition. The General Conditions require all providers of public ECNs to negotiate interconnection with other providers of public ECNs. Specific access conditions may also be imposed on operators with SMP. Although prices charged to end users are not regulated, Ofcom may regulate wholesale rates charged by certain operators to alternative operators for network access. This is the case, inter alia, for wholesale fixed termination rates, wholesale mobile call termination rates, wholesale broadband access rates, local loop unbundling and wholesale line rental services.

Ofcom imposed specific conditions on BT and KCOM in certain areas where they enjoy SMP so as to allow alternative operators to compete in the retail broadband market. These include an obligation to provide general and non-discriminatory network access to BT and KCOM’s wholesale broadband products to alternative operators on reasonable request; an obligation to maintain separate accounts between services to alternative operators and its own retail division as well as other related transparency obligations; and a charge control on BT to ensure that charges for its broadband wholesale products are based on the costs of provision. Network access obligations included virtual access to new fibre lines laid by BT (through its access service division, Openreach), allowing alternative operators to combine their own electronics with physical infrastructure rented from BT. Furthermore, in June 2015, Ofcom proposed a charge control on the wholesale prices BT charges for products using leased telecoms lines, which provide vital high-speed links for businesses and providers of superfast broadband.
broadband and mobile services. In 2016, Ofcom also stated that Openreach must become more independent from BT, and proposed that Openreach become a distinct company with its own board and accountable executives. Likewise, in February 2016, Ofcom committed to making it easier for telecoms providers to invest in advanced, competing infrastructure by improving access to Openreach's network of telegraph poles and ducts, allowing competitors to connect their own fibre-optic cables directly to homes and businesses.

Ofcom's aim to promote the restructuring of BT and Openreach came to fruition in March 2017, when BT agreed that Openreach should become a distinct company with its own staff, management, strategy and legal purpose. This separation will likely take some time to be fully reflected in the market. Indeed, Ofcom noted in April 2018 that many SMEs still perceive BT as having specialist access to the Openreach network for installation and fault-finding, which deters switching between providers. However, significant progress has occurred already.

iii Restrictions on the provision of service
The Digital Economy Act 2010 (DEA 2010) includes provisions that were aimed at tackling online copyright infringement as a result of file sharing. It empowers the Secretary of State to impose obligations on ISPs to limit the internet access of subscribers who engage in online copyright infringement. Under the DEA 2010, Ofcom proposed a code of practice governing the initial obligations on ISPs. A second draft was published in June 2012. However, this version, and legislation on cost sharing in relation to the new obligations on ISPs, have not been finalised, and it is unclear whether they will ever come into force. Instead, the government has looked to industry to develop voluntary measures. In July 2014, the DCMS announced a scheme, Creative Content UK, spearheaded by ISPs and media industry leaders and supported by a government contribution of £3.5 million, to raise awareness of copyright infringement and warn internet users whose accounts are used to illegally access and share copyright material. The subscriber alert programme, which was initially known as the Voluntary Copyright Alert Programme (VCAP), evolved to encompass the Get it Right from a Genuine Site campaign launched in January 2017.

On 28 March 2018, the government launched the Creative Industries Sector Deal, which includes various specific commitments of interest concerning the tackling of online infringement of copyright. More than £150 million will be jointly invested by the government and industry to assist the UK’s cultural and creative businesses thrive in the digital age. As part of the deal, £2 million is being committed to extend the Get it Right from a Genuine Site campaign. On 15 August 2019, Get it Right from a Genuine Site launched an awareness-raising video on its YouTube channel, aimed at encouraging consumers to take time to identify and access genuine and licensed sources of content.

Among the provisions of the DEA is an increased maximum penalty for online copyright infringement of 10 years.

The availability of defences for online intermediaries in respect of unlawful content is governed primarily at a European level by the E-Commerce Directive,\(^53\) as implemented into UK law by the Electronic Commerce (EC Directive) Regulations 2002 and applicable case law. The Directive sets out defences for intermediary information society service providers.

**iv Security**

Privacy and consumer protection overview

In the UK, consumers’ personal data is primarily protected by the GDPR and DPA; the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (ePrivacy UK Regulations), which implement the EU Directive on Privacy and Electronic Communication,\(^54\) as amended by the ePrivacy Directive,\(^55\) and the NISD and NIS Regulation. The GDPR has significantly changed the current UK – and broader European – data protection framework. In line with the Commission’s DSM Strategy and the reforms brought in by the GDPR, the ePrivacy Directive is also undergoing reform. In 2017, the Commission proposed a draft ePrivacy Regulation (Draft ePrivacy Regulation),\(^56\) which is currently partway through the European legislative review process. The Draft ePrivacy Regulation is expected to be agreed and adopted in late 2019 or early 2020, and therefore to come into force in 2020 or 2021 following a minimum transition period of one year.

Data protection

The GDPR and DPA impose strict controls on the use or ‘processing’ (including disclosure) of personal data, including:

\(a\) providing specific conditions that must be met to ensure personal data is processed fairly, lawfully and in a transparent manner, such as that the individual has consented or that the processing is necessary for the purposes of fulfilling a contract;

\(b\) the requirement that data can generally only be processed for the purpose for which it was obtained and for no longer than is necessary, must be kept accurate and up to date, and must not be excessive;

\(c\) the requirement that data be kept secure (i.e., be protected against unlawful processing and accidental loss, destruction or damage);

\(d\) the restriction that data cannot be transferred to countries outside the EEA unless certain conditions are met, such as with the EU–US Privacy Shield (see ‘Litigation and EU–US transfers of personal data’ for more details) or signing the European Commission-approved Standard Contractual Clauses for personal data export; and

\(e\) personal data must be processed in accordance with the rights of the data subject under the GDPR, including that individuals have a right to access the personal data held about them, and a right in certain circumstances to have inaccurate personal data rectified or destroyed, among various other rights.

\(^53\) Directive 2000/31/EC.
\(^54\) Directive 2002/58/EC.
\(^55\) Directive 2009/136/EC.
\(^56\) Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.
As noted above, the GDPR has significantly changed the current UK – and broader European – data protection framework. The key changes under the GDPR include:

- **a** the implementation of the new rules as a regulation, rather than a directive, such that it is directly applicable in every Member State (though Member States are permitted certain derogations in a number of areas);
- **b** the removal of the requirement to notify or register data processing activities with national regulators; however, controllers and processors will need to keep their own record of processing which is disclosable to national regulators;
- **c** an expanded extraterritorial effect, resulting in the regulation applying not only to organisations established within the EEA, but also to organisations established outside the EEA but offering goods or services to, or monitoring the behaviour of, individuals in the EEA. Such non-EEA organisations are required to appoint a legal representative within the EEA, to enable national regulators to effectively communicate with, and take enforcement action against, those organisations without an EEA presence;
- **d** a tightening of the requirements for valid consent, with the effect that consent will only be deemed to be valid if it is freely given, specific, informed and unambiguous;
- **e** a stricter approach to the export of data outside the EEA, resulting from the general standards of data protection being raised throughout the Regulation as a whole;
- **f** the introduction of mandatory data breach notification requirements (including notification to both national regulators and, in certain circumstances, to data subjects affected by a breach). On the occurrence of a breach that is likely to result in harm to individuals, organisations must now inform the ICO without undue delay and, where feasible, not later than 72 hours after becoming aware of a data breach;
- **g** a right to data portability that will require the data controller to provide information to a data subject in a machine-readable format, in certain circumstances, so that it may be transferred to another controller;
- **h** maximum fines of the higher of up to €20 million or 4 per cent of an organisation’s annual global turnover for breaches. The GDPR relies on the European antitrust concept of ‘undertaking’ for the purposes of calculating fines, which encompasses wider corporate groups rather than looking solely at specific legal entities;
- **i** certain categories of online identifiers such as internet cookies and IP addresses may be classified as personal data; and
- **j** new definitions termed genetic data and biometric data, which include data relating to characteristics obtained during foetal development and data that allows the unique identification of a person to be confirmed through facial images or dactyloscopic data – now categorised as special categories of personal data (i.e., sensitive personal data).

---

57 In Patrick Breyer v. Bundesrepublik Deutschland (C-582/14), the CJEU ruled in October 2016 that where a website operator holds IP addresses and has ‘the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person’, then these will be classified as personal data.
The GDPR permits certain derogations by Member States, and the DPA seeks to provide for these accordingly to accommodate various existing UK statutes. For instance:

- it includes exemptions for journalists, research organisations, financial services firms (for anti-money laundering purposes) and employers (to process special categories of personal data and criminal conviction data without consent to comply with employment law obligations);
- certain actions (with some exceptions for actions necessary for preventing crime, etc.) relating to data will be criminal offences (subject to a fine), for example obtaining, procuring, retaining or selling data against a controller’s wishes (even where lawfully obtained); intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data (or knowingly processing such data); and altering records with the intent to prevent disclosure following a subject access request; and
- a parent’s or guardian’s consent will be required to process the personal data of a child who is under 13 years old (the GDPR permits Member States to set this age between 13 and 16 years old).

**Litigation and EU–US transfers of personal data**

There are several valid legal bases for the transfer of personal data from the EU to countries outside the EU, of which two are subject to ongoing litigation: the Privacy Shield (successor to the Safe Harbor) and standard contractual clauses (also known as model clauses).

Under the historic Safe Harbor agreement, if a US recipient of personal data was self-certified under the US Safe Harbor regime, data transfers could be made to that recipient in the US, notwithstanding the general prohibition on transfer under the European data protection legislation in place at that time, because such a recipient was deemed to have adequate protection in place. The Safe Harbor regime was challenged in *Schrems v. Data Protection Commissioner*. This case was brought by privacy activist Max Schrems, who argued that the EU–US Safe Harbor agreement did not provide adequate security for EU citizens in light of the revelations exposed by Edward Snowden about PRISM and United States National Security Agency surveillance programmes. The CJEU invalidated the legal basis for the Safe Harbor Framework on 6 October 2015 with the immediate effect that the agreement was no longer considered to provide adequate protection under the eighth data protection principle.

Following the decision in *Schrems v. Data Protection Commissioner*, the Commission and the US government entered into lengthy negotiations as to a new means of EU–US data transfers. The new EU–US Privacy Shield came into effect on 1 August 2016 following approvals by the Commission and EU Member States. Under the new Privacy Shield, US organisations commit to seven privacy principles to ensure that adequate protections are in place: the notice principle, the data integrity and purpose limitation principle, the choice principle, the security principle, the access principle, the recourse, enforcement and liability principle, and the accountability for onward transfer principle (Principles). To join the Privacy Shield, an organisation must publicly commit to and implement the Principles through a self-certification process, be subject to the authority of US law by the relevant enforcement authority and publicly disclose its privacy policy.58

---

58 Available at www.privacyshield.gov/welcome.
The most significant changes from the Safe Harbor framework to the Privacy Shield include the following:

a individuals affected by non-compliance with the Principles can seek redress (from the organisation itself, from an independent dispute resolution body and from the national DPA) and non-compliance can be enforced by various bodies (the Federal Trade Commission (FTC), a newly created privacy shield panel and judicial redress);

b there are tighter controls on transfers of personal data;

c annual joint reviews by the Commission, the FTC and the Department of Commerce on whether the Privacy Shield meets the adequacy finding that entitles companies to transfer personal data overseas legally; and

d written assurances by the US government that any access to personal data by public authorities will be subject to clear limitations, safeguards and oversight mechanisms.

In April 2017, the European Parliament passed a non-legislative resolution stating that the Commission should review the Privacy Shield to ensure it does not undermine the EU Charter on Fundamental Rights and the GDPR. In September 2017, the first joint review of the Privacy Shield took place between the EU and US. In a report published following the review, the Commission concluded that the Privacy Shield continues to ensure an adequate level of protection for personal data, but that there is room for improvement. The report sets out a number of recommendations to the US authorities on how to improve the functioning of the Privacy Shield, including, for example, that the Department of Commerce should proactively search for and investigate false claims of participation in the Privacy Shield, conduct regular compliance checks and swiftly appoint a Privacy Shield Ombudsman, in addition to increasing its cooperation with the Commission on relevant legal developments in the US. The Article 29 Working Party (which has now been replaced by the European Data Protection Board) also issued a report on the joint review in November 2017 that highlighted commercial issues and issues relating to access by US public authorities to data transferred to the US under the Privacy Shield. The report demands that an action plan be set up immediately (or at latest at the second joint review), and threatens to bring claims regarding the Privacy Shield adequacy decision before EU national courts if the issues are not addressed by the time of the second joint review.

In the wake of the revelation that Facebook had improperly shared the data of approximately 2.7 million European citizens with political consultancy Cambridge Analytica, despite the fact that both entities are signatories to the Privacy Shield, the European Parliament issued a resolution on 5 July 2018. The resolution notes the findings of both the Commission report and the Article 29 Working Party report, and takes the view that the current Privacy Shield arrangement does not provide an adequate level of protection. The resolution stated that, unless the US was fully compliant by 1 September 2018, the European Commission should suspend the Privacy Shield until the US authorities comply with its terms, though the Commission did not ultimately act on that resolution. The European Parliament renewed its

---

call to suspend the Privacy Shield via a further resolution issued in October 2018, during which time the Commission, EU supervisory authorities and the US government conducted their second annual review of the Privacy Shield. Following that second annual review, the Commission again concluded that the Privacy Shield regime does still provide an adequate level of protection for European personal data, though the Commission also called for a number of improvements including the appointment of a permanent US ombudsperson. The Privacy Shield is also under scrutiny from privacy campaigners who have brought claims before the General Court (the lower court of the CJEU) contesting the Commission’s adequacy finding for the Privacy Shield on the grounds that it still does not provide a level of data protection equivalent to the level required by European data protection law.

In May 2016, Max Schrems filed a complaint with the Irish Data Protection Commissioner concerning the legal status of data transfers under Facebook’s standard contractual clauses. The Irish High Court referred the case to the CJEU to determine the legal status of the use of standard contractual clauses to transfer personal data outside the EU. The CJEU heard the reference for a preliminary ruling on 9 July 2019 (the Schrems II case), not only in relation to the validity of the standard contractual clauses, but also on the legal status of the Privacy Shield. The Advocate General is expected to deliver his non-binding opinion on 12 December 2019, with the court’s decision following between three to six months later, possibly earlier.

ePrivacy Regulation

The Draft ePrivacy Regulation is set to replace the existing ePrivacy Directive, and to amend the Directive’s current controls on unsolicited direct marketing, restrictions on the use of cookies, and rules on the use of traffic and location data. The intent with the ePrivacy Regulation is to complement the GDPR, and establish a modern, comprehensive and technologically neutral framework for electronic communications.

In relation to cookies and similar tracking technologies, the ePrivacy Directive, and ePrivacy UK Regulations prescribe that the consent of users of the relevant terminal equipment for the placement of cookies is required, unless a cookie is strictly necessary to provide an online service requested by a user (such as online shopping basket functionality, session cookies for managing security tokens throughout the site, multimedia flash cookies enabling media playback or load-balancing session cookies).

The GDPR introduces a higher level of consent, stating that consent should be a clear affirmative act establishing a freely given, informed and unambiguous indication of the data subject’s agreement to the processing of personal data. Silence or inactivity does not constitute consent, and consent needs to be obtained for each processing purpose. Further, the data subject must have the right to withdraw consent at any time. In July 2019, the

---

65 General Data Protection Regulation: Recitals 26, 30 and 32.
66 General Data Protection Regulation: Article 7(3).
ICO updated its guidance on cookies, to clarify the interplay between the GDPR, DPA and ePrivacy UK Regulations and the standard of consent required for cookies. The ICO’s guidance confirms that consents for cookies should meet the GDPR standard for consent (i.e., consent mechanisms must seek clear, unbundled, express acceptance for each category of cookies (other than those that are strictly necessary to provide the online service; this is narrowly interpreted)). This means that a number of common market practices in this area, including the use of banners that do not interrupt a user’s interaction with a website (rather than those that provide notice and infer consent from continued use, for example) or that rely on implied consent (i.e., consent obtained by means of a pre-ticked opt-in box or an opt-out tick box) will need to be revised to meet the GDPR’s consent standards this approach. Other than functional, strictly necessary cookies, no cookies should be applied before such consent has been sought. Further, such consent should be sought on an unbundled basis (i.e., setting out, and obtaining consent for, each purpose for which cookies are used).

Individual data subjects have the right under the GDPR to notify a data controller to cease or not to begin processing their personal data for the purposes of direct marketing. Under the ePrivacy UK Regulations, an organisation must obtain prior consent before sending a marketing message by automated call, fax, email, SMS text message, video message or picture message to an individual subscriber. There is a limited exemption for marketing by electronic mail (both email and SMS) that allows businesses to send electronic mail to existing customers provided that they are marketing their own goods or services, or goods and services that are similar to those that were being purchased when the contact information was provided; and the customer is given a simple opportunity to opt out free of charge at the time the details were initially collected and in all subsequent messages.

Under the ePrivacy UK Regulations, location data (any data that identifies the geographical location of a person using a mobile device) can be used to provide value-added services (e.g., advertising) only if the user cannot be identified from the data or the customer has given prior consent. To give consent, the user must be aware of the types of location data that will be processed, the purposes and duration of the processing of that data, and whether the data will be transmitted to a third party to provide the value-added service.

The Draft ePrivacy Regulation (which is subject to further changes) aims to improve on the existing ePrivacy Directive in several ways, including:

a expanding the scope of ePrivacy laws to include OTT providers that provide services functionally equivalent to traditional telecoms providers, and apply to organisations worldwide as long as they are providing services to end users in the EU;

b reviewing the rules on the use of cookies and other tracking technologies to establish when consent should be required, and whether the standard of consent should be equivalent to that in the GDPR (e.g., it has been proposed that consent would not be necessary for cookies used for the purposes of analytics);

c tightening rules in relation to direct marketing (including business-to-business marketing);

d restricting use of content and metadata by communications providers. However, the scope of these restrictions is hotly debated, and one of the key topics responsible for the delay in the agreement of the proposed regulation text;

alignment of sanctions to the GDPR: for example, breach could bring liability of up to €20 million or four per cent of annual worldwide turnover; and

unifying the ePrivacy Regulation’s enforcement under GDPR enforcement bodies.

While the Commission’s original intention was for the ePrivacy Regulation to come into force simultaneously with the GDPR in May 2018, the draft has been subject to intense scrutiny and debate and remains under review through the European legislative process. At the time of writing, the next step in this process is the release of the Council’s final position on the regulation. Once the Council’s position is published, the ongoing trialogue process between the Parliament, Council and Commission will continue in order to agree the final wording of the regulation. According to the most recent drafts (the latest Council proposal was released on 26 July 2019), the ePrivacy Regulation is expected to come into force two years after its finalisation and publication date. Given the criticism of the proposal, companies should be prepared to see further changes to the draft before its passage, even at these later stages of the process, and the development of this law should be tracked to ensure ongoing compliance.

**Enforcement**

The ICO is responsible for the enforcement of the GDPR and DPA, the ePrivacy Directive and UK ePrivacy Regulations, the IPA, the NISD and NIS Regulations (NIS enforcement is discussed in more detail below), as well as the Freedom of Information Act 2000 (which provides individuals with the ability to request disclosure of information held by public authorities).

The ICO is increasingly focusing on enforcement generally, and on the use of monetary penalties in particular (under the GDPR, penalties of up to a maximum of 4 per cent of global annual turnover or €20 million, whichever is the higher, may be applied, and equivalent penalties are contemplated in the latest draft ePrivacy Regulation).

According to the ICO’s Annual Report for 2018 and 2019, 2018–2019 was a record-breaking year for monetary penalties in relation to data protection breaches, and also saw the first proposed fines under the GDPR and DPA. The majority of the ICO’s actions in the past year proceeded under the Data Protection Act 1998, rather than the DPA, due to the time taken to conduct and conclude the relevant investigations. The ICO issued 22 monetary penalty notices under the DPA 1998 in 2018–19 Report period, imposing fines totally just over £3 million. In two of these cases, the ICO imposed the maximum available financial sanction under the DPA 1998 (£500,000); these fines represent the highest data protection fines imposed by the ICO at the time of writing. The first of these fines was served on Facebook in July 2018 for failing to safeguard the personal data of millions of users and for failing to be transparent with those users about how their data was in turn being harvested by third parties, including by political consulting firm Cambridge Analytica. The second of these fines was imposed on Equifax Ltd in September 2018 for failing to protect the personal data of up to 15 million UK individuals during a cyberattack which compromised the company’s US systems.

In parallel with the ongoing conclusion of legacy DPA 1998 investigations, the ICO has more recently started to take action under the DPA, though no monetary penalties have been imposed at the time of writing. The ICO has, however, announced its intention to

---

impose two significant fines under the GDPR/DPA (these investigations are ongoing and the final level of fines imposed is not expected to be known until later in 2019). On 8 July, the ICO announced a notice of intent to fine British Airways £183.39 million under the GDPR in relation to a cyberattack and resulting data breach, impacting approximately 500,000 customers. This proposed fine is the largest to date under the GDPR. Then on 9 July 2019, the ICO announced a notice of intent to fine Marriott International £99.2 million for GDPR infringements stemming from a data breach at Starwood, which Marriott acquired in 2016. These latest actions from the ICO are part of a European-wide trend of data protection supervisory authorities starting to utilise their increased powers under the GDPR to impose significant fines, and indicating a sea change in the level of fines organisations can expect for data protection failings.

While the level of monetary penalties for data protection breaches is expected to increase dramatically compared with previous years, the most common grounds for fines and enforcement action remain the loss of data, other major data security breaches and, to a lesser extent, automated marketing calls and other complaints under the ePrivacy UK Regulations. In relation to the latter, the ICO received 138,368 complaints under the ePrivacy UK Regulations in 2018–2019 and issued 23 monetary penalty notices totalling just over £2 million in fines. This represents an increase in the number of complaints received compared to 2017–2018, but a decrease in the number of monetary penalties issued and the total level of fines imposed (in 2017–2018, the ICO issued 26 penalties under the ePrivacy UK Regulations, totalling £3.28 million in fines for that period). The majority of fines imposed under the ePrivacy UK Regulations relate to automated marketing calls.

In May 2017, the ICO issued the highest-ever nuisance calls fine of £400,000 to Keurboom Communication Ltd, which was responsible for 99.5 million nuisance calls. In January 2018, Barrington Claims Ltd was fined £250,000 for making automated marketing calls to individuals whom it could not prove had consented to receiving such calls. Finally, Tax Returned Limited was fined £200,000 in December 2018 for sending out millions of unsolicited marketing text messages.

**Data breach notification**

The GDPR introduces a new personal data breach notification obligation on data controllers requiring notification to the supervisory authorities without undue delay and not later than 72 hours after becoming aware of a breach, unless the data security breach is unlikely to result in a risk to the rights and freedoms of a data subject. If a personal data breach results in a high risk to the rights and freedoms of a natural person, a data controller must inform the natural person of the data breach without undue delay. The GDPR also requires a data processor to notify a data controller if it becomes aware of a personal data breach. An infringement of these provisions can lead to an administrative fine up to €10 million or, in the case of an undertaking, up to two per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher. As a result of this strengthening of the requirements

---

70 Available at https://ico.org.uk/action-weve-taken/enforcement/barrington-claims-ltd/.
71 Available at https://ico.org.uk/action-weve-taken/enforcement/tax-returned-limited-mpn/.
72 General Data Protection Regulation: Articles 33 and 34.
73 General Data Protection Regulation: Article 83(4)(a).
to report personal data breaches, the ICO has seen a significant increase in the number of personal data breaches reported to it: up from 3,311 notifications in 2017–2018 to 13,840 notifications in 2018–2019.\footnote{Available at https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.} The ICO reports that in 82 per cent of those reported cases, the relevant organisation had taken adequate steps to address the breach and no further action was required by the ICO. In the vast majority of the remaining cases, the ICO required the organisation to take further action but did not take enforcement or formal action against the organisation: enforcement action (e.g., monetary penalty or imposition of a mandatory improvement plan) was taken in less than 1 per cent of reported breach cases.\footnote{Available at https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.}

Under the ePrivacy UK Regulations, providers of public ECSs (mainly telecom providers and ISPs) are required to inform the ICO within 24 hours of a personal data security breach and, where that breach is likely to adversely affect the personal data or privacy of a customer, that customer must also be promptly notified. The Draft ePrivacy Regulations intend to align this deadline with the time period set out under the GDPR (72 hours) for consistency. This should be kept under review as the Draft ePrivacy Regulation is finalised.

