THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

ELEVENTH EDITION

Editor
Matthew T Murchison

THE LAWREVIEWS

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

ELEVENTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2020
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Matthew T Murchison

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Joel Woods

SENIOR ACCOUNT MANAGERS
Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS
Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Gavin Jordan

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-508-5

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

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

ANANT LAW

CLEARY GOTTLIEB STEEN & HAMILTON LLP

CMS RUSSIA

ELVINGER HOSS PRUSSEN

LATHAM & WATKINS LLP

LEE AND LI, ATTORNEYS-AT-LAW

RÍOS FERRER, GUILLÉN-LLARENA, TREVIÑO Y RIVERA, SC

SHAHID LAW FIRM

SORAINEN

TRAPLE KONARSKI PODRECKI & PARTNERS

URÍA MENÉNDEZ

WEBB HENDERSON

ZHONG LUN LAW FIRM

CONTENTS

PREFACE

The Technology, Media and Telecommunications Review is now in its 11th edition, and I am excited to be taking the reins of this publication after a decade under the steady hand of long-time editor John Janka. This Review occupies a unique space in the literature on TMT issues. Rather than serving a traditional legal treatise, this publication aims to provide a practical, business-focused survey of law and policy in this arena, along with insights into how this legal and policy landscape continues to evolve from year to year. In the dynamic and ever-changing TMT sector, such perspective is vitally important. And the scope of this Review is global, now covering 20 jurisdictions.

Covid-19 shook the world in 2020, and its reverberations in the TMT sector have been profound. As the threat of infection has led to widespread lockdowns, the importance of connectivity has never been greater nor more obvious. For many businesses, remote working has become the rule rather than the exception. Many schools have switched to distance learning formats. Tele-health is on the rise as doctors check in on patients via videoconference. Even tasks as mundane as grocery shopping have shifted online. And broadband connectivity, where available, has made it all possible.

For policymakers, the experience of covid-19 has begun to reshape their understanding of the TMT arena and to refocus their policy goals. The sudden shift to remote working and distance learning has stress-tested broadband networks across the world – providing a 'natural experiment' for determining whether existing policies have yielded robust systems capable of handling substantial increases in internet traffic. In the European Union, officials called on video-streaming platforms to downgrade high-definition content temporarily to avoid overly straining broadband networks at the start of the pandemic. In the United States, meanwhile, policymakers touted that such measures were not necessary, and have attributed the apparent resilience of broadband networks in the country to deregulatory policies.

At the same time, the pandemic has prompted new initiatives to ensure, improve and expand broadband connectivity for consumers going forward. In various jurisdictions, policymakers are moving forward with subsidy programmes and other efforts to spur the deployment of advanced networks more deeply into unserved and underserved areas. Regulators also have taken steps to preserve internet access where it already exists, including by having service providers 'pledge' that they will not disconnect customers for non-payment in light of the pandemic, or by pursuing more prescriptive measures. In short, covid-19 has been part cautionary tale, part rallying cry, and its long-term impact on the TMT sector remains to be seen.

New technologies likewise have required new approaches and perspectives by policymakers. A notable example is the ongoing deployment of 5G wireless networks, as regulators continue to look for ways to facilitate such deployments. These initiatives take a

variety of forms, and frequently include efforts to free up more spectrum resources, including by adopting new rules for 'sharing' spectrum and by reallocating spectrum from one use to another. 5G spectrum was a significant focus of the World Radio-communication Conference (WRC) of the International Telecommunication Union (ITU), held in late 2019 in Sharm el-Sheikh, Egypt. And multiple jurisdictions have continued to auction off wireless licences in bands newly designated for 5G deployment, capitalising on service providers' strong demand for expanded access for spectrum.

Another example is the planned deployment of multiple large satellite constellations in low-earth orbit to support new broadband services. The providers proposing these networks say they will greatly expand the availability of high-speed internet access service. At the same time, the sheer scale of the planned systems has raised fresh questions about how best to prevent accidental collisions and ensure equitable sharing of spectrum resources.

Even with so many newer issues swirling in the TMT sector, familiar topics have remained in the spotlight as well. Cue network neutrality, the principle that consumers should benefit from an 'open internet' where bits are transmitted in a non-discriminatory manner, without regard for their source, ownership or destination. The basic principle has been around for well over a decade, but policymakers are still sorting out how best to effectuate it without undermining investment and innovation in broadband services. In the United States, network neutrality has become a point of contention between the federal government, which has opted for a light-touch approach, and certain states that wish to impose bright-line prohibitions on internet service providers. In Europe, new guidelines and rulings have addressed internet service providers' 'zero rating' plans, which exempt certain data from counting against a customer's usage allowance. Regulators in Asia are grappling with similar policy questions. And this debate dovetails with efforts in some jurisdictions to increase oversight of the content moderation policies of social media companies and other online platforms.

The country-specific chapters that follow recap these and other developments in the TMT arena, including updates on privacy and data security, regulation of traditional video and voice services, and media ownership. On the issue of foreign ownership in particular, communications policymakers have increasingly incorporated national security considerations into their decision-making, as evidenced by recent actions in the United States against Chinese equipment manufacturers and service providers.

Our authors from around the globe have lent their considerable insight, analysis and experience to the preparation of their respective chapters. I hope readers will find this 11th edition of *The Technology, Media and Telecommunications Review* as helpful as I have found this publication year in and year out.

Matthew T Murchison
Latham & Watkins LLP
Washington, DC
November 2020

Chapter 6

FRANCE

Myria Saarinen and Jean-Luc Juhan[1]

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 (the two 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 reform of the Telecoms Package in 2018, which resulted in the adoption of the European Electronic Communications Code (EECC), is to be transposed into national law by December 2020.[2] As for the audiovisual sector, the Audiovisual Media Services Directive (AMSD) is also awaiting national transposition, the deadline initially set for September 2020 having already passed.[3]

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 various sources and involving a diversity of actors (regulators, telecoms operators, and local, regional and national authorities). The TMT sectors are key to the French economy, and 2019 was once again an important year in many respects for these sectors' business.

II REGULATION

i The regulators

The regulation of the technology, media and telecommunications sector in France is characterised by the large number of authorities:

The Authority for the Regulation of the Post and Electronic Communications (ARCEP) is an independent government agency that oversees the electronic communications and postal

1 Myria Saarinen and Jean-Luc Juhan are partners at Latham & Watkins. This chapter was written with contributions from trainee Alex Park.

2 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) Text with EEA relevance.

3 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

services sector. It ensures the implementation of universal services, imposes requirements on operators exerting a significant influence on the market, participates in defining the regulatory framework, allocates finite resources (RFs and numbers), imposes sanctions, resolves disputes and delivers authorisations for postal activities.

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.

The High Authority for the Distribution of Works and the Protection of Copyright on the Internet (HADOPI) is in charge of protecting intellectual property rights over works of art and