In addition, organisations to which the NIS Regulations apply will have to comply with its notification requirements, as set out below.

**Data retention, interception and disclosure of communications data**

The legislation in this area has been the subject of much change and controversy over the past few years. The powers of government authorities (and, in a more limited capacity, private organisations) to intercept communications, acquire communications data and interfere with communications equipment was previously regulated by a patchwork of legislation, including the Regulation of Investigatory Powers Act 2000 (RIPA), and, until 2016, the Data Retention and Investigatory Powers Act 2014 (DRIPA). The Investigatory Powers Act 2016 (IPA) overhauls, and in some cases extends, the scope of RIPA. It has largely, but not yet entirely, amended or repealed RIPA.

On 8 April 2014, the CJEU held in *Digital Rights Ireland*\footnote{Digital Rights Ireland and Seitlinger and Others, joined cases C-293/12 and 594/12, 8 April 2014.} that the Data Retention Directive\footnote{Directive 2006/24/EC.} was invalid as it violated an individual’s right to privacy and was disproportionate in its aims. Under the Data Retention Directive, public communications providers (e.g., providers of fixed-network telephony, mobile telephony and internet access, internet email or internet telephony) had to retain traffic, subscriber and, where relevant, location data (but excluding content data) for a period of 12 months.\footnote{Judgment in joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others.} The declaration of invalidity meant that the UK’s implementing subordinate legislation, the Data Retention (EC Directive) Regulations 2009, no longer had a basis in primary law and was itself vulnerable to a finding of illegality. The government decided to reintroduce data retention laws as primary legislation by passing DRIPA. In this regard, the UK stood in stark contrast to the rest of Europe, where Germany, the Czech Republic, Romania, Austria, Cyprus, Belgium, Ireland and Bulgaria had already deemed similar provisions unlawful.

DRIPA came into force on 17 July 2014 (with a sunset clause forcing automatic expiry of its provisions on 31 December 2016), and addressed two key issues: the obligation to retain communications data by communications providers and the extraterritorial expansion
of powers under RIPA.79 DRIPA also clarified that interception capability notices under RIPA may be issued to telecommunications providers outside the UK in relation to conduct outside the UK.

Following its passage into law, a legal challenge was mounted questioning the legality of DRIPA. In July 2015, the High Court declared DRIPA’s data retention provisions to be incompatible with EU law on the basis that they interfered with Articles 7 and 8 of the EU Charter of Fundamental Rights (the public’s rights to respect for private life and communications and to the protection of personal data).80 In November 2015, the Court of Appeal referred the case to the CJEU; the CJEU held on 21 December 2016 that the ePrivacy Directive and the Charter of Fundamental Rights preclude laws that require a general and indiscriminate retention of data. However, laws that place targeted data retention obligations on service providers for the purpose of fighting serious crime are permitted provided that the safeguards protecting Article 7 and 8 rights are maintained (as specified in Digital Rights Ireland). The CJEU held that national data retention laws fall within the scope of the ePrivacy Directive.

The CJEU referred the case back to the UK Court of Appeal, which delivered its final judgment on 30 January 2018.81 The Court of Appeal agreed that the DRIPA data retention provisions were incompatible with EU law. It declined to rule on various other issues that had been raised by the parties given the ongoing litigation relating to the IPA by civil rights groups, as described below.

Although DRIPA would itself have expired in accordance with its sunset clause, its spirit survives in the IPA, which received royal assent on 29 November 2016, just in time before DRIPA’s scheduled expiry on 31 December 2016. The IPA is similar to RIPA in various respects. For example, like RIPA, the IPA imposes a general prohibition on the interception of communications unless the interceptor has lawful authority to carry out the interception, such as where a warrant has been issued by the Secretary of State (interception warrant). However, the IPA provides a new legal framework to govern the use and oversight of investigatory powers of the executive branch. Among other things, it:

a includes new powers for UK intelligence agencies and law enforcement to carry out targeted interception of communications, bulk collection of communications data and bulk interception of communications;

b introduces an Investigatory Powers Commission (IPC) to oversee the use of all investigatory powers, alongside oversight provided by the Intelligence and Security Committee of Parliament and the Investigatory Powers Tribunal;

c requires a judge serving on the IPC to review warrants authorised by the Secretary of State for accessing the content of communications and equipment interference before they come into force (commonly referred to as a double lock feature);

d widens the categories of telecommunications operators (TOs) that can be subject to most powers by including private as well as public operators;

e includes the power to require TOs to retain UK internet users’ data, including internet connection records, for up to one year (although it remains to be seen how such powers may be amended following the court rulings described below);

80 R (Davis & Watson) v. Secretary of State for Home Department [2015] EWHC 2092.
permits police, intelligence officers and other government department managers to see internet connection records as part of a targeted and filtered investigation without a warrant;

imposes a legal obligation on TOs to assist with the targeted interception of data and communications and equipment interference in relation to an investigation (however, foreign companies are not required to engage in bulk collection of data or communications);

places the Wilson Doctrine (a convention whereby police and intelligence services are restricted from intercepting communications of Members of Parliament) on a statutory footing for the first time, as well as safeguards for people such as journalists, lawyers and doctors involved in other sensitive professions;

provides local government with some investigatory powers (e.g., to investigate someone fraudulently claiming benefits), but not access to internet connection records;

creates a new criminal offence for unlawfully accessing internet data; and

creates a new criminal offence for a TO or someone who works for a TO to reveal that data has been requested.

The provisions of the IPA are being enacted in stages via a series of statutory instruments (most recently through the Investigatory Powers Act 2016 (Commencement No. 11) Regulations 2019 (SI 2019/174) in force from 5 February 2019). To date, most portions of the IPA have been enacted. The equivalent provisions in the legacy RIPA legislation have been repealed or amended, but the remaining RIPA provisions (i.e., those that have not been expressly repealed or amended to date) continue to govern the UK interception statutory regime. The government’s intention is to repeal RIPA in its entirety, if and when the equivalent, remaining IPA provisions are enacted. As a result, we have a rather complex regulatory landscape in which a patchwork of statutory instruments have largely, but not entirely, brought the IPA into force and amended or repealed the legacy RIPA legislation. Furthermore, in light of recent case law, it remains to be seen to what extent the IPA will survive as currently drafted: the outstanding provisions of the IPA remain under consideration by the government. In addition to Watson, civil liberties group Liberty has mounted a legal challenge to the IPA by way of judicial review. In April 2018, the UK High Court ruled that Part 4 of the IPA, which relates to the retention of communications data, was incompatible with EU law in two respects: in the context of criminal justice, the relevant provisions allowed access to retained data that was not limited to the purpose of combating serious crime, and that access was not subject to prior review by a court or independent body. The High Court decided against making an order of disapplication, but ordered that the government must replace the relevant provisions by 1 November 2018. In response, on 31 October 2018 the government introduced the Data Retention and Acquisition Regulations 2018. However, the Regulations have been criticised as not going far enough to address the human rights concerns raised by the High Court.

---

82 ibid.
On 13 September 2018, the European Court of Human Rights ruled in the case of *Big Brother Watch and Others v. the United Kingdom* that certain aspects of the bulk interception regime under RIPA and the regime for obtaining communications data from communications and service providers violate Article 8 (the right to respect for private and family life and communications) and Article 10 (the right to freedom of expression) of the European Convention on Human Rights (ECHR). Big Brother Watch and the applicant campaign groups requested that the case be referred to the Grand Chamber at the European Court of Human Rights, where it was heard in July 2019; judgment is expected in early 2020, on the primary issues of the bulk interception of communications; intelligence sharing with foreign governments; and the obtaining of communications data from communications service providers.

**Protection for children**

Under the GDPR, children are defined as vulnerable natural persons who merit specific protection with regard to their personal data. The GDPR defines a ‘child’ as anyone below the age of 16, unless a Member State provides, as the UK has done, for a lower age (which cannot be lower than 13) – the DPA has set the age of children at the minimum permitted threshold (i.e., anyone younger than 13 years). Consent to the processing of personal data in connection with the provision of online services to children is required to be given by a person with parental responsibility. Data can also be processed based on legitimate business interests, but it is clear that it will be harder to argue that the interests of a company outweigh those of a child. The GDPR also introduces a right to be forgotten, which will make it necessary for certain service providers, such as social media services, to delete any personal data processed or collected when the user was a child.

In May 2018, the government published a green paper titled Internet Safety Strategy. The paper discusses a series of proposed measures to increase the safety of the online environment in the UK, including a range of measures aimed at protecting children, such as laws related to cyberbullying and online child sexual exploitation and measures to develop children’s digital literacy. Further details of the proposed measures will be set out in a white paper on the same topic, to be published later in 2018.

The Child Exploitation and Online Protection Centre (CEOP) works to prevent exploitation of children online; it is made up of a large number of specialists who work alongside police officers to locate and track possible and registered offenders. CEOP operates as a command of the National Crime Agency. CEOP also offers training, education and public awareness in relation to child safety online.

Internet safety for children in the UK is also monitored by the UK Council for Internet Safety (UKCIS) (previously the UK Council for Child Internet Safety (UKCCIS)),
a forum consisting of government, technology and communications organisations and third sector organisations, collaborating to improve online safety. The UKCIS has most recently published a Digital Resilience Framework\textsuperscript{91} to assist, among other organisations, schools and child services providers to integrate digital resilience into education and other child settings.

Website and software operators may apply for the Kitemark for Child Safety Online. This has been developed through collaboration between the British Standards Institution (BSI) (the UK’s national standards body), the Home Office, Ofcom, and representatives from ISPs and application developers. The BSI tests internet access control products, services, tools and other systems for their ability to block certain categories of websites (e.g., sexually explicit, violent or racist activity).

**Cybersecurity**

The Computer Misuse Act 2000 (as amended by the Police and Justice Act 2006) sets out a number of provisions that make hacking and any other forms of unauthorised access, as well as DoS attacks and the distribution of viruses and other malicious codes, criminal offences. Further offences exist where an individual supplies tools to commit the above-mentioned activities.

The government has consolidated its focus on cybersecurity through the establishment of the National Cyber Security Strategy, with a dedicated pool of funds stretching to £1.9 billion over five years until 2021.\textsuperscript{92} Cybercrime detection and response is primarily led by the National Crime Agency, working together with the National Cyber Security Centre (NCSC), a government body established in 2016 to act as a single national authority on cybersecurity. One of the NCSC’s roles is to manage the Cyber-Security Information Sharing Partnership, which facilitates the sharing of real-time cyber threat information between the public and private sectors. In its National Cyber Security Strategy Progress Report,\textsuperscript{93} published in May 2019, the government reported on a total of 665 cybersecurity response actions carried out between 2017 and 2019, including many undertaken in coordination with international agencies.

At a European level, the European Parliament adopted the NISD in July 2016, which is the first EU-wide legislation on cybersecurity. The aim of the NISD is to enhance network and information system security in essential economic and digital services. It introduces, inter alia, mandatory breach notification requirements and minimum security requirements.\textsuperscript{94} While the GDPR’s aim is to protect personal data, the NISD focuses on protecting essential infrastructure, and is therefore not limited to personal data.

The NISD imposes obligations on two types of organisations: essential service operators (ESOs) within the energy, transport, banking, financial market infrastructure, health, drinking water and digital infrastructure sectors; and digital service providers (DSPs), including entities such as online marketplaces, online search engines and cloud computing service providers. These companies must now report breaches of cybersecurity to the national competent authorities without undue delay where the relevant incident would have a significant impact.

\textsuperscript{91} Available at https://www.gov.uk/government/publications/digital-resilience-framework.
on the core services provided by a company. The NISD had been stuck in negotiations between EU lawmakers and Member States over which sectors the Directive should cover; after months of negotiations, it was decided that digital platforms such as search engines, social networks and cloud computing service providers will be subject to the Directive's remit, albeit with lighter touch requirements. The Directive aims to ensure a uniform level of cybersecurity across the EU as part of the Commission's wider Digital Agenda for Europe.

As of 9 May 2018, the NISD should have been implemented in each EU Member State. In the UK it has been implemented by way of the NIS Regulation, which came into force on 10 May 2018. The NIS Regulation:

\( a \) applies to ESOs and DSPs with thresholds designed to capture the most important operators in their sector due to, for example, their size;

\( b \) is regulated by the ICO in respect of DSPs and, in respect of ESOs, the competent industry-specific regulator, such as the Department for Business Energy and Industrial Strategy, Ofcom and NHS Digital. GCHQ acts as the UK's single point of contact as required by the NISD;

\( c \) requires operators to develop minimum levels of security, as well as evidence that these higher standards have been met, and notify incidents meeting specific thresholds to the relevant regulator. Notifications should be made without undue delay and within 72 hours of becoming aware of the incident where feasible. The NIS Regulation notification obligations are separate from the personal data breach notification obligations under the GDPR and DPA – depending on the specific circumstances, an organisation may be required to report a cybersecurity incident to both its NIS competent authority under the NIS Regulations (i.e., the ICO for DSPs, or relevant industry regulator for ESOs), and to the ICO under the DPA (if the incident also constitutes a relevant personal data breach, and the organisation is acting as a data controller); and

\( d \) imposes harsher penalties to mirror the GDPR, with fines up to the higher of £17 million or 4 per cent of annual worldwide turnover.

While the NISD applies to certain financial institutions, the NIS Regulation does not apply to entities that fall within the remit of the regulatory authority of the Financial Conduct Authority, the Bank of England or the Prudential Regulation Authority, as these institutions have been deemed to impose requirements on financial institutions that meet the obligations under the NISD.

In respect of DSPs, the NIS Regulation does not apply to small and micro businesses (i.e., companies employing fewer than 50 people whose annual turnover or balance sheet total, or both, is less than €10 million). However, if a DSP is part of a larger group, the group's size may need to be taken into account in determining whether the provider is excluded from the application of the NIS Regulation (depending on the level of control exercised over the provider by other group entities).

In respect of ESOs, certain sectors are exempt from some aspects of the NISD where they are obliged to comply with equivalent provisions within existing regulations (e.g., the finance and civil nuclear sectors). The competent authority has a discretion to deem a particular organisation to be an ESO even if the threshold conditions are not met. In addition, ESOs are required to register with their competent authority.
Following the implementation of the NIS Regulations, the ICO reports that it received approximately 2,500 cybersecurity notifications under the NIS Regulations in 2018–2019,\(^\text{95}\) the majority of which related to phishing attaches and unauthorised access.

## IV SPECTRUM POLICY

### i Development

The current EU regulatory framework for spectrum has been in force since 2003 following the introduction of the Telecoms Reform Package. This regulatory framework, in particular the Framework Directive\(^\text{96}\) and the Authorisation Directive,\(^\text{97}\) requires the neutral allocation of spectrum in relation to the technology and services proposed by users (e.g., MNOs and radio broadcasters). Following on from the Telecoms Reform Package, the Commission required Member States to adopt measures including greater neutrality in spectrum allocation, the right of the Commission to propose legislation to coordinate radio spectrum policy, and to reserve part of the spectrum from the digital dividend (from the switchover to digital television services) for mobile broadband services through the Better Regulation Directive and the Citizens’ Rights Directive. In 2016, Ofcom developed a framework for spectrum sharing, highlighting the importance of considering the circumstances of each potential opportunity, covering its costs and benefits.

In the UK, Ofcom is responsible under the Act for the optimal use of the radio spectrum in the interests of consumers. This includes, inter alia, monitoring the airwaves to identify cases of interference, and taking action against illegal broadcasters and the use of unauthorised wireless devices. The 2016 framework established three key elements when identifying potential sharing opportunities in certain bands: characteristics of use for all users that inform the initial view of the potential for sharing, and what tools may be relevant; barriers that may limit the extent of current or future sharing, despite the liberalisation of licences and existing market tools such as trading or leasing; and regulatory tools and market and technology enablers that match the characteristics of use and barriers to facilitate new and more intense sharing.\(^\text{98}\)

### ii Flexible spectrum use

As the uses of the radio spectrum have increased, the allocation of spectrum by the regulator has developed from a centralised system, where use was determined by the regulator, to a market-based approach, where users compete for spectrum. Currently, auctions are the primary market tool used to implement the allocation.

Spectrum trading was introduced in the UK for the first time in 2004, and is permitted under the Wireless Telegraphy Act 2006 and associated regulations. Originally, the trading of spectrum was subject to a multi-stage process that, inter alia, required a decision by Ofcom about whether to consent to the trade. However, the Wireless Telegraphy (Mobile Spectrum Trading) Regulations 2011, directed at making more efficient use of the available spectrum, and improvements in mobile services to meet the demand for faster and more reliable services

---

\(^{95}\) Available at https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

\(^{96}\) Directive 2002/21/EC.

\(^{97}\) Directive 2002/20/EC.

for consumers, made significant changes to this process, removing the need to obtain Ofcom’s consent for proposed trades in most cases. In addition, under these Regulations, a licensee can transfer all or part of the rights and obligations under its licence. A partial transfer, or spectrum leasing, can be limited to a range of frequencies or to a particular area. Ofcom also plans to simplify the process for time-limited transfers in line with the Revised Framework Directive.

In December 2018, Ofcom published a report regarding shared access to spectrum and supporting mobile technology.99 In its report, Ofcom outlines a series of aims and proposals to ensure users have suitable spectrum access. Further, in July 2019, Ofcom published a document setting out proposals relating to local licences for particular spectrum bands in order to support mobile technology for customers.100 To facilitate this, Ofcom has proposed three shared access bands which support mobile technology, each of which is adjacent to bands available (or being considered) for national mobile use.101

iii Broadband and next-generation mobile spectrum use
Ofcom issued a call for information on spectrum above 6GHz that ended in February 2015.102 Following on from this, in April 2016 Ofcom consulted on improving spectrum access for consumers in the 5GHz band. Ofcom subsequently set out plans to open up a sub-band within the 5GHz frequency range for Wi-Fi, which would increase the number of 80MHz channels available for Wi-Fi from four to six to accommodate data-hungry applications and ease congestion. These extra channels, which are already being used in the US, could be opened up within the next few years.103 In March 2017, Ofcom published its Statement on improving spectrum access for consumers in the 5GHz band, and in July 2017 published its Decision to make Wireless Telegraphy Exemption Regulations 2017; this was predominantly due to increasing demand for Wi-Fi and the role of spectrum in addressing such demand.104 The technology has provided more capacity at faster speeds for mobile services on smartphones such as video streaming, email and social networking sites.

iv White space
Free spectrum, or ‘white space’, left over from the UK’s switch from analogue to digital TV and radio, has been available for mobile broadband and enhanced Wi-Fi since 2011. A white space device will search for spectrum that is available and check a third-party database to find out what RFs are available to ensure that it does not interfere with existing licensed

102 Laying the foundations for next generation mobile services, update on bands above 6GHz, Ofcom, 20 April 2015. Available at http://stakeholders.ofcom.org.uk/binaries/consultations/above-6ghz/5G_CFI_Update_and_Next_Steps.pdf.
users of the spectrum. New white space radios use frequencies that are allocated for certain uses elsewhere but are empty locally. Flawless management of spectrum is required to avoid interferences.

Since February 2015, Ofcom has allowed the commercial use and deployment of white space broadband technology, harnessing the unused parts of the radio spectrum in the 470MHz to 790MHz frequency band.

Ofcom is in the relatively early stages of developing spectrum sharing. White space spectrum with a frequency in the spectrum bank 470MHz to 790MHz, which is not being used at particular times, is the key to developing such sharing. This would be enabled by location-aware wireless devices or databases that provide information on white space availability. Likewise, Ofcom set out in its spectrum management strategy that it would place particular emphasis on spectrum sharing. In July 2015, Ofcom published a consultation in an attempt to identify barriers to sharing, include regulatory tools to facilitate further sharing and set out how sharing would be considered on a case-by-case basis. In December 2017, Ofcom published its Review of the authorisation regime for spectrum access in which it detailed several key initiatives aimed at enabling spectrum sharing, such as the licence exemption (mentioned above) and geographic licences as well as dynamic spectrum access (DSA). DSA was first implemented with TV white spaces where valuable, unused, low frequency spectrum in the 470–790MHz band was made available to devices meeting a minimum technical specification.105

In July 2019, the UK published a consultation paper in relation to the proposed approach to implementation of the European Electronic Communications Code Directive.106 Member States have until 21 December 2020 to implement its provisions into domestic law. The UK took an active role in negotiating this directive to ensure it supports the UK’s aim to improve connectivity. Implementation of this directive will support a stable regulatory framework which incentivises competitive network investment. Implementation of the spectrum provisions will also support 5G deployment by allowing for the release of additional spectrum and supporting spectrum sharing, and is anticipated to support the extension of mobile coverage in rural areas.

v Spectrum auctions

The first 5G spectrum auction to be completed by Ofcom took place in April 2018, with O2, EE, Three and Vodafone all winning spectrum. O2 acquired all 40MHz of the 2.3GHz spectrum being auctioned, as well as 40MHz of the 3.4GHz spectrum, making it the biggest winner in the auction. Some of the spectrum was auctioned because it was recently freed up by the government to make it available for civil use, having been previously used by the Ministry of Defence.

Another 5G spectrum auction is expected to take place in 2020, as the 2018 5G auction will not cover the anticipated demand for 5G once it is commercially available.

The last spectrum auction was initially proposed to be in 2015, when licences were to be awarded in the 2.3GHz and 3.4GHz spectrum bands. The auction was postponed to 2016, and a total of 190MHz of high-capacity spectrum was to be made available in two bands,

---

2.3GHz and 3.4GHz, which are those particularly suited to high-speed mobile broadband services. Ofcom planned to set reserve prices totalling £70 million for the spectrum. Most notably, there was to be no cap on the amounts bidders could buy, as Ofcom believes that buying large blocks has the potential to support fast download speeds, helping pave the way for 5G.\footnote{Available at http://stakeholders.ofcom.org.uk/binaries/consultations/2.3-3.4-ghz-auction-design/statement/statement.pdf.} However, following the Commission’s decision to block the proposed acquisition of O2 by CK Hutchison (H3G), Ofcom published a further consultation in November 2016 on competition measures and on specific aspects of auction design for the award of the 2.3GHz and 3.4GHz spectrum bands.\footnote{ibid.} Ofcom subsequently announced the following spectrum caps in July 2017 to satisfy competition concerns: no operator would be able to hold more than 255MHz of immediately usable spectrum, and no operator would be able to hold more than 340MHz of the total amount of spectrum following the auction. In January 2018, UKGI (which administers the Public Sector Spectrum Release Programme through the Central Management Unit) reported that the programme has led to nearly 400MHz having been released so far, with plans to release 750MHz of spectrum from the public to the private sector by 2022 to stimulate economic growth. In December 2018, Ofcom published a report relating to its consultation on the award of the spectrum in the 700MHz and 3.6–3.8GHz bands.\footnote{Available at https://www.ofcom.org.uk/consultations-and-statements/category-1/award-700mhz-3.6-3.8ghz-spectrum.} As a result of stakeholder responses to the consultation, Ofcom considered that it may be appropriate for certain measures to be included in the 2020 5G auction. These proposals were published on 11 June 2019.\footnote{Available at https://www.ofcom.org.uk/consultations-and-statements/category-3/defragmentation-spectrum-holdings.} Ofcom considered the possibility of imposing a restriction on winners of less than 20MHz of the 3.6–3.8GHz spectrum, so they could bid only for the top or bottom of the 3.6–3.8GHz band in the assignment stage of the auction. In addition, Ofcom considered the inclusion of a negotiation phase, within the assignment stage of the auction, during which winners of 3.6–3.8GHz spectrum would have the opportunity to agree the assignment of frequencies in the 3.6–3.8GHz band among themselves.

To ensure competition between the national operators, Ofcom introduced a floor and cap on the amount of spectrum that each operator can win, and imposed safeguard caps to prevent an operator from holding too much spectrum. To diversify the market, Ofcom also reserved parts of the spectrum for a fourth national wholesaler. The reserved lots were won by Hutchison 3G UK.

Despite the fact that the government budgeted a surplus of £3.5 billion for the auctioned spectrum, it only raised a total of £2.34 billion;\footnote{Available at http://www.bbc.co.uk/news/business-21516243.} however, the principal stage of the 2018 spectrum auction has already raised over £1.3 billion.\footnote{Available at https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/results-auction-mobile-airwaves.}

\textbf{vi \quad Emergency services bandwidth prioritisation}

The Universal Services Directive, a further part of the Telecoms Reform Package, introduces several extended obligations in relation to access to national emergency numbers and the single European emergency call number (112). Prior to the Universal Services Directive,
obligations to provide free and uninterrupted access to national and European emergency numbers applied to providers of publicly available telephone services only. Under this Directive, however, these obligations are extended to all undertakings that provide to end users ‘an electronic communication service for originating national calls to a number or numbers in a national telephone numbering plan’, and the UK has mirrored this wording in its revisions to General Condition 4 under the Act. Such electronic service providers are therefore required to ensure that a user can access both the 112 and 999 emergency call numbers at no charge and, to the extent technically feasible, make caller location information for such emergency calls available to the relevant emergency response organisations. Ofcom’s revised general conditions for emergency services network (ESN) provider compliance came into force on 1 October 2018, amending the obligations relating to access to emergency services. The changes include extending the current requirements to ensure end users can access emergency organisations through eCalls.

In 2013, the Home Office announced the Emergency Services Mobile Communications Programme for a dedicated ESN that would provide the next-generation communication system for emergency services. However, one of the lots, relating to a contracted agreement for an MNO to extend guaranteed signal coverage to ensure mobile coverage, was withdrawn in January 2015. The remaining contracts for the operation of the ESN were won by EE, which provides the network, and Motorola Solutions, which supplies the user services (supported by Kellogg Brown Root as a delivery partner). Together they work to provide the UK’s emergency services with a 4G LTE mobile network, replacing the existing private terrestrial trunked radio (Tetra) system. According to the Home Office, the UK is first in the world to deliver critical voice and data for emergency services over an enhanced and more resilient commercial 4G network.113 The new system has the key advantage of allowing emergency services traffic to be prioritised ahead of communications by the general public, and this was successfully tested in February 2018 for the first time between an EE mobile mast site in Bristol and a location in Basingstoke.114 In July 2019, the Commons Select Committee published a progress review in relation to the implementation of ESN, finding that the costs of crucial communications systems continue to rise, while the benefit to the emergency services is still unclear.115 The report recommended that by October 2019, the Home Office should agree specific and detailed criteria which will determine when ESN is ready to replace the airwave radio system. The report also recommended that the risks presented by Motorola’s position (as supplier to ESN and owner of the airwave radio system) and the possible need to extend the airwave radio system until it can be replaced by ESN should be considered and presented to the Parliamentary Committee. A revised business plan in relation to ESN should be completed by the end of 2019.


115 Available at https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1755/1755.pdf.
V MEDIA

The transition from traditional forms of media distribution and consumption towards digital converged media platforms continues to disrupt and change the commercial foundations of the entertainment and media industry in the UK. Members of the industry are all grappling with new business models to monetise content and control frameworks to provide sufficient protection for the rights of content creators and consumers alike. The Commission's DSM Strategy has wide-ranging implications for the UK media sector (subject to changes to national law as a result of Brexit). Areas of particular relevance to the media sector include the regulation on cross-border portability of online content services, amendments to the Audiovisual Media Services Directive and updates to the European copyright law regime, including in the form of the recent EU Copyright Directive.

i Superfast broadband and media

Fast broadband underpins the accessibility to consumers of internet-delivered content services. The Commission has highlighted that the global internet video share in consumer internet traffic is expected to increase from 64 per cent in 2014 to 80 per cent by 2019.\(^{116}\)

By the end of March 2018, the government’s rollout of superfast broadband had reached 4.85 million homes and businesses across the UK. This means that the government delivered on its commitment to extend superfast broadband to 95 per cent of UK homes and businesses by the end of 2017, and at the time of writing is pushing beyond 96 per cent with an ambition to reach at least 97 per cent coverage by March 2020. The focus is now shifting to exploring ways to take superfast broadband to the most remote and hardest-to-reach places in the UK. Seven market test pilots ran between June 2014 and March 2016 to test ways to take broadband to remote communities. The government published its findings in February 2016.\(^{117}\) This is consistent with the DEA, which provides for a USO whereby consumers may request a minimum download speed of 10Mbps by 2020. On 19 May 2019, the government launched the Rural Gigabit Connectivity programme, which will trial a model to deliver full fibre broadband to premises in rural and remote areas.\(^{118}\)

ii European DSM Strategy and media

**Audiovisual Media Services Directive**

As part of the DSM Strategy, in May 2016, the Commission adopted a legislative proposal to revise the Audiovisual Media Services Directive (AVMSD), which coordinates national legislation on all audiovisual media including both TV broadcasts and on-demand services. In June 2018, the European Parliament, the Council and the Commission confirmed the preliminary political agreement reached on the proposed revisions. On 6 November 2018, the Council adopted the revised text, marking the final step in the legislative process.\(^{119}\)

---


\(^{118}\) Available at https://deframedia.blog.gov.uk/2019/05/20/200-million-rollout-of-full-fibre-broadband-begins-and-the-guardian-on-ca-eel-research/.

revised Directive entered into force on 19 December 2018. Following its entry into force, Member States will then have a 21-month period to transpose the changes into national law. The revisions include:

a extending the AVMSD’s application to video-sharing platforms where the principal purpose of the service is the provision of programmes or user-generated videos, or both, to the public, and which organise content in a way determined by the provider of the service (e.g., by algorithmic means);

b clarifications to the establishment test (i.e., which determines which Member State has jurisdiction over a linear or on-demand service provider);

c changes to place linear and on-demand services on an equal footing when it comes to measures to protect minors from harmful content;

d offering broadcasters more flexibility in television advertising – in particular, the advertising limit of 20 per cent of broadcasting time will apply between 6am and 6pm, and the same share will be permitted during prime time (i.e., 6pm to midnight) (rather than 20 per cent per clock hour); and

e an obligation on on-demand audiovisual media services to ensure 30 per cent of the works in their catalogues are European works and to ensure prominence of those works. Furthermore, Member States will have the option to require linear and on-demand service providers to invest in European works, including via direct investment in content and contributions to national funds.

The Commission and UK government have each published notes on the implications of Brexit on the audiovisual media sector. Subject to any agreement that the UK may reach with the EU, post-Brexit, the AVMSD, including the country of origin principle and the rule on freedom of reception and retransmission, will cease to benefit services under UK jurisdiction, and the UK will be treated as a third country. According to the recitals to the earlier version of the AVMSD, Member States are free to take whatever measures they deem appropriate with regard to audiovisual media services that come from third countries, provided they comply with EU law and the international obligations of the EU. Under the AVMSD, a complex test applies to determine which country has jurisdiction over a media service provider (largely based on the location of the head office, editorial decision making and the workforce). Post-Brexit, it would be possible for a media service provider to keep a

---


122 The country of origin principle is found in two places: The AVMSD (Directive 2010/13/EU) is based on the country of origin principle, whereby service providers are subject to the regulations in their country of origin only and are not subject to regulation in the destination country, except in limited circumstances (Article 2(1)). Under the Satellite and Cable Directive (Directive 98/83/EEC), this principle effectively allows broadcasters to clear rights for satellite broadcasting in one Member State and allows them to then make their satellite transmissions available in other Member States.

123 Article 3(1) of AVMSD.

124 Recital 54 of AVMSD.
UK head office but be subject to the jurisdiction of a Member State (and therefore continue to benefit from the country of origin principle within the EU), provided a significant part of the workforce operates in that Member State.

The UK government’s consultation on its proposed approach to implementing the AVMSD ended on 22 August 2019, with feedback at the time of writing yet to be published. The consultation document sets out the UK’s proposed approach to enshrining the AVMSD into national law.

In light of Brexit, the extent to which the UK is legally obliged to implement the AVMSD is currently unclear. The Withdrawal Agreement of November 2018 included a transition period that would extend through to 31 December 2020. During this time, EU law would still apply to the UK, therefore the UK would be obliged to implement the AVMSD into national law. Any deal negotiated with the EU would likely enshrine a similar transition period, which in turn would likely extend beyond the deadline for Member States to implement the AVMSD into national law.

In the event of the UK leaving the EU without a deal, the government’s ‘no-deal’ Brexit technical note on broadcasting and video-on-demand confirms the AVMSD will no longer apply to the UK. In this scenario, the UK would be free to determine the extent to which elements of the AVMSD are implemented into national law.

Separately, and along with 20 other EU countries,125 the UK is party to the Council of Europe Convention on Transfrontier Television (ECTT),126 which provides for freedom of reception and retransmission.127 This is also relevant to the European works test, which is satisfied if a programme originates from a non-EU country that is party to the Convention.128 The AVMSD takes precedence among EU Member States, but the UK’s position as a party to the Convention will not be affected by its exit from the EU. Therefore, in the absence of a Brexit deal, the Convention could be relied upon as between the UK and the 20 Member States that have signed and ratified it.

For the seven non-Convention countries, additional licences and consents will be required, subject to local law requirements. Works originating in the UK will continue to be classed as European works. However, VOD services are outside of the scope of the Convention and, if subject to UK jurisdiction according to the AVMSD test, would need to comply with the local law requirements in each Member State in which they are offered.

The UK government has published the Broadcasting (Amendment) (EU Exit) Regulations 2019,129 which will come into force on exit day in the event of a no-deal Brexit. The regulations change the authorisation system in the UK to a country-of-destination system, thus requiring broadcasts into the UK (and accessible via a licensed electronic programme guide) to be licensed and regulated by Ofcom, irrespective of the origin of the broadcast. An important exception to these regulations is broadcasts originating from countries that are signatories to, and have ratified, the ECTT (including non-EU Member States). Broadcasters in states that are members of the ECTT will not need a licence from Ofcom to broadcast into the UK, meaning that in effect, the country of origin principle would be retained in respect of these countries.

---

125 Excluding Belgium, Denmark, Greece, Ireland, Luxembourg, the Netherlands and Sweden.
127 Article 4 of Council of Europe Convention on Transfrontier Television.
128 See Article 1(1)(n) of AVMSD.
Portability Regulation

On 9 December 2015, the Commission proposed a regulation to enable the cross-border portability of online content services.\(^{130}\) The resulting Portability Regulation was published in the Official Journal on 30 June 2017\(^{131}\) and came into force on 1 April 2018.\(^{132}\) It allows Europeans who purchase or subscribe to audiovisual content (such as films, sports broadcasts, music, e-books and games) in their home Member State to access this content when they travel or stay temporarily in another Member State. Providers of online content services that are provided for payment (it is optional for free services) must ensure the cross-border portability of their services such that subscribers may access and use the services when temporarily present in another Member State. When verifying the subscriber’s Member State of residence, service providers must limit the means to verify residence to two means of verification in a list (such as, for example, an identity card and payment details).

However, the Portability Regulation will cease to apply to UK–EEA travel post-Brexit in the absence of a reciprocal agreement with the EU. This is because the Regulation relies on a legal fiction whereby the provision of and access to the relevant service is deemed to take place in the subscriber’s country of residence, effectively disapplying the local law of the country of temporary presence. The Regulation only applies to EEA Member States and its effects do not extend to third countries. In the UK, the Regulation will be revoked on exit.

Post-Brexit, content service providers will not be obliged under the Regulation to provide cross-border portability for customers travelling between the UK and EEA. Content service providers will be free to continue providing cross-border portability to their customers on a voluntary basis. The practical effect of this change is that, dependent on the terms of a service and licences in place between the service provider and the rights holders, UK customers in the EEA (and vice versa) may note restrictions on the content ordinarily available to them in their home country.\(^{133}\)

Copyright reform

Satellite and Cable Directive

On 14 September 2016, in addition to the telecoms proposals outlined in Section II.v, the Commission adopted new proposals for copyright reform as part of its DSM Strategy. The Commission released proposals for a regulation laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes (such regulation proposals have since been passed as the Satellite and Cable Directive (as opposed to a directly applicable regulation), amending the 1993 Directive of the same name);\(^{134}\) a directive on copyright in

---
\(^{130}\) Available at https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-627-EN-F1-1.PDF.

\(^{131}\) Available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1128&from=EN.


the DSM (Copyright Directive); and proposals for an additional directive and regulation to implement the Marrakesh Treaty to Facilitate Access to Published Works for Persons who are Blind, Visually Impaired, or Otherwise Print Disabled (Marrakesh Treaty).

The Satellite and Cable Directive entered into force on 7 June 2019, following which date Member States have two years (until 7 June 2021) to transpose the Directive into national law. The Commission’s initial proposal was aimed at introducing a cross-border clearance mechanism for digital broadcasting by broadcasters and retransmission of broadcasts online. Broadcasters transmit programmes on their services that they have licensed from others or produced themselves, but programmes will inevitably contain content that is protected by copyright and needs to be cleared for use. The Satellite and Cable Directive extends the country of origin principle – which has been in place for decades in respect of cable and satellite communications – to online simulcasts and catch-up services (‘ancillary online services’) in respect of (1) radio programmes; and (2) broadcasters’ TV programmes which are news and current affairs programmes, or broadcasters’ own fully financed productions. This means that, in respect of ancillary online services, broadcasters will only need to clear rights once, in the Member State in which the broadcasting organisation has its principal establishment. However, the Directive does not extend to TV broadcasts of sports events and TV productions acquired or commissioned from third parties. The Satellite and Cable Directive also extends the current system of mandatory collective management for retransmissions by cable of television and radio broadcasts from other Member States to wire or over-the-air means (including, e.g., satellite, DTT and IPTV), provided that the original transmission was not purely online. This means that instead of negotiating individually with every rights holder, operators who offer packages of channels will be able to obtain licences from collective management organisations.

Further, the Satellite and Cable Directive clarifies the principle of ‘direct injection’ by confirming that when a broadcaster transmits programmes to a distributor (without the broadcaster itself simultaneously transmitting the programmes to the public), and the distributor then transmits those programme-carrying signals to the public, the broadcaster and distributor are deemed to have singularly participated in communicating the programmes to the public. As such, this will require the relevant rights holders’ authorisation, therefore ensuring that rights holders are remunerated for the same.


137 Text adopted available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2019.130.01.0082.01.ENG.
Copyright Directive

The Commission’s original proposal for the Copyright Directive was the subject of extensive lobbying by digital platforms and content creators. On 12 September 2018, the European Parliament adopted amendments to the proposed text (particularly to Articles 15 and 17 (originally Articles 11 and 13 respectively), which proved to be the most controversial) and referred it for informal trilogue negotiations with the Council and Commission. On 15 April 2019, the European Council voted to adopt into EU law the amended Copyright Directive.

The Copyright Directive focuses on three areas. First, it introduces measures to achieve a well-functioning marketplace for copyright. These include provisions for:

a. a new related right in publication that will allow publishers to charge fees for digital uses of the copyright works they have invested in the distribution of (not extending to mere hyperlinks or to the use of individual words or very short extracts of a press publication) This Article does not prevent legitimate private or non-commercial uses of press publications by individual users, nor does its application extend to blog posts or scientific/academic publications (Article 15);

b. a requirement for online content-sharing service providers (OCSSP) to obtain authorisation from rights holders. If no authorisation is granted, OCSSP will be liable for unauthorised acts of communication to the public of copyright-protected works, unless they can show they (1) used best efforts to obtain authorisation; (2) used their best efforts (in accordance with high industry standards of professional diligence) to ensure the unavailability of specific works identified by rights holders; and (3) acted expeditiously to remove or disable access to any unauthorised content after being notified (Article 17); and

c. an obligation to ensure authors and performers are entitled to receive ‘appropriate and proportionate’ remuneration for exclusive licences of their works, and a mechanism for increasing the transparency to rights holders of the exploitation of their works and performances, with an alternative contract adjustment mechanism to allow authors and performers to rebalance contracts (Articles 18, 19 and 20).

Secondly, it introduces measures to improve licensing practices and ensure wider access to content by:

a. implementing a legal mechanism to facilitate easier licensing of out-of-commerce works (which are works that are not available to the public through customary channels of commerce after a reasonable effort has been made to determine whether they are available to the public) by cultural institutions to aid cultural institutions in making these works, which have significant cultural and educational value, available to the public (Article 8);

b. allowing Member States to extend collective licensing to cover rights holders within a class who are not members of the relevant CMO. The CMO will be presumed to be representing such rights holders, but such rights holders must be able to opt out at any time in order to exclude their works from the collective licences (Article 12);

c. requiring Member States to set up impartial bodies to assist in the negotiation of licensing agreements between audiovisual rights holders and VOD platforms (Article 13); and

d. ensuring that when the term of protection of a work of visual art has expired, any material reproduced from that work is not subject to copyright, unless the reproducer has added something original to the reproduction (Article 14).
Thirdly, the Directive introduces measures to adapt exceptions and limitations to the digital and cross-border environment in relation to research and other organisations conducting text and data mining; the digital use of works and other subject matter for distance-learning educational purposes; and cultural heritage organisations making digital copies of their permanent collections for preservation purposes (Articles 3–6 inclusive).

Implementation of the Marrakesh Treaty

The directive designed to implement the Marrakesh Treaty introduces a new mandatory exception to the copyright rights harmonised under EU law, allowing people who are blind or otherwise print-disabled to access books and other content in formats that are accessible to them, including across borders. The regulation governs exchanges of accessible format copies between the European Union and third countries that are parties to the Marrakesh Treaty. The regulation and directive implementing the Marrakesh Treaty were published in the Official Journal on 20 September 2017. The regulation applied from 12 October 2018, and Member States had to implement the directive by 11 October 2018. Accordingly, the Copyright and Related Rights (Marrakesh Treaty etc.) (Amendment) Regulations (2018/995) came into force on 11 October 2018 and amended the UK’s copyright law to make the UK’s laws compatible with the Marrakesh Directive. The UK government has confirmed that the regulation and the UK’s implementation of the directive will be retained in UK law post-Brexit. However, the UK is party to the Treaty through its membership of the EU. Until the UK government ratifies the Treaty in its own right after Brexit, the cross-border exchange of accessible format copies with the UK may be restricted.

Changes to copyright law in the event of a ‘no deal’ Brexit

A government guidance note published on 5 September 2019 sets out a number of key changes to UK copyright law as a result of the UK’s exit from the EU. In addition to country of origin issues, the revocation of the Portability Regulation, and the continued implementation of the Marrakesh Treaty (each as discussed above), the following points from the government’s note are of relevance to the media sector:

a Sui generis database rights. Sui generis database rights prevent the unauthorised copying or extraction of data from databases which involve a substantial investment in time, money or effort and were created by an EEA national, resident or business. Following Brexit, UK citizens, residents and businesses will no longer be eligible to receive or hold sui generis database rights in the EEA. Pre-existing database rights will continue to exist in the UK for the remainder of their duration. Those in the UK who wish to use databases protected by these rights will continue to need the permission of the rights holder(s).

139 Available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017L1564&from=EN.
b Collective rights management. EU collective management organisations (CMOs) are required by the EU Collective Rights Management (CRM) Directive to represent, on request, rights holders of any EEA Member State. Post-Brexit, EEA CMOs will not be required by the CRM Directive to represent UK rights holders or to represent the catalogues of UK CMOs for online licensing of music rights.

c Orphan works. The EU Orphan Works Directive provides an exception to copyright infringement of orphan works (works where the rights holder is unknown or cannot be found), enabling cultural heritage institutions (CHIs) established in the EEA to digitise and make orphan works available online across EEA Member States. UK CHIs will not be able to make use of the orphan works exception after a no-deal Brexit and may face claims of copyright infringement if they make orphan works available online in the EEA.

Commission investigation into US film studios

The Commission has investigated the practices of six major US film studios (Disney, NBCUniversal, Paramount Pictures, Sony, Twentieth Century Fox and Warner Bros) with respect to clauses in their licensing agreements with telecommunications company Sky UK concerning absolute territorial exclusivity (preventing passive sales). On 26 July 2016, the Commission accepted commitments from Viacom-owned Paramount to end a probe into potentially anticompetitive film licensing contracts. As a result, Paramount agreed to stop enforcing contractual clauses that prevent European consumers outside the UK and Ireland watching Paramount films on Sky’s UK satellite and online channels, and prevent rival broadcasters from airing its pay-TV content in the UK. The probe dealt only with Sky UK in the UK and Ireland, but the Commission also investigated the British pay-TV operator’s approach to consumers in France, Italy and Germany. Likewise, Paramount will not introduce or renew similar clauses in film licensing contracts with other broadcasters that operate in other European countries. Paramount will run the commitments package for five years, and it will cover both standard pay-TV and on-demand services, both online and by satellite. The effect of the Commission accepting the commitments is that the studio will not be required to pay a fine, nor to admit liability. On 6 February 2017, details were published of an appeal by Canal+ against the Commission’s decision to accept commitments from Paramount.142 In November 2018, the General Court ruled the Commission’s decision to settle the probe was ‘sufficiently grounded in law as regards whether the commitments offered by Paramount were suitable to resolve the competition concerns expressed by the Commission’.143

The European Commission closed its investigation in March 2019, following legally binding commitments from Disney,144 NBCUniversal, Sony Pictures and Warner Bros as well as from Sky UK, addressing the competition concerns raised by the Commission’s investigations.145 The studios committed not to apply in respect of any broadcaster in the EEA, clauses in existing film licensing contracts for pay-TV that prevent EU consumers outside the UK and Ireland subscribing to pay-TV services to access films via satellite or

---

The studios further committed to refraining from re-introducing similar clauses in film licensing contracts for pay-TV with any broadcaster in the EEA. The settlement commitments will apply throughout the EEA for a period of five years.

The Commission expressly stated that the commitments did not prejudice the studios rights under copyright law, thus ensuring the studios may still engage in licensing of their rights and enforcement of such rights under copyright laws. Additionally, the Commission clarified that the settlement does not prevent the rights of the studios or a pay-TV broadcaster to decide unilaterally to employ geo-filtering technology.

### iii OTT delivery of content and broadcast TV

An OTT platform is typically a platform that allows users to stream audiovisual content using the internet or mobile delivery means. The key benefit of OTT delivery is that it allows users to interact with content because data can flow both ways in an IP network.

OTT delivery is utilised by a range of content providers in the UK, including PSBs (i.e., BBC iPlayer, ITV Hub, All4 and My5), cable and satellite platforms (e.g., both Virgin Media and Sky offer VOD products), mobile operators, online aggregators and standalone VOD platforms (e.g., Netflix, Amazon Prime Video and NowTV). To further facilitate user access to internet-delivered services, the BBC, ITV, Channel 4, Channel 5, BT, TalkTalk and Arqiva have collaborated on an open-technology offering called YouView, which enables viewers to access free-to-air channels and catch-up and on-demand programming via their televisions (along with the ability to add access to pay-TV channels and on-demand services).

The industry is being transformed as the take-up of superfast broadband and connected televisions changes the way in which people watch television. According to Ofcom's Media Nations: UK 2019 report, across all devices, people's total television and audiovisual viewing in 2018 was four hours and 54 minutes per day. Broadcast content made up 69 per cent of this, while the remaining 31 per cent was composed of viewing non-broadcast content such as content available via standalone VOD platforms and YouTube. On average, people view three hours and 22 minutes of broadcast television a day (including seven-day catch-up) (this has fallen by 11 minutes since 2018). Despite the variety of devices available and the increased use of smartphones in the UK, the TV set is still the most popular way to view audiovisual content, with 95.2 per cent of UK homes having a working TV set in the first quarter of 2019. This proportion has decreased slightly in recent years (in 2012 it was 96.3 per cent).

The change in viewing habits is in part driven by younger viewers, who watch more non-broadcast than broadcast content. In 2018, 16 to 34 year olds watched an average of four and a half hours of content a day across all devices. This daily average is split into three main parts: live TV (83 mins – 31 per cent); YouTube (64 mins – 23 per cent); and SVoD content (52 mins – 19 per cent). Viewing of SVoD by adults aged 16–34 has increased particularly steeply in the past year, up by 22 minutes to an average of 52 minutes a day.

The total TV and online video industry revenue has grown, driven by the further expansion of the online sector, which continued its steep growth in 2018. Online subscription

---


services were a key driver of growth; however, revenue from pay-TV subscription services also increased by 1.1 per cent during 2018. The increase was the result of pay-TV price hikes which offset a small decline in subscriber numbers.\(^\text{148}\)

PSBs face challenges in light of this drastically changing landscape. While PSBs command half of all broadcast viewing, they are investing less money in first-run UK originals as increasingly they utilise third-party funding (such as co-production arrangements with third parties). However, Ofcom reports that the majority of viewers are either very or quite satisfied with PSB broadcasting,\(^\text{149}\) and that PSBs still provide a vital news service to viewers, with 73 per cent giving the provision of a trustworthy news source a 7–10 importance rating, where 10 means ‘extremely important’ and 1 is ‘not at all important’.\(^\text{150}\)

iv PSBs

The BBC Royal Charter was renewed in early 2017 and runs to the end of 2027. From 3 April 2017, a unitary board has replaced the two-tier structure of the BBC Trust and the BBC’s Executive Board as the BBC’s governing body. The Board is responsible for ensuring that the BBC fulfils its mission and promotes its public purposes, including by setting the strategic direction for the BBC within the framework of the Charter and the accompanying Framework Agreement between the BBC and the Secretary of State for DCMS, and by setting the BBC’s creative remit.\(^\text{151}\) Ofcom also became the BBC’s first external regulator, developing an operating framework for the BBC that covers regulation of the BBC’s performance, compliance with content standards and impact on competition. In October 2017, Ofcom published a new operating licence for the BBC. The licence requires the BBC to broadcast more original UK programmes, and also requires more BBC content to be made across the UK’s nations and regions.\(^\text{152}\)

In November 2017, the BBC announced its decision to bring together two of its commercial subsidiaries, BBC Studios and BBC Worldwide, to trade as a single entity known as BBC Studios. The newly created BBC Studios launched on 3 April 2018. It is the primary entity for the BBC’s commercial production and distribution activities globally.\(^\text{153}\)

On 8 March 2018, Ofcom published a report that discusses the challenges facing PSBs in the context of increased media consumption via internet-delivered services and competition from global OTT services.\(^\text{154}\) Ofcom’s findings include:

\[\begin{align*}
  a & \quad \text{the level of competition from global VOD platforms, along with the likes of Apple and Facebook, is creating a ‘rush to scale’ that is resulting in further market consolidation;} \\
  b & \quad \text{public service broadcasting has so far held up well to increased global competition. The main PSB channels still account for half of all viewing and TV advertising has been fairly resilient, although Ofcom states that this is ‘softening’. The reasoning for this is}
\end{align*}\]

---


149 Ofcom PSB tracker 2018, satisfaction of regular or occasional viewers with PSB channels.


151 See the Royal Charter available at http://downloads.bbc.co.uk/bbctrust/assets/files/pdf/about/how_we_govern/2016/charter.pdf, article 20(3).


153 For further information, see: https://www.bbcstudios.com/about/about-us/.

unclear, although Ofcom cites macroeconomic uncertainty and weakened consumer confidence as key drivers. While ITV has reduced its reliance on TV advertising revenues, Channel 4 is heavily reliant on advertising and sponsorship;

c young people are watching less scheduled TV, and brand awareness of the BBC among them is lower than Netflix and YouTube;

d Ofcom intends to support PSBs by strengthening its EPG Code through a consultation; and

e PSBs should continue to have access to digital terrestrial television (DTT) for at least the next 10 years, as mobile demand for the relevant spectrum has diminished due to 5G requiring spectrum at higher frequencies.

Ofcom has since published a report entitled ‘The Future of Public Service Media’ in July 2019,\textsuperscript{155} which notes public service broadcasting is now at a critical juncture. Since the publication of its 2018 report, the challenges facing PSBs have significantly increased pace. In response to these challenges, PSBs have developed differing approaches to meet the demand for online and on-demand viewing. By way of example, the BBC and ITV have announced plans for a new subscription service, BritBox, to make available more recent and historic BBC and ITV content than any other platform. On 19 September 2019, Ofcom published its final determination that the BBC’s involvement in BritBox did not constitute a material change to its commercial activities.\textsuperscript{156} Additionally, the BBC has put forward a series of changes to iPlayer, which have been formally approved by Ofcom.\textsuperscript{157} The changes centre on changing iPlayer from a service whereby programmes are available to ‘catch-up’ for 30 days after broadcast, to one in which programmes are available for 12 months as standard, with some available for longer. ITV and STV are now offering subscription versions of their online players. Channel 4 is trialling an ad-free version of its All4 service, and has also partnered with Sky to provide viewers with additional drama and comedy box sets.

The July 2019 report sets out the steps being taken by Ofcom with a view to establishing a new framework for public service media, to ensure its prominence and ongoing resilience in an increasingly online environment. Ofcom itself has taken the following steps, each of which are discussed in further detail below: (1) publishing a decision to update the rules on the prominence of PSB channels in electronic programme guides; (2) making recommendations to the government to ensure PSB content remains easy to find in an online and on-demand world; and (3) endorsing a range of commitments by ITV, Channel 4 and Channel 5 to invest more in original UK content for children, following an Ofcom review of this area.

The DEA added a requirement under the Act for Ofcom to periodically review and report on the provision by EPGs of information on and access to PSB channels and content via PSB VOD services. Ofcom published its first such report on 27 July 2018.\textsuperscript{158} The DEA also required Ofcom to review and revise the EPG Code prior to 1 December 2020. Pursuant to this, alongside its first EPG prominence report, Ofcom published a consultation on proposed

\begin{itemize}
  \item \textsuperscript{155} Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0022/155155/future-public-service-media.pdf.
  \item \textsuperscript{156} Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0028/167149/statement-britbox-final-determination.pdf.
  \item \textsuperscript{157} Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0029/159725/statement-bbc-iplayer-final-determination.pdf.
  \item \textsuperscript{158} Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0026/116288/report-psb-local-tv-discoverability.pdf.
\end{itemize}
changes to the linear EPG Code and options for the future regulation of prominence for VOD services. The closing date for responses was 5 October 2018, and subsequently on 4 July 2019, Ofcom published both its recommendations to the government, and its decision to update the EPG Code.

Currently in the UK, regulations guarantee the PSBs’ prominence on the traditional Ofcom-licensed linear EPGs, but no such protections are afforded to PSBs in respect of other search functionality (e.g., on connected devices and searches via voice) or in respect of PSB VOD services. While PSB VOD and catch-up services are currently generally well-positioned, this is due to commercial negotiation rather than regulation. Ofcom’s changes to the existing linear EPG Code will come into force on 4 January 2021 with 18 months for EPG providers to implement the new rules. The amendments to the EPG Code include:

- the five main PSB channels (BBC One, BBC Two, Channel 3 licensees, Channel 4 and Channel 5) being guaranteed their current positions in the top five EPG slots (subject to regional variations for Wales);
- BBC Four being guaranteed a slot within the first 24 slots of any licensed EPG;
- BBC News, BBC Parliament, CBBC and CBeebies being guaranteed slots within the first eight slots of the relevant EPG genre or section; and
- local TV services being located in the first 24 slots on digital terrestrial television of any EPG.

Ofcom’s recommendations to the government for a new framework to keep PSB TV prominent in an online world analysed options for the future regulation of prominence in the context of VOD services (including the position of PSB VOD players and the availability of PSB content on a VOD basis elsewhere within platforms and via devices). Any such changes would be the subject of future legislation. Ofcom has stated that it would support new legislation to address the prominence of internet-delivered PSB content to secure the health of the PSB system and, accordingly (following consultation), has set out the following recommendations:

- new legislation is needed to keep PSBs prominent and support the sustainability of the PSBs;
- these new rules should specify which PSB content is given prominence, and on which platforms;
- the initial focus should be on connected TVs;
- viewers should be able to find PSB content easily on the homepage of connected TVs;
- on-demand services should only be given prominence if the service is clearly delivering PSB content;
- PSB content should also be given protected prominence within TV platforms’ recommendations and search results;


the new framework should protect the prominence of PSB content that is made available without charge; and

there may need to be new obligations to ensure the continued availability of PSB on-demand content to viewers.

The DEA further granted Ofcom power to publish criteria for the provision of children’s programming and, if appropriate, to set related conditions (e.g., quotas) on the licensed public service channels. Following a review of the sector and a consultation with ITV, Channel 4 and Channel 5, Ofcom has published its view of the plans proposed by each channel and the appropriate next steps. Each channel has renewed its commitment to children’s content and committed to creating and investing more in original UK programmes made for UK children and teenagers, including live action, entertainment and news. Ofcom will monitor the broadcasters’ implementation of its plans and will continue to work with the industry to ensure children and teenagers enjoy a range of high-quality programmes from the PSBs.

VI THE YEAR IN REVIEW

i Brexit

On 23 June 2016, the UK voted to leave the EU by a vote of 51.9 per cent in favour of leave to 48.1 per cent in favour of remain. The government invoked Article 50 of the Treaty on European Union on 29 March 2017, thereby starting the period of negotiation between the UK and the EU on the terms of the UK’s exit, with exit taking effect once those negotiations have concluded or after two years (if sooner), irrespective of what terms have been agreed.

The European Union (Withdrawal) Act 2018 (Withdrawal Act) received royal assent on 26 June 2018. It provides that, on exit day (31 October 2019, at the time of writing):

- the European Communities Act (ECA) 1972 shall be repealed;
- all existing EU legislation (including EU-derived legislation, such as national implementing legislation) shall be enshrined into British law;
- the jurisdiction of the CJEU over the UK shall end; and
- the government shall be permitted to remove or amend EU laws that apply to the UK (whether directly effective or enshrined in UK law by a separate Act of Parliament) with primary legislation and, in some cases, secondary legislation via the Henry VIII clauses.

Certain provisions came into force when the Withdrawal Act received royal assent. These include provisions relating to:

- the implementation of the Withdrawal Act itself;
- border arrangements with Northern Ireland;
- powers and restrictions relating to devolved authorities;
- Parliamentary approval of the outcome of negotiations with the EU;
- negotiations for a customs arrangement with the EU and family unity for asylum seekers in the EU;
- publication of a draft bill relating to maintenance of certain environmental principles; and

the power to make secondary legislation under the Withdrawal Act, and the Parliament’s and the devolved authorities’ scrutiny of any such secondary legislation.

The remaining provisions, which relate to repeal of the ECA and the enshrining of existing EU legislation into national law (and the concurrent loss of jurisdiction of European courts over its interpretation as applied in the UK and the sovereignty of Parliament to amend such laws), shall come into force as specified in regulations made by the government.

The Withdrawal Act has been received with mixed feelings in the UK and in the EU. Within the UK, the Scottish government has refused to endorse the Withdrawal Act on the basis that it attempts to further centralise power within the UK Parliament to the detriment of the devolved regions. The Welsh government provided its endorsement only after months of negotiations. Critics within the EU query how the UK government can state that it provides equivalent protections to EU laws, for example in the context of personal data, while also retaining authority to amend at will any EU law that has been enshrined into national law. The European Parliament’s report on transfers of personal data points to the sovereignty of the UK Parliament and the loss of jurisdiction of European courts as major stumbling blocks in the search for an alternative to the UK becoming a third country for the purposes of such data transfers after Brexit. As such, its status remains uncertain.

The Withdrawal Act does not make direct provision for a transition period following exit day, and the impact of any such transitional period on the provisions of the Act remains unclear.

ii Commission proposals for a DSM Strategy

The Commission’s ambitious DSM Strategy proposals (announced 14 September 2016) signpost that Europe’s approach to digital market access is likely to:

- change significantly;
- dramatically enhance Europe’s connectivity;
- rationalise its telecoms regulatory regime;
- end certain geographical restrictions; and
- reform the European copyright regime in favour of European interests.

However, the proposals are ambitious both in terms of scale and cost: using the 5G Action Plan as an illustrative example, the Commission estimates that €500 billion in private investment will be required to deliver the Plan, of which it is projected there will be a €155 billion shortfall based on current investment trends. In February 2018, the Commission took a step forward regarding the Plan by establishing the 5G Observatory to monitor market developments in 5G technology and observe national strategies by EU Member States, particularly with regard to coverage and quality. The Commission, which appointed Mariya Gabriel to be responsible for the DSM as of July 2017, has indicated that part of the intent of the reforms, such as the 5G Observatory, is to stimulate competition and investment in the sector. To achieve this, the Connecting Europe Broadband Fund (comprising both private and public funds) has been established to help make up this shortfall. The fund aims to raise €500 million for broadband investment by 2020 and is expected to unlock total investments

---

of €1–1.7 billion. While the WiFi4EU initiative will be funded by the EU (for installation and equipment costs only) for an initial budgeted amount of €120 million, €70 million of this is reallocated funding from the Connecting Europe Facility. Only €50 million will be previously unallocated funds.

In July 2019, the Commission published a fact sheet that includes a timeline of DSM Strategy actions that had been taken up to that date. Recent progress has included the January 2018 Regulation establishing the European High Performance Computing Joint Undertaking; the successful abolition of roaming charges for EU citizens travelling within the EU, which has been effective since June 2017; and the coming into force of the (directly effective) Portability Regulation on 1 April 2018. However, the continued application of the Portability Regulation in the UK post-Brexit will require a reciprocal agreement with the EU. It remains to be seen how the UK government will deal with data roaming surcharges post-Brexit – it has published a note indicating that, in the absence of a deal with the EU, the government would legislate to retain the requirement on mobile operators to apply a financial limit on mobile data usage while abroad. The government has also published a note on the impact on telecoms businesses in the event there is no Brexit deal. The government states that if the European Electronic Communications Code is adopted prior to exit day, but with a deadline for transposition into national law post-Brexit, the government would ‘be minded to implement, where appropriate, its substantive provisions in UK law’.

VII CONCLUSIONS AND OUTLOOK

Recent years have seen privacy debates continued both inside and outside the courtroom, highlighting the ever-evolving regulatory landscape and the ongoing legal controversies about the scope and extent of a citizen’s right to privacy. The implementation of the GDPR has been a milestone in the area of data protection law, and companies continue to take steps to adjust their policies as the ICO’s and EU regulators’ approach to, and appetite for, enforcement become clearer. A close eye should also be kept on the developments of the Draft ePrivacy Regulation as it continues through the legislative process.

Following its fast-tracked introduction in 2014, the DRIPA legislation was declared incompatible with EU law on the basis that its data retention provisions violated the right of respect for private life and the protection of personal data, and its replacement, the IPA, will have to be amended in light of the UK High Court’s findings in R (Liberty).

An EU–US Privacy Shield is now in place to provide a legal basis for transfers of personal data to the US from the EU (replacing the Safe Harbor framework), but it is still the subject of further claims by privacy campaigners that it remains insufficient. Furthermore, standard contractual clauses are also being challenged in the courts.

With regard to the media and entertainment industry in the UK, the rise in popularity of SVoD services has led to announcements most notably from Apple and Disney with

intentions to launch their own streaming services to rival established players such as Netflix and Amazon. Apple TV+ is set to launch later in the year and Disney+ is set to launch in early 2020. These launches seem set to further alter the film and TV landscape in the UK.

Brexit will undoubtedly continue to have an influence on the policy and regulatory landscape in the UK and the EU27. The extent and nature of this will become clearer as more specific details emerge from the UK’s Brexit negotiations with the EU27.
Chapter 21

UNITED STATES

John P Janka, Matthew T Murchison, and Michael H Herman

I  OVERVIEW

This chapter provides an overview of telecommunications, broadband internet access and media regulation in the United States. Given the complexity of such regulation – which is constantly evolving in response to technological advances, market shifts and political dynamics – this chapter is not intended to be comprehensive. Rather, it is intended to demonstrate the nature and scope of such regulation, and to identify some of the more significant legal and policy developments of the past year.

II  REGULATION

i  The regulators

Regulation of telecommunications, broadband internet access and media in the United States is governed primarily by the following authorities, within parameters established under federal and state statutes and constitutions.

The Federal Communications Commission

The Federal Communications Commission (FCC) is an independent US regulatory agency established by the US Congress pursuant to the Communications Act of 1934, as amended (Communications Act). The FCC is charged with regulating all non-federal government use of the radiofrequency spectrum, all interstate telecommunications and all international telecommunications involving an end-point in the United States. Together with the US State Department Office of Communications and Information Policy, the FCC participates in international spectrum negotiations and related matters at the International Telecommunication Union (ITU).

The National Telecommunications and Information Administration

The National Telecommunications and Information Administration (NTIA) is an executive agency of the federal government within the US Department of Commerce. The NTIA has primary responsibility for regulating all use of the radiofrequency spectrum by federal government users, and works with the FCC to coordinate spectrum use between federal and non-federal users.

1  John P Janka and Matthew T Murchison are partners and Michael H Herman is an associate at Latham & Watkins LLP.
The Department of Commerce

The United States Department of Commerce (DOC) has oversight of remote sensing satellites and certain export issues related to space technology. The DOC is developing an increased role with respect to facilitating the commercialisation of space, including spectrum-related matters.

State and local regulators

Telecommunications within a single US state are governed by individual state regulatory agencies, typically having jurisdiction over telephone companies and other ‘public utilities’ providing services within the state, as well as over many consumer protection matters. State or local authorities typically issue franchises to operators of CATV systems whose service lines cross locally controlled, public rights of way. Such authorities also have jurisdiction over the siting of telecommunications facilities. The jurisdiction of state public utility commissions (PUCs) and of other state and local authorities over these types of matters is limited by state constitutions and statutes as well as by federal supremacy. For example, in the case of a conflict between the FCC and state or local regulations, the state or local regulation is typically pre-empted unless the US Congress or the FCC expressly permits state or local authorities to enforce their own regulations. The FCC has effectively exercised exclusive jurisdiction over most matters involving internet access services due to the interstate and international nature of the internet.

The Federal Trade Commission

The Federal Trade Commission (FTC) protects consumer interests in such areas as online marketing and telemarketing. Both the FTC and the FCC have oversight over certain telemarketing matters. Both the FTC and the US Department of Justice (DOJ) antitrust division police market concentration by examining mergers and other major transactions in the sector, along with the attorneys general of the 50 US states and the District of Columbia.

Other executive branch agencies

Other executive branch agencies play an important but less direct role in the regulation of traditional telecommunications, broadband internet access and media. First, these agencies often provide input as the FCC explores substantive issues and implements regulations through its rulemaking and licensing processes, occasionally engaging in public disagreements with the FCC over such matters. In addition, executive branch agencies with national security and law enforcement responsibilities typically are consulted (or may otherwise provide input) in connection with proposed transactions that would result in legally cognisable non-US ownership of FCC-regulated businesses. Notably, Team Telecom, an informal group made up of staff from the DOJ, the Federal Bureau of Investigation, the Department of Homeland Security and the Department of Defense, routinely participates in FCC proceedings, reviewing such transactions and often gathering additional information from the parties. Because the FCC typically will not consent to such transactions until Team Telecom has ‘signed off’, Team Telecom effectively has the power to delay, if not block, a transaction until its concerns are addressed. Transactions involving FCC-regulated businesses (like other US businesses) are also subject to potential review by the Committee on Foreign Investment in the United States (CFIUS), a multi-agency group with the statutory authority to review proposed investments in US businesses from non-US sources. Because CFIUS can
recommend that the President block or impose significant conditions on such transactions even after they have closed if they have not been ‘cleared’ by CFIUS, parties often file with CFIUS on a ‘voluntary’ basis prior to closing.

**ii Sources of federal telecommunications and media law and policy**

In the US, federal telecommunications law is derived principally from statutes enacted by Congress (and signed by the President) as well as administrative regulations, orders and policies adopted by the FCC.

**The Communications Act**

The FCC’s governing statute, codified in Title 47 of the United States Code, establishes the framework for federal regulation of traditional telecommunications, broadband internet access and media in the United States. The Communications Act consists of seven major sections, or ‘Titles’. The most significant of these are Title I (establishing the FCC and defining the scope of its authority), Title II (governing the activities of telecommunications carriers), Title III (governing the use of radio spectrum, including by wireless carriers and mass media broadcasters) and Title VI (governing the provision of cable television services). The Communications Act was substantially amended by the Telecommunications Act of 1996, which opened the US domestic market to greater competition in many respects.

**Ancillary authority**

Section 4(i) of the Communications Act provides that the FCC ‘may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions’. In a number of instances, the FCC has attempted to use this ‘ancillary authority’ to regulate subject matter outside the traditional scope of its jurisdiction (e.g., VoIP services).

**Forbearance authority**

Section 10(a) of the Communications Act enables the FCC to ‘forbear’ from applying any provision of the Act to a Title II ‘telecommunications’ carrier or service (but not other types of providers or services) if the FCC determines that enforcement of such provision is not necessary to ensure just, reasonable and non-discriminatory rates, terms and conditions of service; enforcement of such provision is not necessary for the protection of consumers; and forbearance from applying such provision is consistent with the public interest. The FCC has used this authority to free telecommunications carriers from restrictive common carrier regulations, particularly where the relevant market sector is competitive. The FCC also used this authority in early 2015 in connection with its reclassification of broadband internet access service as a ‘telecommunications service’ (discussed in greater detail below).

**FCC regulations and orders**

In fulfilling its statutory mandate, the FCC plays a quasi-legislative role by promulgating administrative regulations, after providing notice to the public and an opportunity for public comment, as required by the Administrative Procedure Act. The FCC also plays a quasi-judicial role in interpreting existing law in evaluating any number of disputes and
applications (e.g., licence applications or petitions for interpretation of the law). The resulting orders and regulations constitute an extensive body of administrative law governing telecommunications, broadband internet access and media in the United States.

Judge-made law

The judicial branch of the government also plays an important role in US lawmaking, at both the state and the federal level, reviewing administrative agency decisions for consistency with the governing statutes, and reviewing statutory law for compliance with the federal and state constitutions. Any party with a legally cognisable interest in the matter may seek review of an FCC action in a federal court of appeals. The courts review FCC decisions for consistency with its governing statutes and the US Constitution. In general, the FCC is entitled to deference in interpreting the Communications Act where it is ambiguous and capable of more than one reasonable interpretation. In addition, the courts review FCC decisions to ensure that they are not ‘arbitrary or capricious’: for example, the FCC may not depart from its own precedent without a reasoned basis for doing so, and more generally must have a reasoned basis for its decisions.

iii Regulated activities

Among other things, the Communications Act requires a party to obtain authority from the FCC prior to constructing or operating an ‘apparatus for the transmission of energy or communications or signals by radio’ or engaging in the provision of interstate or international telecommunications services. The specific procedures for obtaining such authority vary based on a number of factors, including the nature of the underlying authorisation, the nature of the proposed service, and the suborganisation of the FCC with primary responsibility for that service.

In most cases in which an applicant must file an application to obtain authority from the FCC, that application must be placed on ‘public notice’, giving interested parties an opportunity to comment during a specified period (e.g., 30 days). Certain types of applications (e.g., many non-common carrier wireless applications, requests for short-term authority or experimental licences) are subject to more streamlined processing, which may circumvent the need for public notice and comment in the first instance. Notably, the FCC now permits most applications to be filed electronically, and also allows the public to track the status of such applications through electronic filing systems (databases) accessible over the internet.

The FCC has granted certain types of operating authority by rule, obviating the need for individual users to seek and obtain separate authority from the FCC. For instance, the FCC has authorised by rule all common carriers to provide domestic interstate telecommunications services (this does not obviate the general need for wireless service providers to obtain separate spectrum licences, as discussed below) and, in certain cases, has eliminated the requirement to obtain authority before constructing radio facilities. The FCC has also permitted certain wireless operations to proceed on an ‘unlicensed’ basis, provided that the equipment used in such operations has been evaluated and authorised in accordance with the FCC’s procedures.
Ownership and market access restrictions

Foreign ownership restrictions

Sections 310(a) and (b) of the Communications Act restrict foreign ownership of common carrier, aeronautical and broadcast spectrum licences, and of US entities holding those licences. These statutory sections provide that foreign individuals and entities may not directly hold more than 20 per cent of the equity or voting interests in an entity that holds one of these types of FCC licences. Higher levels of indirect foreign ownership of a licensee are permissible where such ownership is held through US entities. More specifically, where the FCC licensee is owned and controlled directly by another US company, the 20 per cent limit effectively increases to 25 per cent, and the FCC may allow foreign ownership in excess of 25 per cent at or above the US parent company level where it determines that allowing such ownership would serve the ‘public interest’. In addition, as the result of a forbearance order issued in 2012 (which effectively overrides certain arcane language in the text of the Communications Act), the FCC will now permit higher levels of indirect foreign ownership in common carriers held through a non-controlling US company where the FCC concludes that such ownership would serve the ‘public interest’. Often, the FCC has permitted up to 100 per cent foreign ownership of common carriers. The FCC has found that higher levels of foreign ownership from WTO Member States presumptively serve the ‘public interest’.

Historically, the FCC generally has not waived the 25 per cent limit with respect to broadcast licensees. However, in late 2013, the FCC indicated that in order to facilitate foreign investment, it would consider such waivers on a case-by-case basis, taking into account any concerns raised by other executive branch agencies with respect to national security, trade policy and law enforcement. In May 2015, the FCC granted such a waiver to Pandora Radio LLC to allow Pandora to buy a radio station, and sustained that waiver against a legal challenge that was resolved in September 2015. In late 2016, the FCC extended to broadcast licensees the same standardised, streamlined rules and procedures that common carrier wireless licensees have been using to seek approval for foreign ownership, with appropriate broadcast-specific modifications. The FCC also established a methodology through which a publicly traded common carrier or broadcast licensee or controlling US parent could reliably ascertain its foreign ownership levels. The FCC has granted several requests seeking approval of foreign ownership in excess of the 25 per cent statutory limit.

Even transactions that are consistent with the foreign ownership limits described above may be scrutinised, and effectively blocked, as a result of a review by Team Telecom or CFIUS (as described above).

Market access

Generally, the FCC does not authorise facilities located entirely outside the United States to serve the US market. An exception arises with respect to non-US-licensed satellites, which may serve the US if the satellite is licensed by a non-US jurisdiction that permits US satellites to serve that jurisdiction without undue restrictions (such access is presumed where the non-US jurisdiction is a WTO Member State); the satellite complies with the same FCC technical and service requirements that apply to US satellites; and the satellite’s operation would not give rise to any national security, spectrum policy or other policy concerns. In reviewing requests for US market access, the FCC increasingly considers the extent to which the relevant non-US-licensed satellite enjoys ‘priority’ to the spectrum in question as a result of filings made by its licensing administration with the ITU.
Multiple or cross-ownership

With the exception of its broadcast licences, the FCC generally does not limit the number of spectrum licences that may be held by or ‘attributed’ to (i.e., deemed to be held by) a single individual or entity. However, in evaluating the likely competitive effects of significant wireless transactions, the FCC has utilised a ‘spectrum screen’ to identify local markets that merit closer scrutiny by looking at the total amount of spectrum that would be controlled by one individual or entity, and the FCC has initiated a proceeding to re-examine its use and definition of such spectrum screens. The FCC has also imposed certain limitations on the ability of authorised parties of one type to hold licences or authorisations of another type. For example, the FCC’s rules prohibit cable service providers from holding an attributable interest in the incumbent local exchange carrier serving the same market, and vice versa. The FCC has explicit limits on the number of broadcast stations (radio and TV) an individual or entity can own in a given local market, as well as the percentage of households nationwide that can be covered by television stations attributable to a single individual or entity. Historically, the FCC limited cross-ownership of radio and television stations, as well as cross-ownership of broadcast stations and newspapers. In November 2017, the FCC eliminated these restrictions. However, in September 2019, the United States Court of Appeals for the Third Circuit effectively reinstated the cross-ownership restrictions following a legal challenge, finding that the FCC had failed to consider the consequences of such deregulation on diversity in media ownership. The FCC is expected to revisit these issues, and any future revisions to the cross-ownership rules may face renewed judicial scrutiny.

v Transfers of control and assignments

Under Section 310(d) of the Communications Act, FCC approval must be obtained prior to assigning most types of radiofrequency-based licences, permits or authorisations from one party to another, or transferring ‘control’ of a holder of such radiofrequency authority from one party to another. Exceptions exist for certain pro forma transactions and certain types of licences. Similarly, under Section 214 of the Communications Act, FCC approval is required prior to assigning interstate or international telecommunications authorisations or transferring control of a US carrier that provides interstate or international telecommunications services. In reviewing such applications, the FCC typically attempts to gauge whether the application will serve the ‘public interest, convenience, and necessity’ by weighing the expected benefits of the proposed transaction against its expected harms, including the effects on competition and consumers. Most states have similar requirements applicable with respect to intrastate activities, and some require prior approval or notice regarding the issuance of debt by, or changes in the debt structure of, entities that are subject to their jurisdiction. State statutes sometimes require that other factors be considered as well, such as the expected effect on jobs in the state.

The time frames for obtaining FCC approvals in connection with mergers, acquisitions or other major transactions can vary widely. The FCC’s non-binding goal is to process combined applications for major transactions within six months. The FCC has exceeded this time frame on many occasions, typically when a transaction poses competitive concerns or is contested by third parties, in which case approval can take nine to 12 months, or possibly longer. More routine transactions are often processed in a shorter period, but there can be no assurance that the FCC will act by any deadline.

Since late 2018, the FCC has reviewed several major telecommunications and media transactions. Most notably:
In October 2019, the FCC approved applications seeking approval to transfer control of various licences and authorisations held by Sprint Corp (the nation’s fourth-largest wireless carrier) and its wholly owned subsidiaries to T-Mobile US, Inc (the nation’s third-largest wireless carrier). The proposed merger had already been approved by the DOJ, subject to divestitures of Sprint’s prepaid assets to DISH Network Corp in order to facilitate the direct-broadcast satellite (DBS) provider’s entry into the wireless market. Nevertheless, attorneys general of a number of states and the District of Columbia have filed a separate lawsuit challenging the transaction, which they contend would ultimately harm competition and consumers. As the time of writing, a trial in the states’ lawsuit is scheduled for December 2019 in the United States District Court for the Southern District of New York.

In September 2019, the FCC approved a series of applications seeking consent for the merger of Tribune Media Co with Nexstar Media Group, Inc (both American television conglomerates with numerous broadcast television licences). As a result of the transaction, in which Tribune survived as a wholly owned subsidiary of Nexstar, the combined entities own, operate, or manage nearly 200 television stations across the United States. Nexstar also acquired WGN America and a minority stake in Food Network, both cable networks with national audiences. To comply with FCC ownership rules, the parties divested a number of broadcast licences in various markets.

Several other transactions that are not currently subject to FCC review are also significant:

- The acquisition of Time Warner Inc (a large media and entertainment conglomerate in the United States) by AT&T Inc (a provider of video, broadband and voice services), while not subject to FCC review due to Time Warner’s pre-merger divestment of its FCC authorisations, remained subject to approval by the DOJ. In November 2017, the DOJ sued to block the transaction on antitrust grounds, but following a trial in June 2018, a district court ruled against the DOJ and allowed the acquisition to proceed. In February 2019, that decision was affirmed by the US Court of Appeals for the DC Circuit, and the DOJ subsequently announced that it would not pursue further appeals.

- In August 2019, Sinclair Broadcast Group, Inc (one of the largest television broadcast companies in the US) acquired 21 former Fox regional sports networks as well as Fox College Sports from The Walt Disney Co. Disney originally acquired the sports networks as part of its March 2019 purchase of Twenty-First Century Fox, Inc but was required to divest them as a condition of the DOJ’s approval of that transaction. In a separate deal consummated in March 2019, Sinclair acquired Disney’s interest in YES Network (another former Fox sports network) alongside the New York Yankees and several other investors.

### Enforcement

Violations of the Communications Act, the FCC’s implementing rules, orders and policies, and specific licence terms and conditions can result in enforcement proceedings before the FCC, and potentially before the DOJ. The FCC has explained that it intends to investigate and respond quickly to potentially unlawful conduct to ensure, among other things:

- that consumers are protected;
- robust competition;
- responsible use of the public airwaves; and
- strict compliance with public safety-related rules.
Violations of FCC requirements can result in a variety of sanctions, ranging from fines and forfeitures, to consent decrees designed to ensure corrective action; in egregious cases, criminal enforcement is possible. In recent years, the FCC has issued several multimillion-dollar fines, as well as a number of fines of several hundred thousand dollars each. The cited infractions include deceptive consumer practices, unauthorised operation of radio facilities, selling illegal equipment, violating the FCC’s ownership rules and providing materially incorrect information to the FCC.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol transmission

Before 2015, the United States used a relatively light touch with respect to the regulation of internet service providers (ISPs) and broadband internet access providers (BIAPs), relying largely on market forces instead of prescriptive regulation. By many accounts, this ‘hands-off’ approach contributed to the rapid growth of the US internet-based sector. Subsequent activity at the FCC – including, in particular, the agency’s imposition of net neutrality regulations and reclassification of retail broadband internet access services – suggested that it would play a more active role in the regulation of internet-based services. However, more recently the pendulum has swung in the other direction, with the FCC returning to a lighter touch with respect to internet access services (e.g., with respect to ‘net neutrality’ regulation).

ii Universal service

The Communications Act directs the FCC to take steps to facilitate the universal availability of essential telecommunications services through, inter alia, the use of a federal universal service fund (USF). The USF supports various programmes that seek to promote the availability of quality telecommunications services at just, reasonable and affordable rates on a nationwide basis to high-cost areas, low-income individuals, schools, libraries and rural healthcare facilities. The USF is funded through revenue-based contributions from providers of interstate and international telecommunications and interconnected VoIP services, as well as certain other providers of ‘telecommunications’. The contribution factor (essentially, that rate at which interstate and international revenues are assessed for USF contribution purposes) varies during the course of the year, and has fluctuated between approximately 19 and 25 per cent of covered revenues for most of 2019. Universal service programmes and contribution obligations are administered by the Universal Service Administrative Company, a legally independent entity that is subject to the FCC’s oversight.

The National Broadband Plan recommends that the FCC modify existing universal service subsidy programmes to target broadband expansion into areas where the FCC asserts BIAPs would not find it economically viable to provide broadband service in the absence of this type of financial support. Consistent with this recommendation, the FCC has established the Connect America Fund (CAF) to support the deployment of broadband infrastructure to areas that are currently ‘unserved’, and to phase out legacy universal service support mechanisms in the process. Under the FCC’s implementing rules, certain wireline incumbents called ‘price cap carriers’ enjoy significant funding preferences through, inter alia, a ‘right of first refusal’ in connection with available funding. As a result, a much smaller pool of support is available to competitive providers. The FCC, which is currently implementing Phase II of the CAF programme, held a reverse-auction in July and August 2018 to distribute funding in areas where price-cap incumbents declined preferential funding. In the auction,
more than 103 bidders were awarded more than US$1.49 billion of support to offer service to more than 700,000 locations in 45 states over the next decade. Over the course of 2019, the FCC began disbursing funds to the reverse-auction’s winning bidders. In addition, the FCC is implementing CAF rules for ‘rate of return’ incumbent carriers. These changes are being coupled with changes to the existing – and exceedingly complex – ‘intercarrier compensation’ scheme by which local and long-distance service providers pay or receive compensation for traffic that is handed off to each other’s networks.

In August 2019, the FCC proposed the establishment of a new Rural Digital Opportunity Fund (RDOF). Modelled after the CAF programme, the RDOF would provide approximately US$20 billion over a 10-year period to support deployment of broadband service with minimum speeds of 25/3Mbps in rural areas, with the goal of improving connectivity for millions of Americans. The FCC also is continuing to develop other mechanisms and seek additional funding to extend broadband service to the most remote and hardest to serve locations in the United States.

The FCC also has a ‘Lifeline’ programme, which uses a portion of the USF to subsidise the costs of certain supported telecommunications services so that they can be purchased by individuals who otherwise would be unable to afford them. Broadband is included in the list of supported services, providing low-income consumers a means of obtaining internet access at reduced rates. Minimum standards exist for supported voice and broadband services in order for a service to qualify for the Lifeline subsidy. In November 2017, the FCC proposed modifications to Lifeline that would, among other changes, limit the ability of resellers (service providers that lease, rather than own, network capacity) to participate in the programme. Opponents challenged the new rules in the United States Court of Appeals for the District of Columbia Circuit, which, in February 2019, rejected these recent changes and remanded the matter to the FCC for reconsideration.

### iii Restrictions on the provision of service

**Common carriage**

The Communications Act subjects all providers of ‘telecommunications services’ to common carrier regulation (e.g., the duty to provide service to all members of the public, including other carriers, without unreasonable discrimination). ‘Telecommunications services’ are defined to include the provision of ‘telecommunications’ to the public for a fee. ‘Telecommunications’, in turn, are defined to include the transmission, between or among points specified by the user, of information of the user’s choosing without change in the form or content of the information as sent and received. Notably, this definition does not encompass the creation or publication of mere ‘content’. Traditional telecommunications carriers tend to be heavily regulated by both the FCC and the state PUCs.

In contrast, ‘information services’ are defined to include the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilising or making available information via telecommunications. These services typically involve what is called a ‘net protocol conversion’ – essentially, a change in the form, structure or substance of the underlying communication. Providers of ‘information services’ are not subject to common carrier regulation and traditionally have been lightly regulated at the federal level. State and local jurisdiction over internet services is severely circumscribed, as the services are considered ‘interstate’ for most purposes.

As communications technologies have continued to evolve, the lines between ‘telecommunications services’ and ‘information services’ have blurred, and the FCC has
been slow to classify new service offerings. The FCC thus far has declined to classify VoIP services, creating uncertainty as to which regulations apply at both the federal and state levels. This uncertainty has been exacerbated by the FCC’s attempted use of its ‘ancillary’ authority to extend a number of common carrier-type requirements to such otherwise-unregulated services.

Because the classification of a service is of critical importance in determining the regulations applicable to that service, the reclassification of a service can have significant consequences. The FCC’s treatment of internet access services provides a vivid illustration of this fact. Broadband internet access services require, inter alia, the transmission of data between an end user and an ISP, and any number of other individuals or entities. For years, the FCC viewed this transmission capability as a ‘telecommunications service’, and required BIAPs to offer it to competitors on a stand-alone, common carrier basis. However, in a series of orders issued during the 2000s, the FCC reclassified broadband internet access services as ‘information services’ functionally integrated with a ‘telecommunications’ component, such that BIAPs are no longer required to make the transmission capability available to competitors (unless that capability is offered to the public voluntarily on a non-integrated, stand-alone basis).

The classification of broadband internet access service has remained an area of significant regulatory interest. In February 2015, the FCC reclassified retail broadband internet access service as a ‘telecommunications service’ as part of the FCC’s ‘net neutrality’ proceeding. This action was taken for the stated purpose of creating a clearer jurisdictional basis for the imposition of net neutrality rules on BIAPs, though it also automatically subjected BIAPs to various common carrier provisions appearing in Title II of the Communications Act, including privacy-related obligations. However, in January 2018, the FCC restored its prior classification of broadband internet access service as an ‘information service’, in conjunction with the FCC’s repeal of certain of those net neutrality rules, and in doing so also relieved BIAPs of Title II’s privacy obligations and other common carrier requirements. Appeals of the FCC’s 2015 decision accordingly became moot, though the 2018 order was appealed to the United States Court of Appeals for the District of Columbia Circuit. In October 2019, the DC Circuit upheld the majority of the FCC’s 2018 order, including its classification of broadband internet access service as an ‘information service’ exempt from the requirements imposed on common carriers under Title II.

**Price regulation**

The Communications Act gives the FCC the authority to regulate the rates charged by common carriers in connection with the telecommunications services they provide, and ensure that those rates are ‘just and reasonable’. Prior to the passage of the Telecommunications Act of 1996, rate regulation was accomplished through the filing of tariffs with the FCC and state PUCs. More recently, the FCC has eliminated much of its tariffing regime and instead relied upon market competition (backed by a complaint mechanism) to ensure that rates are ‘just and reasonable’.

In other respects, the FCC has taken steps toward the re-regulation of certain services that are critical inputs to broadband services. In 2016, the FCC found that certain incumbents were abusing their market power and charging unreasonably high rates for the broadband ‘special access’ services necessary for ‘business data service’ firms to function and serve their customers. The FCC subsequently proposed and adopted a new regulatory framework for such special access services in which individual geographic markets are classified as either
‘competitive’ or ‘non-competitive’, with the former subject to relatively lower levels of new regulation, and the latter subject to more onerous requirements and oversight. The new rules went into effect in August 2017 and were upheld in nearly all respects by the Eighth Circuit Court of Appeals in a ruling issued in August 2018.

The FCC also has taken a hands-on approach to the regulation of franchise fees that municipalities can charge CATV operators (which often offer broadband and voice services in addition to video service). By statute, such fees cannot exceed 5 per cent of the revenues that a CATV operator derives from providing video service in the municipality. In August 2019, however, the FCC clarified that the value of ‘in-kind exactions’ (e.g., services that CATV operators may be asked to provide without charge to government buildings and schools) count towards the 5 per cent cap.

**Net neutrality**

In recent years, one of the most significant policy debates at the FCC has focused on an ‘open internet policy’ or ‘net neutrality’. Although the meaning of ‘net neutrality’ is itself a subject of debate, net neutrality advocates generally aim to constrain the rights of broadband network providers to block, filter or prioritise lawful internet applications, websites and content.

The FCC’s direct involvement with a net neutrality policy began in 2005 with the issuance of its Broadband Policy Statement. Although the FCC’s authority under the Communications Act to regulate the internet was not clearly articulated, the Broadband Policy Statement expressed four principles that the FCC indicated were intended to preserve the ‘open’ nature of the internet for consumers, without discouraging broadband deployment by network operators. All subject to a service provider’s right to engage in ‘reasonable network management’, the FCC stated that consumers are entitled to gain access to the lawful internet content of their choice; run applications and use services of their choice, subject to the needs of law enforcement; connect their choice of legal devices that do not harm the network; and benefit from competition among network providers, application and service providers and content providers.

In 2008, the FCC ruled that Comcast Corp, the largest US CATV company, had violated the Broadband Policy Statement by inhibiting users of its high-speed internet service from using BitTorrent and other file-sharing software, a practice Comcast claimed was a type of ‘reasonable network management’ designed to block pirated content and alleviate network congestion. Comcast appealed this decision, arguing, inter alia, that the FCC lacked the statutory authority to adopt or enforce net neutrality requirements. In early 2010, a US court of appeals agreed with Comcast and vacated the FCC’s order. In doing so, the court rejected the FCC’s attempt to rely on its ‘ancillary’ authority as a basis for its enforcement of the Broadband Policy Statement against Comcast, insofar as the FCC had failed to identify a source for such authority in the Communications Act.

The FCC then adopted new rules on broadband internet access services, applicable only to ‘mass-market retail services’. Those rules required all broadband internet access service providers to disclose the network management practices, performance characteristics and terms and conditions of their services; prohibited fixed broadband internet access providers from blocking lawful content, applications, services or non-harmful devices; prohibited mobile wireless broadband internet access providers from blocking lawful websites or applications that compete with their voice or video telephony services; and prohibited fixed broadband internet access providers from unreasonably discriminating in transmitting lawful network traffic. In 2014, the US Court of Appeals for the District of Columbia Circuit
vacated the FCC’s ‘anti-discrimination’ and ‘anti-blocking’ rules, finding that they amounted to impermissible common carrier regulation of internet access services, since the FCC had classified those services as ‘information services’ not subject to Title II of the Communications Act (the Court upheld the FCC’s disclosure requirements). However, the Court also suggested that the FCC could adopt modified versions of these rules under Section 706 of the Telecommunications Act of 1996, which potentially grants the FCC relatively broad authority to promote the ‘virtuous circle’ of internet-related innovation.

In May 2014, the FCC launched a new rulemaking to explore whether new ‘net neutrality’ rules could be adopted pursuant to Section 706, or whether the FCC instead should regulate BIAPs as ‘Title II’ common carriers. In 2015, the FCC opted for the latter approach, reclassifying retail broadband internet access service as a ‘telecommunications service’ subject to Title II. At the same time, the FCC exercised its forbearance authority to free BIAPs from much of the regulation that otherwise would apply under Title II (such as tariffing obligations and mandatory federal universal service contributions). Notably, several core common carrier regulations continue to apply notwithstanding such forbearance, including statutory requirements that ‘charges’ and ‘practices’ be just, reasonable and not unreasonably discriminatory; requirements to maintain the privacy of customer information; and the right of consumers to seek damages and pursue complaints in courts for claimed violations by common carriers. Soon after the FCC’s ruling, a broad coalition of BIAPs and trade associations filed an appeal in the US Court of Appeals for the District of Columbia Circuit. That court upheld the FCC’s ruling in a decision issued in June 2016, and the US Supreme Court ultimately denied further review in November 2018.

In January 2018, the FCC revisited these issues yet again, this time restoring the classification of broadband internet access service as an ‘information service’ and repealing its 2015 bans on blocking, throttling and paid prioritisation as well as its general ‘internet conduct standard’. In place of these prophylactic rules, the FCC adopted a revised transparency rule requiring BIAPs to disclose any blocking, throttling or paid prioritisation on their networks. The FCC also entrusted the FTC with the task of bringing enforcement actions for ‘unfair and deceptive practices’ if BIAPs violate their own stated commitments not to engage in such conduct, and for ‘unfair methods of competition’ if BIAPs otherwise engage in anticompetitive conduct. An appeal of this order was brought by a group of public advocacy organisations, internet content providers and state attorneys general in the US Court of Appeals for the District of Columbia Circuit.

In an opinion issued in October 2019, the DC Circuit upheld the majority of the FCC’s 2018 order, including its classification of broadband internet access service as an ‘information service’. The court did, however, remand three discrete issues to the FCC for further review: the potential impacts of the order’s deregulatory reforms on public safety, pole attachments and BIAPs’ participation in the Lifeline programme. The DC Circuit also vacated the 2018 order’s express pre-emption provision, although it left room for challenges to state net neutrality laws based on conflict pre-emption principles. At the time of writing, it is unknown whether the parties to the appeal will seek a rehearing by the DC Circuit or review by the US Supreme Court.

In the aftermath of the 2018 order, several states have attempted to establish their own net neutrality requirements for BIAPs, in the form of either direct regulation (e.g., California’s SB-822) or conditions on government procurement contracts (e.g., Vermont’s EO 2-18 and S-289). The federal government and BIAPs sued to block California’s net neutrality law on pre-emption grounds in September 2018, leading to a concession by the
state not to enforce the law while the appeal of the FCC’s 2018 order was pending. BIAPs brought a similar lawsuit in Vermont in October 2018, which also was stayed pending the resolution of the appeal.

iv Security

**US regulatory approach to emergency preparedness**

Because US commercial communications networks are privately owned, the FCC’s role in ensuring emergency preparedness primarily is one of gathering and disseminating information and coordinating among different governmental agencies. Facilities-based telecommunications service providers participate in industry-run working groups focused on developing best practices to ensure network reliability, to report network outages and to be prepared to restore network services as rapidly as possible in the event of an outage. The recommendations of these groups do not have the binding force of law, but have played an important role in shaping industry practice and have prompted some limited FCC rulemaking activity. For example:

a FCC rules now require all wireline and wireless telecommunications service providers to maintain on site a back-up power source (typically, a generator) capable of keeping networks functioning for a minimum number of hours. In addition, FCC rules require providers of fixed residential voice services (including interconnected VoIP) to offer customer premises equipment along with a backup power source.

b Under the Telecommunications Service Priority (TSP) programme, service providers must afford priority service to federal, state and local governments and other critical institutions.

c The FCC has adopted outage reporting rules that require network operators to notify the FCC of significant outages that may impact end-user communications, and recently extended these rules to VoIP providers.

d The FCC has established rules governing the Emergency Alert System (EAS), a national public warning system that requires broadcasters, CATV operators, satellite broadcasters and others to provide communications capability to the President to address the American public during a national emergency. The system may also be used by state and local authorities to deliver important emergency information, such as AMBER alerts and weather information targeted to specific areas.

e The FCC has established rules requiring deployment of enhanced 911 services with the aim of providing accurate and precise caller location data to facilitate a rapid and effective emergency response.

The FCC is also responsible for the emergency preparedness of US network operators, the radiofrequency spectrum needs of non-federal ‘first responders’ (police, fire, ambulance and emergency medical teams) and coordination among network operators and various governmental organisations to address cybersecurity concerns. Much of this activity has focused on ensuring adequate spectrum for public safety users, and ensuring the interoperability of different public safety networks.

Congress has authorised the creation of a nationwide, interoperable, high-speed network dedicated to public safety applications. This network is being managed by FirstNet, an independent entity within the NTIA that is overseen by a board including representation from the public safety community, wireless experts and current and former federal, state and local government officials. Notably, a significant portion of FirstNet operations is funded by the proceeds of spectrum auctions.
The Communications Assistance for Law Enforcement Act

Communications Assistance for Law Enforcement Act (CALEA) requires ‘telecommunications carriers’ to implement specific capabilities in their networks to permit law enforcement agencies to intercept call identifying information and call content pursuant to a lawful authorisation. For this purpose, the term ‘telecommunications carriers’ is defined broadly to include interconnected VoIP providers as well as facilities-based BIAPs. CALEA establishes both minimum capacity requirements and capability requirements. CALEA does not specify the means by which providers must comply with these capability requirements, but creates a safe harbour for carriers that implement industry standards. CALEA does not grant law enforcement agencies any surveillance authority beyond what otherwise exists under US law.

Cybersecurity

US cybersecurity policy following the completion of the federal government’s Cyberspace Policy Review has sought to:

a create or enhance shared situational awareness of network vulnerabilities, threats and events and the ability to act quickly to reduce current vulnerabilities and prevent intrusions;
b enhance US counterintelligence capabilities and increase the security of the supply chain for key information technologies; and
c strengthen the future cybersecurity environment by expanding cyber education, coordinating and redirecting research and development efforts and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

Consistent with these goals, the FCC has explained that one of its core objectives is ‘to strengthen the protection of critical communications infrastructure’. In advancing this objective, the FCC has focused on educating consumers and small businesses about the importance of cybersecurity, developing cybersecurity best practices in cooperation with industry leaders and facilitating the ability of small businesses to develop their own cybersecurity plans.

Online protections for children

The Children’s Online Privacy Protection Act of 1998 restricts the ability of website operators to collect personal information from children under 13 years of age. The type of ‘verifiable parental consent’ that is required before collecting and using information provided by children under 13 is based upon a ‘sliding scale’ set forth in an FTC regulation that takes into account the manner in which the information is being collected and the uses to which the information will be put. While children under 13 can legally give out personal information with their parents’ permission, many websites disallow underage children from using their services due to the regulatory burdens involved.

Protection of personal data and privacy

The Communications Act protects the privacy of ‘customer proprietary network information’, which includes the date, time, duration and location of a call, type of service used and other details derived from the use of a telecommunications service. US law also protects the contents of any telecommunications message from eavesdropping, recording, use or disclosure by a third party without a user’s consent. Users of online services enjoy similar protection from
United States

eavesdropping or disclosure of their communications. Exceptions apply where access to, or use or disclosure of, such information is necessary for law enforcement, which in most cases requires prior approval by a judge. In addition, the NTIA has formed an Internet Policy Task Force, which has recommended the adoption of voluntary codes of conduct by industry participants, and continues to examine ‘the nexus between privacy policy and innovation in the Internet economy’.

Notably, this legal framework is targeted at carriers and other private actors, as opposed to the government. However, in 2013 it was the policies and practices of the latter that prompted the most significant privacy concerns, and added fuel to the ongoing debate over how much privacy should be sacrificed by individuals in the name of national security. The controversy erupted in June 2013 when the British newspaper *The Guardian* published a series of exposés containing information leaked to it by Edward Snowden, who had been employed as a contractor for the US National Security Agency (NSA). More specifically, Snowden disclosed classified information regarding NSA surveillance programmes, including NSA efforts to compile a database containing the metadata for hundreds of billions of telephone calls made through the largest US carriers and collect stored internet communications from large internet companies like Google. While some of these activities apparently were authorised by special courts established under the Federal Intelligence Surveillance Act, the activities of these courts are not subject to public scrutiny and have been criticised as little more than a rubber stamp for proposed executive branch activities.

The FCC has also tried to ensure that consumers can effectively block calls and text messages that they do not wish to receive, using authority provided by Congress in the Telephone Consumer Protection Act (TCPA). Among other things, in June 2015 the FCC attempted to strengthen restrictions on the practice of ‘robocalling’ using ‘automatic telephone dialling systems’ (i.e., ‘autodiallers’) by issuing a series of declaratory rulings. Among other things, the FCC ruled that a device is an impermissible autodialler if it had either the present ability or potential future ability to be used to store or produce telephone numbers to be called, using a random or sequential number generator, and to dial such numbers. Numerous parties sought review of this ruling in the US Court of Appeals for the District of Columbia Circuit, arguing, among other things, that the FCC’s action actually obfuscates matters and unreasonably expands the reach of the TCPA, because, for example, a smartphone could be classified as an impermissible autodialler simply because it could use an autodialling application. In March 2018, the court struck down the FCC’s autodialler ruling and other aspects of the 2015 order, and in May 2018, the FCC opened a new proceeding to consider reforms to its implementation of the TCPA in light of the court’s ruling. In tandem with such efforts, the FCC has taken steps to facilitate voice service providers’ identification and blocking of illegal and unwanted robocalls. For example, in June 2019, the FCC issued a declaratory ruling permitting voice service providers to offer call-blocking functionality to their subscribers on an ‘opt-out’ basis. Moreover, many of the nation’s largest carriers have committed to implementing SHAKEN/STIR, an end-to-end call authentication protocol aimed at curtailing unwanted ‘spoofed’ robocall traffic travelling on and among their networks, by the end of 2019.
IV SPECTRUM POLICY

i Flexible spectrum use

In recent decades, the FCC increasingly has adopted a flexible approach to defining the uses to which a particular radiofrequency band may be put, or the optimal scope of licences that an entity can use to meet its business needs. For example, the FCC has granted many licensees (but not broadcasters) flexibility to redefine their own service territory, dividing or combining geographically bounded licences, and to subdivide their assigned spectrum and sell or lease a portion to another user. The FCC has also adopted more fluid service definitions – for example, permitting fixed and mobile operations, or terrestrial and satellite operations – in the same band.

The FCC has been examining ways to increase flexibility and efficiency in the use of available spectrum resources. It has recognised that one key failing of its spectrum policy is that administrative rigidities historically have prevented more efficient use of the spectrum resource. As a result, the FCC’s spectrum policy has evolved towards more flexible and market-oriented regulatory models.

For example, to facilitate the development of secondary markets in spectrum usage rights involving terrestrial radiofrequency-based services, the FCC has adopted rules to facilitate two types of leasing arrangements: a ‘spectrum manager’ lease, in which a lessee is permitted to use spectrum subject to the oversight and control of the initial licensee; and a ‘de facto transfer’ lease, in which the lessee assumes many of the obligations of a licensee, and exercises control over its own spectrum operations. The FCC has also examined ways to facilitate unlicensed use of certain spectrum bands, provided that such use does not interfere with licensed operations (if any) in those bands. Among other things, the FCC has adopted rules permitting certain devices to operate on a secondary, unlicensed basis in unused broadcast television spectrum, also known as ‘white spaces’, and has sought to facilitate the ability of unlicensed Wi-Fi networks to share portions of the 5GHz band that previously were designated for other purposes.

ii Broadband and spectrum use

Federal law and policy has sought to encourage the growth of broadband networks, including through access to additional spectrum. More specifically, Congress has directed the FCC and the NTIA to make additional federal government spectrum available for commercial use. The FCC and the NTIA are also exploring ways that commercial users might share federal government spectrum.

The FCC has also identified existing commercial spectrum that could be reallocated and thus used more efficiently in support of broadband services. After Congress enacted legislation that allowed television broadcasters to ‘turn in’ some of the spectrum they use for their television channels in return for a portion of auction proceeds, the FCC conducted its first ‘incentive auction’. The auction of the voluntarily returned broadcast channels for new mobile broadband use yielded US$19.8 billion in revenue, including more than US$7 billion for the government.

In addition, the FCC has continued work in its ‘spectrum frontiers’ proceeding, which seeks to make additional spectrum above 24GHz available for ‘5G’ wireless mobile and other broadband services. In a second phase of this proceeding, the FCC made available 1,700MHz of millimetre-wave spectrum for flexible wireless use, in the 24.25–24.45 and 24.75–25.25GHz band (24GHz band) and the 47.2–48.2GHz band. This is in
addition to the 27.5–28.35GHz, 37–38.6GHz, 38.6–40GHz and 64–71GHz bands that the Commission previously made available for flexible wireless use. The FCC has begun auctioning off terrestrial usage rights for this spectrum; in January 2019, for instance, the FCC completed its auction of terrestrial rights to the 27.5–28.35GHz band, which raised over US$700 million and resulted in the grant of new licences to dozens of winning bidders in October 2019. The FCC also enabled the millimetre wave bands to be used for a variety of other uses, including satellite, fixed and federal government uses. The FCC targeted the 40–42GHz and 48.2–50.2GHz bands for expansion of fixed satellite service, and adjusted previously adopted earth station requirements in the 28GHz and 39GHz bands to permit greater flexibility in the deployment of earth stations. This expanded on the FCC’s prior decision, which allowed the deployment of over 9,000 individually licensed earth stations on an interference-protected basis in the 27.5–28.35GHz band, and committed to consider allowing ubiquitously deployed satellite user terminals access to 27.5–28.35GHz in light of ‘the evolving nature of technology and deployment’ in this band segment. The FCC also provided for expanded unlicensed use of the 57–71GHz band on-board aircraft.

With respect to broadband service on aircraft, as well as on as ships and vehicles, the FCC adopted new rules to better enable satellite-delivered connectivity to passengers and crew. The FCC allowed so-called ‘earth stations in motion’ to operate in more satellite frequencies than before, in an effort to connect even more consumers in this fast-growing segment of the marketplace and provided more certainty be adopted a simplified, regulatory framework for licensing these spectrum uses. Pending before the FCC is also an inquiry into potential ways to facilitate more intensive use of the frequencies between 3.7GHz and 24GHz.

There also have been a number of other new developments with respect to satellite spectrum policy. The DOC has expressed plans to simplify aspects of the existing commercial licensing regime and also to develop radio spectrum policies to serve the needs of the commercial industry. In addition, the President has issued a number of space policy directives, which require, among other things, that the DOC and the Director of the Office of Science and Technology Policy at the White House provide to the President a report on improving the global competitiveness of the US space sector through radio frequency spectrum policies, regulation and US activities at the ITU and other multilateral forums.

iii Spectrum auctions and fees

Where spectrum is to be assigned to an individual licensee, and more than one party applies to use such spectrum (i.e., mutually exclusive applications are received by the FCC), the FCC may choose from several mechanisms under the Communications Act by which to designate the ‘winning’ licensee. Most new spectrum assigned since 1993 has been licensed through the use of competitive bidding (i.e., spectrum auctions). The statute excludes certain specific types of spectrum licences (international satellite, public safety, non-commercial broadcast, etc.) from the scope of the FCC’s auction authority. The FCC has completed over 100 radiofrequency spectrum auctions to date.

Historically, proceeds from all spectrum auctions have gone to the US treasury. Under the recently used incentive auction (described above), current licensees have the option to contribute spectrum rights in exchange for a portion of the proceeds from the auction of that spectrum.
V MEDIA

i Regulation of media distribution outlets generally

The regulation of media distribution outlets and content varies depending on the business model and technology being used. As previously noted, internet-based content delivery is very lightly regulated in the US. Traditional media outlets historically have been regulated more heavily by the FCC.

Regulation of content and content providers

The First Amendment to the US Constitution guarantees the freedom of speech, and limits the ability of the government to regulate the content of a broadcaster’s programming, or content providers directly. Several decades ago, the courts recognised the FCC’s authority to prohibit ‘indecent’ programming by free, over-the-air broadcasters, based on the government’s interest in ensuring that scarce spectrum rights are used in a manner that serves the public interest, and the unique pervasiveness of broadcast media in the lives of Americans and their children. As discussed below, those rules do not apply to the CATV and satellite video and audio service providers whose coverage extends throughout the US. It is unclear whether the FCC’s rules remain constitutional in today’s media-rich market where many different media outlets serve the same household.

In recent years, the FCC has fined stations that aired ‘fleeting expletives’ (incidental words or gestures that are broadcast despite the reasonable precautions taken by the licensee to avoid indecent broadcasting). For example, in 2006 the FCC fined affiliates of the ABC and Fox networks millions of dollars for airing such material during their programming. Both networks subsequently challenged these fines in the courts. In June 2012, the US Supreme Court invalidated the fines on due process grounds, finding that the FCC had not fully articulated its rule against fleeting expletives until after the programmes in question had been aired. In taking this approach, the Court left open broader questions as to whether the FCC’s ‘fleeting expletives’ policy violates the First Amendment or otherwise is unconstitutional.

Terrestrial broadcasting

Television and radio stations broadcasting video content for free to listeners and viewers via terrestrial radiofrequency spectrum are subject to extensive regulation by the FCC, which has exclusive licensing authority over such stations in the United States. Among other things, the FCC has adopted detailed technical rules governing this type of broadcaster, restricted their ability to air ‘indecent’ programming, imposed political broadcasting and other ‘public interest’ obligations on them and adopted multiple ownership restrictions. These regulations are largely premised on the idea that radiofrequency spectrum is a scarce resource, and thus the FCC should promote localism, diversity of ownership and service in the public interest.

Subscription media

Entities providing electronic media services by subscription – CATV, DBS service, subscription radio or even subscription over-the-air TV stations – generally are subject to less restrictive content regulation than terrestrial ‘free over-the-air’ broadcasters (‘obscene’ material is prohibited, but not material that is merely ‘indecent’). Because subscribers pay for their service, by definition, arguments that they must be protected from unwittingly accessing ‘indecent’ content are less convincing. Subscription satellite radio providers and multichannel video programming distributors (MVPDs), such as DBS and CATV providers,
remain subject to FCC regulation with respect to their use of radiofrequency spectrum and certain other matters. Moreover, terrestrial CATV operators are also subject to franchising by state or local authorities for the use of public rights of way.

**Carriage of broadcast television programming by MVPDs and other parties**

When Congress imposed a variety of obligations on cable operators with respect to their carriage of local broadcast television signals in 1992, it was concerned that the MVPD industry posed a threat to broadcast TV stations (given better transmission quality, greater choice of programming, etc.). Congress was also concerned that MVPDs would become the predominant means of distributing video programming to consumers, and then could use that market position to preclude local broadcasters from reaching those consumers effectively.

To address this concern, Congress established a statutory framework allowing each over-the-air TV station, on a local-MVPD-by-MVPD-basis, to elect either ‘must carry’ status (ensuring mandatory carriage on an MVPD serving the local market of that station) or ‘retransmission consent’ (requiring an MVPD to obtain the station’s consent before carrying its signal). This new right supplemented the compulsory copyright licence established in the Copyright Act, under which content owners receive a statutory fee from MVPDs in connection with their retransmission of broadcast signals, but MVPDs do not need the consent of those content owners.

Initially, most local broadcasters were unable to negotiate cash compensation in exchange for granting ‘retransmission consent’ to MVPDs; at best, they typically were able to negotiate ‘in kind’ deals, such as commitments from MVPDs to purchase advertising time. More recently, local broadcasters have begun to demand cash compensation, and many have indicated they would withhold ‘retransmission consent’ from an MVPD unless they are paid for the carriage of their signal. For example, in 2013, the CBS network declined to extend its grant on retransmission consent on existing terms, and carriage of that network on a major MVPD was disrupted in a number of major US markets for several weeks. However, in March 2014, the FCC took action that increased MVPDs’ bargaining position somewhat; specifically, the FCC revised its rules to preclude the joint negotiation of ‘retransmission consent’ agreements by multiple broadcast television stations that are ranked among the top four stations in a local market and not commonly owned. The FCC explained that such action was necessary to ensure that broadcasters did not enjoy undue leverage in such negotiations. Nevertheless, disputes between MVPDs and broadcasters continue, and the FCC occasionally is called upon to adjudicate claims of ‘bad faith’ retransmission consent negotiations.

In addition to the ‘retransmission consent’ requirements described above, any party that retransmits broadcast programming must comply with US copyright law. Federal law creates compulsory licences allowing ‘cable systems’ and other MVPDs to retransmit such programming without obtaining specific licences from every relevant copyright holder in the programming stream. Other types of services do not benefit from this compulsory licence and must respect relevant copyright, as the US Supreme Court confirmed in June 2014 when it released its decision in *American Broadcasting Cos v. Aereo, Inc*, which involved a service that leased each subscriber an individual remote antenna that allowed that subscriber to receive broadcast signals and retransmit that signal over the internet for near-live viewing. The Court concluded that Aereo’s retransmission of these signals constituted a ‘public performance’ of programming material that infringed on the rights of the copyright holders. The Aereo decision does not address how US copyright law could apply to other ‘retransmission’ services
on a going-forward basis, and in particular does not fully resolve whether modest changes to the structure of an Aereo-like service (e.g., recording programming for later viewing instead of engaging in near-live retransmission) would change the outcome. Relatedly, a non-profit entity called Locast launched a service in 2018 that allows users to stream local broadcast television stations in exchange for voluntary donations, relying on an exception in the retransmission consent regime for governmental and non-profit entities seeking to retransmit signals with no desire for ‘commercial advantage’. In July 2019, a number of programmers and broadcasters filed suit against Locast, challenging its non-profit status and alleging violation of US copyright laws; Locast, for its part, has filed counterclaims alleging that the plaintiffs are misusing their copyrights and are engaged in anticompetitive behaviour. The dispute has not yet been resolved.

ii Internet-delivered video content

The regulatory status of internet-delivered video content turns in part on whether it can be considered ‘video programming’ under the Communications Act. This term encompasses ‘programming provided by, or generally considered comparable to programming provided by, a television broadcast station’. Much online video content does not fall into this category, and as such lies outside the FCC’s jurisdiction.

Also significant is the manner and form in which ‘video programming’ is delivered to the viewer. ‘Video programming’ may be subject to minimal regulation if it is incorporated into an ‘information service’ by virtue of the use of the internet or other broadband technologies as a delivery mechanism. Moreover, the FCC has identified a category of ‘interactive television’ services – defined as ‘a service that supports subscriber-initiated choices or actions that are related to one or more video programming streams’ – but it has not decided what requirements, if any, should apply to such services. The manner in which these classification issues are resolved can have significant implications in other regulatory areas. For example, IP-delivered video programming in the form of a traditional cable service arguably falls outside the scope of the FCC’s net neutrality rules. Notwithstanding general uncertainty with respect to the regulatory status of internet-delivered video content, IPTV services delivered by telecommunications companies have been subject to franchising as ‘cable’ systems under some state and local requirements. To expedite competitive entry into the IPTV market, and to facilitate competition to entrenched CATV operators, several states have adopted state-wide franchising, and have pre-empted separate approval requirements in individual municipalities. The FCC encourages rapid approval of competitive franchising requests and has indicated that it may pre-empt states that do not promptly act on such requests.

iii Mobile services

Consumer demand for access to audio and video programming through mobile platforms is one of the primary drivers of increased demand for mobile broadband access generally. As noted above, the National Broadband Plan aims to free additional spectrum resources for such services. The advent of these services, many of which would not use ‘broadcast’ spectrum, reflects increasing convergence in the communications industry, and could lead to increased pressure to reconcile regulatory frameworks that treat similar services differently.
VI CONCLUSIONS AND OUTLOOK

The FCC continues to focus its regulatory efforts on broadband-related matters, and recent developments have carried on the recent trend toward deregulation of BIAPs. The FCC has continued its efforts to free additional spectrum for wireless broadband operations, both on a licensed and unlicensed basis, to facilitate continued growth in broadband markets. At the same time, the FCC has continued to explore ways to make broadband more accessible, including in areas of the country the FCC deems 'underserved' and to individuals who otherwise would lack the resources to pay for such access.

The FCC’s previous efforts to impose substantive regulations on broadband internet access services remain controversial and have been rescinded in large part by the FCC itself. Attention has increasingly turned to federal legislative proposals to establish net neutrality requirements in some form, though such requirements may well turn out to be less stringent than those adopted by the FCC in 2015.
Appendix 1

ABOUT THE AUTHORS

AYAH ABDIN

*Bird & Bird*

Ayah is a trainee associate in Bird & Bird’s corporate practice in the UAE. Her experience covers advice on local legislation and regulations, advising on foreign companies’ establishment and deregistration in the UAE, and the related legal requirements.

ELENA ANDRIANOVA

*CMS Russia*

Elena Andrianova is a senior associate in the TMT and competition teams at CMS Russia. She specialises in commercial law with a particular focus on TMT regulatory aspects, as well as antimonopoly issues.

She has broad experience in advising major clients in the IT and media sectors on various regulatory issues. She often advises on mass media legislation and licensing and certification. She assists Russian subsidiaries of major foreign and Russian companies on a broad spectrum of regulatory issues. She has gained practical experience in relation to joint venture structuring and M&A projects in the TMT sector. She has also taken part in due diligence investigations in relation to regulatory issues.

Ms Andrianova holds a law degree from the Moscow State Law Academy (MGYuA) as well as an LLM degree from Queen Mary, University of London.

She is a native Russian speaker and is fluent in French and English.

MANUELA BECCHIMANZI

*Cleary Gottlieb Steen & Hamilton LLP*

Manuela Becchimanzi is an associate of Cleary Gottlieb Steen & Hamilton LLP, based in the Rome office. Her practice focuses primarily on Italian and European antitrust laws and administrative law.

Ms Becchimanzi graduated *summa cum laude* from the University of Genoa in 2012. She received an LLM in European legal studies from the College of Europe, Bruges, in 2016.

Ms Becchimanzi has been a member of the Rome Bar since 2016. She is a native Italian speaker and is fluent in English and French.
DAVID BINTLIFF
*Bird & Bird*

Praised by clients for his relationship skills, the ‘exceptional’ David Bintliff is consistently ranked as an expert adviser on complex projects and strategic partnerships in the digital world (‘absolutely outstanding’, *Chambers*, 2017, ‘a superstar’, *The Legal 500*, 2017).

David heads Bird & Bird’s technology and communications and media, entertainment and sports groups in the Middle East.

He has advised clients in the MENA region for over 10 years, having previously worked in our Abu Dhabi office, supporting the growth of the team in the region. David has a particular focus on digital business innovation and transformation and the interplay between content and technology.

MAXIM BOULBA
*CMS Russia*

Maxim Boulba is a partner and head of telecom licensing and regulatory matters at CMS Russia. His practice focuses on telecom-related issues; technical protection of information; radio and TV broadcasting; licensing regulations; e-commerce and internet advertisement-related issues; intellectual property rights; and data protection and processing issues. He has participated in media and telecoms projects, particularly with a leading European radio group, a leading European TV holding and publishing companies.

He advises clients on the best available corporate structures for carrying out TMT business in Russia. He has represented purchasers and sellers across Russia and CIS countries in a large number of M&A deals, and provides general corporate and commercial advice to public and private client companies that operate in the telecommunications and media sectors.

He is a recommended lawyer in the TMT area and is mentioned in the leading legal directories.

Mr Boulba holds a law degree from the Moscow State University (MGU) and a postgraduate diploma in EU competition law from King’s College London. He is fluent in French and English.

JIHONG CHEN
*Zhong Lun Law Firm*

Mr Jihong Chen is an equity partner at Zhong Lun Law Firm. His practice includes telecoms law, intellectual property protection, IP portfolio management, IP licensing, privacy protection, anti-unfair competition, trademark and patent prosecution, domain name dispute resolution, IT and high-tech related legal matters.

In recognition of his influence in the area of IP, Mr Chen was selected as one of the 50 best Chinese lawyers by *Corporate INTL* magazine in 2011. In 2012, Mr Chen was selected the national IP expert by SIPO. In 2013, Mr Chen was awarded ‘Ten Best IP Lawyers’ title by Beijing Bar Association. In 2015, Mr Chen was awarded ‘Best 15 IP Lawyers in China’ by Asia Law and Business. In 2016, Mr Chen was awarded was awarded ‘Telecommunications Law – Lawyer of the Year in China – 2016’ by Global Law Experts and ‘IP Stars’ by Managing Intellectual Property. In 2016 and 2017, Mr Chen was awarded ‘Telecommunications Law – Lawyer of the Year in China’ by Corporate INTL. In 2017, Mr Chen was awarded ‘TMT
Lawyer of the Year’ by Finance Monthly. In 2018, Mr Chen was listed in the ‘WIPR 2018 Leaders’ in the 2018 edition of World IP Review Patents & Trademarks Directory, and was awarded ‘Leading Lawyer’ by AsianLaw Profiles 2018, ‘IP Star’ by Managing Intellectual Property and ‘Telecom Sector Lawyer of the Year in China’ by Corporate INTL. In 2019, he was named one of ‘China’s Top 15 TMT Attorneys in 2019’ by ALB. For years, Mr Chen has continuously been recommended by Chambers and Partners, The Legal 500, LegalBand and other lawyer ranking agencies in the IP and TMT areas.

KEN CHIA

Baker & McKenzie, Wong & Leow

Ken Chia leads the IT and communications team at Baker & McKenzie, Wong & Leow. Mr Chia has represented governments, multinational corporations and enterprises in large-scale procurement, outsourcing and regional cross-border transactions, and also provides strategic regulatory and day-to-day commercial advice. Mr Chia is a member of the firm’s IT and communications, global trade and commerce and competition practices, and sits on the firm’s global privacy steering committee.

VICK CHIEN

Lee and Li, Attorneys-at-Law

Vick Chien graduated from the Department of Power Mechanical Engineering and Graduate School of Law for Science and Technology, National Tsing Hua University, and is currently a doctoral candidate of technology laws of National Chiao Tung University. Prior to joining Lee and Li, Vick served in the National Communications Commission and Taiwan Mobile Co, Ltd, one of the main MNOs in Taiwan. Having extensive experience in the field of info-communication and media, Vick has represented several famous international enterprises in handling licence applications and civil and administrative litigations, and provided legal advice on their business models. He is highly sought after for his dual credentials and expertise in engineering and law. Aside from the field of info-communication law, Vick also focuses on competition law, e-commerce and personal data protection, and frequently publishes articles and policy advice concerning the aforementioned areas in major newspapers and journals. Recognised for his expertise and insights in communication and media law, competition law and e-commerce payment issues, Vick is often invited to give lectures and speeches at public and private institutions and corporations.

PATRICK MARROS CHU

Lee and Li, Attorneys-at-Law

Patrick Chu is a member of the Taiwan Bar Association. He is an experienced litigation lawyer at Lee and Li, and his main practice areas include dispute resolution, corporate reorganisation, bankruptcy, consumer protection, antitrust law, media and sports law, and distribution and franchise contract review. Patrick represents many international financial institutions and international companies, handling civil actions and advising them on potential disputes and compliance issues. Patrick also assists international TV content providers and media businesses with regulatory issues and contract reviews. Patrick’s extensive experience in handling disputes and litigation, and insights from having advised multinational companies...
in various industries, enable him to offer clients sophisticated legal solutions. In addition to handling English matters, Patrick worked for Nagashima Ohno & Tsunematsu, a Japanese law firm, as a visiting lawyer, and is very experienced in Japan-related legal affairs and matters.

JOHN D COLAHAN  
*Latham & Watkins LLP*  
John Colahan is based in Latham & Watkins’ London office and divides his time with the Brussels office. He is a member of the global antitrust and competition practice, having previously been a legal adviser at the UK Cabinet Office and international competition law counsel at The Coca-Cola Company. John represents clients before the European Commission and national authorities in Europe, and internationally, as well as conducting litigation in the European courts and numerous national courts. He has advised on a variety of international antitrust and regulatory matters, including the structuring and implementation of international mergers, acquisitions and joint ventures, cartel enforcement, single firm conduct, regulatory access and compliance counselling. He has covered a wide range of markets including telecommunications and media.

GAIL CRAWFORD  
*Latham & Watkins LLP*  
Gail Crawford is a partner in Latham & Watkins’ London office. Her practice focuses primarily on technology, data privacy and security, intellectual property and commercial law, and includes advising on technology licensing agreements and joint ventures, technology procurement, data protection issues, and e-commerce and communications regulation. She also advises both customers and suppliers on multi-jurisdictional IT, business process and transformation outsourcing transactions. Ms Crawford has extensive experience advising on data protection issues, including advising a global corporation with operations in over 100 countries on its compliance strategy, and advising a number of US e-commerce and web businesses as they expand into Europe and beyond. She also advises online businesses and providers of communications services on the impact of the UK and European restrictions on interception and disclosure of communications data.

RICHARD DAMPNEY  
*Webb Henderson*  
Richard Dampney is a senior associate at Webb Henderson who advises on commercial and regulatory issues with a focus on the telecommunications, media and technology sector and a background in commercial litigation.

Richard advises large global telecommunications companies across Australia, Asia-Pacific and the Middle East, including nbn, and has extensive experience with commercial negotiations and in contract law. Most recently, Richard has acted as a key adviser on the negotiation of nbn’s wholesale broadband agreement, which is the primary agreement under which nbn supplies products and services to its wholesale customers.

Prior to joining Webb Henderson, Richard worked for Ashurst where he advised clients in a diverse range of industries including the technology sector, financial services and resources.
Richard holds a bachelor of laws with first-class honours from the University of Sydney as well as a bachelor of arts (languages) with first-class honours.

MARCO D’OSTUNI

Cleary Gottlieb Steen & Hamilton LLP

Marco D’Ostuni is a partner based in the Italian offices of Cleary Gottlieb. He focuses mainly on competition law and on regulation in the energy, telecommunications and media sectors. He has represented clients in some of the leading EU and Italian competition law cases, often in liberalised and heavily regulated sectors.

He is distinguished as a leading lawyer in Italy in competition and EU law by Chambers Europe, The Legal 500 EMEA and as a Thought Leader in Who’s Who Legal; in technology, media and telecommunications by Chambers Europe and The Legal 500 EMEA; and in Who’s Who Legal: Data – Telecoms & Media. In 2018 and 2014, he was named Italian ‘Telecommunications Lawyer of the Year’ by online magazine Legal Community. In 2019, he won the Client Choice Award for competition in Italy and in 2018 he was named ‘Antitrust Lawyer of the Year’ in Italy by the Toplegal magazine. He is a member of the Rome Bar and the New York Bar. He is widely published on antitrust matters and regularly lectures at numerous conferences and universities. He graduated with honours (University of Naples Law School, 1996), obtained two LLM degrees (College of Europe of Bruges, 1998, including Best Advocate General prize in the European Law Moot Court Competition; and Columbia University School of Law, 2000, Fulbright and Harlan Fiske Stone Scholar) and holds a PhD in competition law (University of Perugia, 2008).

STASYS DRAZDAUSKAS

Sorainen

Dr Stasys Drazdauskas is head of the Sorainen technology, media and telecommunications sector group in Lithuania. He is a highly experienced lawyer, practising in intellectual property, information technology, dispute resolution and other practice areas.

Stasys advises companies involved in the media, retail and wholesale, financial services, pharmaceuticals, and consumer product manufacturing on matters related to intellectual property as well as information technologies and data protection. He helps strategise trademark registration and scope of protection, protects against IP infringements, advises on acquiring or commercialising IP rights, including copyright, trademarks, domain names, trade secrets and inventions.

Stasys is on the list of arbitrators recommended by the Vilnius Court of Commercial Arbitration.

In addition to his professional career, he is also active in the academic field and currently lectures on European private law at Vilnius University’s Faculty of Law.

Stasys appears in the following directories: Chambers Global for dispute resolution (‘His mind is very sharp and he is really talented,’ say clients). Stasys is recognised for his growing arbitration practice and is noted for his particular focus on IP, IT and data-related corporate conflicts; The Legal 500 for intellectual property and IT (‘On the technology and telecoms side, Stasys Drazdauskas handles data protection and cloud law issues and is praised for his “frankness and result-oriented approach”’); World Trademark Review 1000 recommends Stasys as a leading trademark professional; and Best Lawyers for intellectual property, information technology and media resolution.
CHRISTOPHER EKLUND

Bird & Bird

Christopher is an associate in Bird & Bird’s media, entertainment, sport and technology groups, based in the UAE. He offers technical, industry specific knowledge and expertise in the media, sport and digital sectors with a particular focus on media content, music, intellectual property, smart technologies and digital transformation. Christopher works closely with some of the world’s most recognisable, innovative and forward-thinking brands, advising their teams worldwide on local matters and the implementation of global policies and programmes. He previously combined his legal work with a commercial role at a highly successful and growth focused LawTech start-up.

LENA EL-MALAK

Bird & Bird

Lena is a senior associate in Bird & Bird’s media, entertainment, sport and technology groups, based in the UAE. Having spent several years working in-house in one of the leading technology companies in the world and in a well-known regional e-commerce platform, Lena offers deep insight into clients’ needs in the Middle East. Her key areas of expertise include advising on complex regulatory issues in the fields of data protection and privacy law and innovative and emerging technologies including cloud, artificial intelligence, big data, autonomous vehicles, telecommunications, digital healthcare and media and sport. She also has expertise in negotiating high-value commercial agreements.

GIANLUCA FAELLA

Cleary Gottlieb Steen & Hamilton LLP

Gianluca Faella is counsel of Cleary Gottlieb Steen & Hamilton LLP, based in the Rome office. His practice focuses on EU and Italian competition law, as well as regulation, state aid, intellectual property, contract law and litigation. Mr Faella is the author of several publications on antitrust, unfair competition, intellectual property and civil law issues. He obtained an LLM degree in competition law and economics at the Erasmus University Rotterdam in 2003, and a PhD in law and economics at LUISS Guido Carli University in 2005. He is an associate professor at the Link Campus University of Rome, where he teaches competition and intellectual property law and private comparative law, and adjunct professor of law and economics at the LUISS Guido Carli University of Rome. He is a native Italian speaker, and is fluent in English and Spanish.

LINDA FUNCK

Elvinger Hoss Prussen

Linda Funck is a partner with Elvinger, Hoss, Prussen, which she joined in 2000 when she became a member of the Luxembourg Bar.

Her principal fields of activity are mergers and acquisitions, banking, financial and securities laws, corporate restructuring and IT, IP and data protection law. In the field of TMT, Linda Funck regularly advises local and international companies on all IT aspects, and is a regular adviser to clients seeking to establish, restructure or develop their TMT activities in Luxembourg.
She is member of the Commission dealing with intangible law matters of Luxembourg of the Luxembourg Bar Association.

She holds a master's degree in law from the Université Paul Verlaine in Metz. She is fluent in English, French, German and Luxembourgish.

**PABLO GONZÁLEZ-ESPEJO**

*Uría Menéndez*

Pablo González-Espejo is a lawyer based in the Madrid office of Uría Menéndez. He joined the firm in 1994 and was made partner in 2004. In 1999, he opened Uría Menéndez’s São Paulo office, which he headed until September 2003. He advised foreign investors in Brazil and was one of the first foreign lawyers to be registered with the Brazilian Bar Association. Since returning to the firm’s Madrid office in October 2003, he has focused his practice mainly on commercial and company law in the audiovisual, telecommunications, sports and IT sectors.

He advises companies on regulatory and commercial matters. He is regularly involved in major transactions advising businesses and investors in acquisitions, IPOs, joint ventures and outsourcing projects. His international experience includes cross-border deals, especially in Latin America.

Mr González-Espejo also heads the sports law practice group at Uría Menéndez, advising sports clubs, leagues and athletes. He has taken part in international arbitrations before the CAS and is part of the team of experts that drafted a White Paper to reform Spanish professional sports.

He is considered a leading practitioner in M&A, new technologies, telecommunications, media and sports by the most prestigious legal directories, such as *Chambers, PLC Which Lawyer?* and *Best Lawyers in Spain*.

**IRENE HALFORTY**

*Webb Henderson*

Irene is a commercial and regulatory lawyer experienced in providing legal and regulatory advice in TMT, privacy and data, communications, media and IP, as well as general corporate and commercial matters.

Irene has worked extensively in advising on various aspects of technology projects, communications technologies and communications service supply, and undertaking compliance audits in relation to privacy, cybersecurity, data governance, communications, and telecommunications obligations. Irene has experience in large multiparty negotiations, having drafted and negotiated an industry code of practice for data governance with key industry, government, regulators and consumer group stakeholders and has experience in writing submissions to, and engaging with, key government and regulatory stakeholders on policy and law reform issues.

In 2018 she was appointed to the Law Society of NSW Privacy & Data Committee and elected as the co vice chair of the Communications, Entertainment and Technology Law Committee (NSW Young Lawyers).
ANGUS HENDERSON

Webb Henderson

Angus Henderson has worked on communications regulatory, wholesale and commercial transactions over the past 25 years in Australia, Asia-Pacific, the Middle East and beyond. He has worked for leading telecommunications operators in the sector on some of the leading telecommunications, pay television and broadband deals during this time.

A large proportion of his practice is devoted to the development of competitive regulatory models in the telecommunications and broadcasting industries. He provides extensive advice on deregulation of communication markets to operators and regulators throughout Asia-Pacific and the Middle East on these matters.

In 2015 and 2012, Mr Henderson was named as ‘Telecommunications Lawyer of the Year (Sydney)’ by Best Lawyers. He is ranked in Band 1 by Chambers Asia Pacific 2017 in telecommunications in Australia. He is named as a ‘pre-eminent’ telecommunications lawyer by Doyle’s Guide 2017 and is also named as a ‘Leading Individual in TMT’ in The Legal 500 2017. He is also the co-editor of Communications Law and Policy in Australia.

MICHAEL H HERMAN

Latham & Watkins LLP

Michael H Herman is an associate in the Washington, DC office of Latham & Watkins LLP, where he was a summer associate prior to joining the firm full-time. Mr Herman received his JD from Wake Forest University School of Law, graduating summa cum laude. During law school, Mr Herman served as editor-in-chief of the Wake Forest Law Review and interned for Judge Jimmie V Reyna of the United States Court of Appeals for the Federal Circuit. Prior to law school, Mr Herman attended Wake Forest University, graduating cum laude with a BA in politics and international affairs.

FEDERICO HERNÁNDEZ ARROYO

Hogan Lovells BSTL, SC

Federico Hernández, who previously worked in-house at Cofetel, Mexico’s former Federal Telecommunications Commission, has first-hand knowledge of complex regulatory issues regarding the telecommunications sector. He helps clients with regulatory, commercial and procurement transactions. National and international companies call on Federico to help them navigate the regulatory challenges and other hurdles involved in establishing and maintaining operations in Mexico. His unique perspective and experience in working with both public and private clients allow him to provide practical and efficient solutions to legal and business problems.

Federico has counselled clients on administrative, procurement, infrastructure, antitrust, corporate and commercial matters. Clients in industries including TMT, education, sports, consumer, transportation, infrastructure, entertainment and gaming, and non-governmental organisations turn to Federico for his creative approaches and his ability to put together the right legal team. Earlier in his career, Federico served as director of regulatory affairs of Cofetel, where he helped draft policies, regulations and other resolutions. Since then, in his private practice, Federico has advised the government in complex regulatory and policy
projects. Federico regularly publishes articles and moderates or speaks on panels on such topics as net neutrality, the internet of things, machine to machine, the right to be forgotten, big data, mobile technology and other hot topics.

SAM HUANG
*Lee and Li, Attorneys-at-Law*

Sam Huang is an associate at Lee and Li. His primary areas of practice include privacy and data protection laws, e-commerce and cyber laws, telecom and media laws, labour law, corporate governance, etc. He regularly advises clients, mostly multinational companies, on the areas of privacy and data protection, cross-border data transfers, e-marketing, electronic signatures, as well as other e-commerce and internet-related matters.

JOHN P JANKA
*Latham & Watkins LLP*

John P Janka is a partner in the Washington, DC office of Latham & Watkins LLP, where he served as a global leader of the communications law practice group for a decade. For over three decades, Mr Janka has counselled international telecommunications operators and ISPs, content providers, investors and banks on a variety of regulatory, transactional and controversy matters. His experience includes the purchase, sale and financing of communications companies, the procurement and deployment of communications facilities, global spectrum strategies and dispute resolution, the provision of communications capacity, content distribution, strategic planning, and effectuating changes in legal and regulatory frameworks. His clients include satellite operators, broadband providers, wireless and other terrestrial communications companies, video programming suppliers, ISPs, television and radio broadcast stations, and firms that invest in and finance these types of entities.

Mr Janka has served as a United States delegate to an ITU World Radio-communication Conference in Geneva, and as a law clerk to the Honourable Cynthia Holcomb Hall, United States Court of Appeals for the Ninth Circuit. Mr Janka holds a JD degree from the University of California at Los Angeles School of Law, where he graduated as a member of the Order of the Coif, and an AB degree from Duke University, where he graduated magna cum laude.

JEAN-LUC JUHAN
*Latham & Watkins*

Jean-Luc Juhan is a partner in the corporate department of the Paris office of Latham & Watkins.

His practice focuses on outsourcing and technology transactions, including business processes, information technology, telecommunications, systems and software procurement and integration. He also has extensive experience advising clients on all the commercial and legal aspects of technology development, licensing arrangements, web hosting, manufacturing, distribution, e-commerce, entertainment and technology joint ventures.

Mr Juhan is in particular cited in *Chambers Europe* and *The Legal 500 Paris*: the ‘exceptional’ Jean-Luc Juhan, ‘whose negotiating skills and expertise are remarkable’, is ‘very sharp and down-to-earth’ and has ‘very good knowledge of the industry’; he advises high-profile French and international groups on large outsourcing, telecommunication and integration system projects.

© 2019 Law Business Research Ltd
HIROKI KOBAYASHI
Latham & Watkins Gaikokuho Joint Enterprise

Hiroki Kobayashi is a corporate partner of Latham & Watkins Gaikokuho Joint Enterprise in Tokyo. He advises on Japanese legal issues relating to a variety of areas of transactional practice, including corporate law and various government regulatory matters. He handles cross-border M&A matters in collaboration with Latham & Watkins attorneys in other offices, and counsels clients on M&A transactions conducted under different business practices. His experience includes an acquisition by Turner Broadcasting System, Inc through its Japanese subsidiary Japan Entertainment Network KK of Japan Image Communications Co, Ltd, a licensed operator of multiple TV channels, and a sale by Liberty Global of its US subsidiaries holding shares in Jupiter Telecommunications, Japan’s largest cable television operator, to KDDI. Mr Kobayashi has spoken on the topic of privacy in cyberspace at a meeting of an academic society of computer scientists. Mr Kobayashi is admitted to practise in Japan and New York, and is a member of the Dai-ichi Tokyo Bar Association and the New York State Bar Association. He is a native speaker of Japanese and fluent in English.

XAWERY KONARSKI
Traple Konarski Podrecki & Partners

Xawery Konarski is a legal expert with more than 20 years’ experience in new technologies. He is a senior partner and co-founder of the law firm Traple Konarski Podrecki & Partners, where he supervises the technologies, media and telecommunications practices.

Xawery Konarski is vice-president of the Polish Chamber of Information Technology and Telecommunications (PIIT) and president of the New Technologies Law Association (SPNT). He is also a legal adviser to the Internet Advertising Bureau Poland (IAB Poland) and the Polish Chamber of Insurance (PIU).

As an legal expert he participated in the legislative work on a number of laws in the field of new technologies. He is an arbitrator for the Arbitration Court for Internet Domains at the PIIT.

He is the author of several academic publications in the field of new technologies and personal data protection law.

Xawery Konarski has been repeatedly recommended in Polish and international rankings of specialist TMT lawyers (including Chambers Europe, The Legal 500 and Rzeczpospolita).

OLIVER KUUSK
Sorainen

Mr Oliver Kuusk is a legal assistant of the competition and regulatory practice group at Sorainen.

Mr Kuusk assists lawyers in a range of matters including data protection, information technology, infrastructure, telecommunications, media and intellectual property, among others.

Mr Kuusk is passionate about media and intellectual property law, having attended the ELSA Summer Law School on film law at the University of Łódź and researched the use of trademarks in audiovisual works as part of his bachelor studies.
Prior to joining Sorainen as a legal assistant in 2018, he assisted the Sorainen competition and regulatory practice group as a legal trainee and completed traineeships at the Police and Border Guard Board and Nelja Energia, a renewable energy company.

Mr Kuusk holds a BA degree in law and is currently obtaining an MA degree in law at the University of Tartu. He previously studied at the University of Sheffield Law School as an exchange student.

LIISA MARIA KUUSKMAA
Sorainen

Ms Liisa Maria Kuuskmaa is a legal assistant of the competition and regulatory practice group at Sorainen.

Ms Kuuskmaa assists lawyers in a broad spectrum of areas such as competition law, information technology and data protection, telecommunications, distribution and trade, and infrastructure and regulatory. She has experience in assisting lawyers in numerous complex cases, including advising clients in various regulatory compliance and trade regulation matters, drafting and implementing agreements, and resolving related disputes.

Prior to joining Sorainen as a legal assistant in 2018, she completed a traineeship at the firm, and also gained experience at the legal clinic of the University of Tartu and as an intern at the Estonian Prosecutor’s Office.

Ms Kuuskmaa holds a BA degree in law, cum laude, and is currently obtaining an MA degree in law at the University of Tartu. She was also a member of the winning team at the XXI Estonian Moot Court Competition in 2018.

DAVID LAI
Latham & Watkins Gaikokuho Joint Enterprise

David Lai is a corporate associate of Latham & Watkins Gaikokuho Joint Enterprise in Tokyo. Mr Lai’s practice covers a broad range of corporate transactions, including cross-border mergers and acquisitions, joint ventures and strategic alliances, and general corporate counselling. His representative experience in the telecommunications industry includes counselling Qualcomm Incorporated in connection with its RFFE module joint venture with TDK Corporation, representing a Japan-based internet and television service provider in its acquisition by a large Japanese fund, and advising NextRoll, Inc in its Japan-based joint venture with Rakuten K.K. Prior to joining Latham & Watkins, Mr Lai served as an associate in the corporate department of a major international law firm in Seattle, Washington. Mr Lai is admitted to practise in the states of New York and Washington, and as a registered foreign lawyer in Japan.

KIRILL LAPTEV
Sorainen

Kirill is head of the technology, media and telecommunications (TMT) sector group in Belarus.

Kirill leads most of the IT related projects coordinating the TMT team in Belarus. Kirill’s key areas of expertise include commercial contracts and regulatory matters. He is highly experienced in advising major international clients of the TMT sector in their distinctive projects involving Belarus on complex matters such as the special regime for
residents of High Tech Park, including IT related tax matters as well as new crypto regulations and blockchain projects and IP matters in IT and legal due diligence for IT companies with unique experience of dispute resolution in IT. Kirill also is one of the shortlisted specialists in the country for data protection and privacy matters both on a national level and from an EU perspective, with a deep understanding of GDPR specifics. He also represents clients in their relations with higher state authorities in significant projects in the telecoms sector in Belarus, as well as advising international companies on online media regulations.

Kirill is frequently invited as a speaker to IT related events for lawyers and IT businesses as well as writing on the topic of IT law. Due to his reputation as TMT sector group leader and a key expert in the IT sphere, he has been recognised as one of the ‘Next generation lawyers for commercial, corporate and M&A’ by The Legal 500 along with nominations for arbitration and trade and customs by Who’s Who Legal.

PAVEL LASHUK
Sorainen

Pavel Lashuk is an associate of the commercial and regulatory practice group at Sorainen and specialises in data protection and regulatory matters.

As part of his day-to-day work, Pavel assists both local and international TMT clients in developing their business in Belarus considering the progressive involvement of technologies and concomitant laws. As a part of his expertise, Pavel helps clients to derive the advantages and exercise modern technologies within the High-Tech Park. Pavel ensures proper legal support to clients engaged in software and database development, including intellectual property and data protection advice.

Pavel is the author of a number of articles on TMT law topics.

MICHĂŁ MATYSIAK
Trplode Konarski Podrecki & Partners

Michał Matysiak is a member of the IT-Telco and public procurement law teams at T raple Konarski Podrecki & Partners. He provides legal advisory services in the areas of IT, telecommunications, and public procurement law.

He is currently a trainee legal adviser at the Cracow Bar Association. In 2018, he enrolled in a PhD programme at the Institute of Law Studies of the Polish Academy of Sciences, where he also serves as teaching assistant in the Department of Private Law and the New Technologies Law Centre.

Michał gained practical experience while working for reputed Cracow law firms. During his studies, he was involved in the activities of the University Legal Clinic of the Jagiellonian University in Cracow.

He graduated from the Faculty of Law and Administration of the Jagiellonian University (2017), where he defended his MA thesis, entitled Wybrane aspekty ochrony gier komputerowych przed zjawiskiem klonowania (Selected Aspects of Protecting Computer Games against Cloning), in the Department of Intellectual Property Law. He also graduated from the School of American Law organised by the Columbus School of Law at The Catholic University of America in Washington, DC (2017).
MADARA MEĻŅIKA
Sorainen

Ms Madara Meļņika, an associate working in Sorainen’s dispute resolution and C&R practice areas, obtained bachelor’s and master’s degrees from the University of Latvia, Faculty of Law. During her bachelor’s studies, on the Erasmus+ mobility programme Madara spent a semester at the University of Salzburg, and during her master’s studies she used a scholarship from Kurt Hagen to research and study German law for six months at Freie Universität Berlin. In addition, Madara represented the University of Latvia in the Price Media Law Moot Court Competition where her team won the regional rounds of North Europe. She has also participated as a co-author in a legal research group on the protection of journalists’ sources organised by ELSA International and the Council of Europe, and has been a member of the Youth Board in Index on Censorship. In 2019, Madara, as the only representative from Latvia, was awarded a place in the International Scholarship Programme of German Parliament. She took part in the five-month internship at the Parliament, working at the Deputy responsible for Culture and Media issues.

Currently, Madara Meļņika is involved in various media law and human rights projects.

MIHKEL MIIDLA
Sorainen

Mr Mihkel Miidla is a partner and head of the regional technology, media and telecommunications sector group at Sorainen as well as head of the information technology and data protection practice in Estonia. He advises clients in all IT and telecoms-related matters. As a specialist in IT law, Mr Miidla provides outstanding support in cases where IT and IP are closely related.

Mr Miidla is one of Estonia’s leading experts on data protection with his extensive experience in advising clients on personal data protection matters and as a visiting lecturer on privacy and data protection issues at the University of Tartu. He advises on all aspects of data protection, including implementation of the General Data Protection Regulation, cybersecurity, online privacy and data breach response strategies.

Mr Miidla is passionate about novel technologies and disruptive innovation. He advises clients on regulatory matters relating to launching innovative services and products in Estonia.

Mr Miidla also has significant experience in the field of service and trade contracts, including agency, supply and distribution arrangements. He has assisted many local and international businesses in trade deals as well as in setting up trade operations in Estonia and abroad. He has valuable experience in product and service-related issues ranging from advertising and labelling requirements to complex industry-specific regulatory and competition (e.g., automotive industry, energy and utilities) issues.

MATTHEW T MURCHISON
Latham & Watkins LLP

Matthew T Murchison is a partner in the Washington, DC office of Latham & Watkins LLP, where his practice focuses on communications and appellate matters. Mr Murchison advises clients on a range of regulatory, litigation, and transactional matters in the communications sector. He routinely appears before the Federal Communications Commission to represent clients on a variety of significant issues, including net neutrality, major transaction reviews,
retransmission consent, and spectrum policy. In addition, he has drafted key advocacy filings on these and other regulatory issues for clients in the broadband, video, wireless and satellite industries, and regularly counsels these clients on regulatory matters that affect their businesses. Mr Murchison has also successfully presented oral argument in the DC Circuit and US district courts, and has authored briefs before the US Supreme Court, US courts of appeal, and US district courts, in cases concerning the First Amendment, communications law, administrative law, intellectual property, and privacy. Mr Murchison obtained his JD from Stanford Law School and his BA from Yale University, where he graduated magna cum laude.

MAYOWA OLUSOLA
Bird & Bird

Mayowa is an associate in Bird & Bird’s corporate practice in the UAE where she advises clients from a number of sectors including banking, energy and infrastructure, aviation, education, media and hospitality. Her work involves company formation, acquisitions, joint ventures, due diligence, M&A, private equity, debt capital markets and fund transactions. It also involves a range of general commercial and global IP matters such as franchising, regulatory compliance and rights enforcement.

ADEMIR ANTONIO PEREIRA JUNIOR
Advocacia José Del Chiaro

Ademir Antonio Pereira Junior is a partner at Advocacia José Del Chiaro, functioning as co-head of the antitrust and privacy departments. He has acted in several complex competition and regulatory cases, assisting companies in the digital economy in navigating a changing regulatory landscape. His experience comprises merger review, cartel investigations and landmark single-firm conduct cases in several industries, including internet, telecom, consumer products, automotive and pharmaceuticals. He has been closely involved in the latest discussions involving regulatory and antitrust problems in fast-developing industries such as internet, mobile communication and cloud computing. In addition to competition law, Ademir has significant experience with data protection and privacy.

Ademir holds a PhD in commercial law from the University of São Paulo, a master’s degree in law, science and technology from Stanford University, a master’s degree in economic law from the University of São Paulo and a bachelor’s degree in law from the University of São Paulo. He is currently a fellow at the Stanford Center for Internet and Society at Stanford University.

LUIZ FELIPE ROSA RAMOS
Advocacia José Del Chiaro

Luiz Felipe Rosa Ramos is the co-head of the privacy and data protection area at Advocacia Jose Del Chiaro. He was trained by IAPP in data protection and privacy at Fieldfisher (London). He has also extensive experience in competition law, working with traditional industries and matters related to the digital economy. He has acted in cases of cartel, unilateral conducts and merger review, as well as in business litigation. He has experience in antitrust compliance and in legal counselling to companies, associations and unions.
Luiz holds a PhD in law from the University of São Paulo, with a sandwich-doctorate at University of Bielefeld (Germany), a master’s degree in law from the University of São Paulo, with a research period at the University of Salento (Italy), and a bachelor’s degree in law from the University of São Paulo. Luiz is a Fox International Alumni of Yale University. He co-authored *Orlando Gomes* (Elsevier, 2015) and is the author of *Por Trás dos Casos Difíceis* (Juruá, 2017).

**MYRIA SAARINEN**  
*Latham & Watkins*

Myria Saarinen is a partner in the litigation and trial department of the Paris office of Latham & Watkins, and leads the IT litigation practice, and data protection matters.

Myria Saarinen has been advising high-profile clients for more than 20 years with a proven expertise in complex commercial litigation matters, with clients in different industry sectors namely in IT and other technology-related disputes. Myria Saarinen’s impressive client list include disruptive technology game changers and industry leaders in the pharmaceutical, aerospace and insurance sectors, among others.

Myria Saarinen leads all data privacy matters for the French market, with specific expertise in data protection including advising clients on their transborder data flows and complex negotiations with the French Data Protection Authority.

Myria Saarinen is also an active member of various data privacy working groups within the firm. She is a key member of the Latham Data Privacy global team, a member of the Data Privacy Committee and global co-chair of the Technology Industry Group within the firm and aims at unlocking the global platform around data protection issues globally.

**NEREA SANJUAN**  
*Uría Menéndez*

Nerea Sanjuan is a lawyer based in the Madrid office of Uría Menéndez. She joined the firm in 2017 after working since 2008 in the telecommunications multinational Vodafone as a senior counsel, in charge of all issues related to intellectual property, information technology and audiovisual law. Between 2000 and 2008, she also worked as a senior lawyer in the Madrid and Lisbon offices of the law firm Cuatrecasas, in the areas of intellectual and industrial property, entertainment law and information technology.

At Uría Menéndez, Nerea focuses her practice in the areas of intellectual property, telecommunications, media, audiovisual and entertainment law, advertising, information technology and e-commerce. She provides legal advice to national and international clients that operate in all fields of the entertainment and IT industries, including music, audiovisual, editorial, internet service and software providers and electronic communications operators, as well as in the area of sports and gambling.

**TAKAKI SATO**  
*Latham & Watkins Gaikokuho Joint Enterprise*

Takaki Sato is a corporate associate of Latham & Watkins Gaikokuho Joint Enterprise in Tokyo. Mr Sato’s practice covers a broad range of corporate matters, including mergers and acquisitions, general corporate, antitrust and data privacy. His representative experience in the
telecommunications industry includes advising NextRoll, Inc in its Japan-based joint venture with Rakuten K.K. Prior to joining Latham & Watkins, Mr Sato served as an associate at a major law firm in Tokyo. Mr Sato is admitted to practise in Japan and New York.

LISBETH SAVILL
*Latham & Watkins LLP*

Lisbeth Savill is a partner in Latham & Watkins’ London office and a member of its entertainment, sports and media practice. She focuses on commercial work in the media and entertainment sectors, including financing, distribution and licensing arrangements for audiovisual content, and the purchase, sale and financing of entertainment companies. Her clients cover a wide range of interests in the entertainment and media sectors, including equity and debt financiers, major studios, independent producers, rights holders and distributors of film and television content. Lisbeth has been recognised as a leading lawyer in the film and television industries for many years. She is actively involved in issues important to the entertainment sector.

DARYL SEETOH
*Baker & McKenzie.Wong & Leow*

Daryl’s practice covers information technology, data privacy, commercial and compliance work. Daryl advises frequently on telecommunications and e-commerce as well as general licensing and regulatory matters including anti-bribery and corruption, consumer products, consumer protection, environmental, customs, and sanctions and trade compliance.

ANDRIS TAURIŅŠ
*Sorainen*

Mr Andris Tauriņš is the co-head of the dispute resolution team and head of the TMT sector group of Sorainen Latvia. His main specialisation is dispute resolution in court and by way of arbitration, intellectual property, information technology and pharmacy law, as well as e-commerce issues. He lectures on topics involving intellectual property rights and has been a lecturer on intellectual property rights at Riga Business School, as well as on copyright matters at Latvia Culture College.

In addition, Andris is a licensed professional patent attorney specialising in trademarks. This qualifies him to represent international clients before the Latvian Patent Authority in trademark-related matters, including international trademark registration applications.

Senior associate Andris Tauriņš appears in *Chambers Europe* rankings as a result of positive market feedback and increased visibility. According to clients, he is dedicated and highly responsive. Andris also is a recommended practitioner by Best Lawyers for IT law in Latvia.

YAN VILLELA VIEIRA
*Advocacia José Del Chiaro*

Yan Villela Vieira is an associate at Advocacia José Del Chiaro. He represents clients on cases that involve competition law, such as cartel investigations, unilateral conducts and merger proceedings in various industries, including the telecommunications, technology, mining
and automotive. He also consults on antitrust compliance programmes, reviews commercial practices of domestic and foreign companies and represents clients in regulatory matters involving telecommunications and media.

Yan holds a master’s degree in business economics from the School of Economics at Getulio Vargas Foundation and a bachelor’s degree in law from the University of São Paulo, having participated in an exchange programme at Leipzig University (Germany). He is currently a master’s candidate in law at the University of São Paulo.

MARCO ZOTTA
_Cleary Gottlieb Steen & Hamilton LLP_

Marco Zotta is a senior attorney of Cleary Gottlieb Steen & Hamilton LLP, based in the Rome office. His practice focuses on administrative law, European and Italian antitrust laws and telecommunications law.

He graduated with honours (Law School of Rome ‘La Sapienza’, 2003), obtained an LLM degree from the University of California at Berkeley School of Law (Boalt Hall, 2009) and holds a in law and economics (LUISS Guido Carli University, Rome, 2015).

Mr Zotta has been a member of the Rome Bar since 2006. He is a native Italian speaker and is fluent in English.
Appendix 2

CONTRIBUTORS’ CONTACT DETAILS

ADVOCACIA JOSÉ DEL CHIARO
Avenida Brigadeiro Faria Lima, nº 2012, 9th floor
São Paulo/SP
Brazil
Tel: +55 11 3030 9000
api@ajdc.com.br
lfr@ajdc.com.br
yvv@ajdc.com.br
www.ajdc.com.br

BAKER & MCKENZIE.WONG & LEOW
8 Marina Boulevard
#05-01 Marina Bay Financial Centre Tower 1
018981 Singapore
Tel: +65 6434 2558
Fax: +65 6337 5100
ken.chia@bakermckenzie.com
www.bakermckenzie.com/singapore

BIRD & BIRD
Level 8
Al Maqam Tower
ADGM Square
PO Box 144991
Abu Dhabi
United Arab Emirates

CLEARY GOTTLIEB STEEN & HAMILTON LLP
Piazza di Spagna 15
00187 Rome
Italy
Tel: +39 06 69 52 21
Fax: +39 06 69 20 06 65
mbecchimanzi@cgsh.com
mdostuni@cgsh.com
gfaella@cgsh.com
mzotta@cgsh.com
www.clearygottlieb.com
Contributors' Contact Details

CMS RUSSIA
Naberezhnaya Tower, block C
10 Presnenskaya Naberezhnaya
123112 Moscow
Russia
Tel: +7 495 786 4000
Fax: +7 495 786 4001
maxim.boulba@cmslegal.ru
elena.andrianova@cmslegal.ru
www.cms.law

ELVINGER HESS PRUSSEN
2, Place Winston Churchill
BP 425
L-2014 Luxembourg
Tel: +352 4466440
Fax: +352 442255
lindafunck@elvingerhoss.lu
www.elvingerhoss.lu

HOGAN LOVELLS BSTL, SC
Paseo de los Tamarindos 150-PB
Bosques de las Lomas
Mexico City 05120
Mexico
Tel: +52 55 5091 0164
Fax: +52 55 5091 0123
federico.hernandez@hoganlovells.com
www.hoganlovells.com

LATHAM & WATKINS LLP
45 rue Saint-Dominique
75007 Paris
France
Tel: +33 1 4062 2000
Fax: +33 1 4062 2062
myria.saarinen@lw.com
jean-luc.juhan@lw.com

Latham & Watkins Gaikokuho Joint Enterprise
Marunouchi Building, 32nd Floor
2-4-1 Marunouchi, Chiyoda-ku
Tokyo 100-6332
Japan
Tel: +81 3 6212 7800
Fax: +81 3 6212 7801
hiroki.kobayashi@lw.com

99 Bishopsgate
London EC2M 3XF
United Kingdom
Tel: +44 20 7710 1000
Fax: +44 20 7374 4460
john.colahan@lw.com
gail.crawford@lw.com
lisbeth.savill@lw.com

555 Eleventh Street, NW
Suite 1000
Washington, DC 20004-1304
United States
Tel: +1 202 637 2200
Fax: +1 202 637 2201
john.janka@lw.com
matthew.murchison@lw.com
michael.herman@lw.com
www.lw.com

LEE AND LI, ATTORNEYS-AT-LAW
8F, No. 555 Zhongxiao E. Road
Taipei 11072
Taiwan
Tel: +886 2 2763 8000, extensions 2122/2214/2360
Fax: +886 2 2766 5566
marrosju@leeandli.com
vickchien@leeandli.com
samhuang@leeandli.com
www.leeandli.com

© 2019 Law Business Research Ltd
Contributors' Contact Details

SORAINEN
ul Internatsionalnaya 36-1
220030 Minsk
Belarus
Tel: +375 17 306 2102
Fax: +375 17 306 2079
kirill.laptev@sorainen.com
pavel.lashuk@sorainen.com

Kirill Laptev
Pavel Lashuk
ksdPLP

Kawe Plaza, 7th floor
Pärnu mnt 15
Tallinn 10141
Estonia
Tel: +372 6 400 900
Fax: +372 6 400 901
mihkel.miidla@sorainen.com
liisa.kuuskmaa@sorainen.com
oliver.kuusk@sorainen.com

Mihkel Miidla
Liisa Kuuskmaa
Oliver Kuusk
ksdPLP

Kr Valdemāra iela 21
1010 Riga
Latvia
Tel: +371 67 365 000
Fax: +371 67 365 001
andris.taurins@sorainen.com
madara.melnika@sorainen.com

Andris Taurins
Madara Melnīka
ksdPLP

Gedimino ave 44A
Vilnius 01110
Lithuania
Tel: +370 5 2685040
Fax: +370 5 2685041
stasys.drazdauskas@sorainen.com

Stasys Drazdauskas
ksdPLP

www.sorainen.com
TRAPLE KONARSKI PODRECKI & PARTNERS
ul. Królowej Jadwigi 170
30-212 Cracow
Poland
Tel: +48 12 426 05 30

ul. Twarda 4
00-105 Warsaw
Poland
Tel: +48 22 850 10 10
www.traple.pl

URÍA MENÉNDEZ
Edificio Rodrigo Uría
c/Príncipe de Vergara, 187
Plaza de Rodrigo Uría
28002 Madrid
Spain
Tel: +34 915 860 409 / 754
Fax: +34 915 860 080
pablo.gonzalez@uria.com
nera.sanjuan@uria.com
www.uria.com

WEBB HENDERSON
Level 18, 420 George St
Sydney NSW 2000
Australia
Tel: +61 2 8214 3500
angus.henderson@webbhenderson.com
richard.dampney@webbhenderson.com
irene.half@webbhenderson.com
www.webbhenderson.com

ZHONG LUN LAW FIRM
28, 31, 33, 36, 37/F, SK Tower
6A Jianguomenwai Avenue
Chaoyang District
Beijing 100022
China
Tel: +86 10 5957 2288
Fax: +86 10 6568 1022
chenjichong@zhonglun.com
www.zhonglun.com
THE CORPORATE GOVERNANCE REVIEW
Willem J L Calkoen
NautaDutilh

THE CORPORATE IMMIGRATION REVIEW
Chris Magrath
Magrath LLP

THE CORPORATE TAX PLANNING LAW REVIEW
Jodi J Schwartz and Swift S O Edgar
Wachtell, Lipton, Rosen & Katz

THE DISPUTE RESOLUTION REVIEW
Damian Taylor
Slaughter and May

THE DOMINANCE AND MONOPOLIES REVIEW
Maurits J F M Dolmans and Henry Mostyn
Cleary Gottlieb Steen & Hamilton LLP

THE e-DISCOVERY AND INFORMATION GOVERNANCE LAW REVIEW
Tess Blair
Morgan, Lewis & Bockius LLP

THE EMPLOYMENT LAW REVIEW
Erika C Collins
Proskauer Rose LLP

THE ENERGY REGULATION AND MARKETS REVIEW
David L Schwartz
Latham & Watkins

THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW
Theodore L Garrett
Covington & Burling LLP

THE EXECUTIVE REMUNERATION REVIEW
Arthur Kohn and Janet Cooper
Cleary Gottlieb Steen & Hamilton LLP and Tapestry Compliance

THE FINANCIAL TECHNOLOGY LAW REVIEW
Thomas A Frick
Niederer Kraft Frey

THE FOREIGN INVESTMENT REGULATION REVIEW
Calvin S Goldman QC and Michael Koch
Goodmans LLP

THE FRANCHISE LAW REVIEW
Mark Abell
Bird & Bird LLP

© 2019 Law Business Research Ltd
THE INTERNATIONAL TRADE LAW REVIEW
Folkert Graafsma and Joris Cornelis
Vermula Verhaeghe Graafsma & Bronckers (VVGB)

THE INVESTMENT TREATY ARBITRATION REVIEW
Barton Legum
Dentons

THE INWARD INVESTMENT AND INTERNATIONAL TAXATION REVIEW
Tim Sanders
Skadden, Arps, Slate, Meagher & Flom LLP

THE ISLAMIC FINANCE AND MARKETS LAW REVIEW
John Dewar and Munib Hussain
Milbank LLP

THE LABOUR AND EMPLOYMENT DISPUTES REVIEW
Nicholas Robertson
Mayer Brown

THE LENDING AND SECURED FINANCE REVIEW
Azadeh Nassiri
Slaughter and May

THE LIFE SCIENCES LAW REVIEW
Richard Kingham
Covington & Burling LLP

THE MERGER CONTROL REVIEW
Ilene Knable Gotts
Wachtell, Lipton, Rosen & Katz

THE MERGERS AND ACQUISITIONS REVIEW
Mark Zerdin
Slaughter and May

THE MINING LAW REVIEW
Erik Richer La Flèche
Stikeman Elliott LLP

THE OIL AND GAS LAW REVIEW
Christopher B Strong
Vinson & Elkins LLP

THE PATENT LITIGATION LAW REVIEW
Trevor Cook
WilmerHale

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW
Alan Charles Raul
Sidley Austin LLP

© 2019 Law Business Research Ltd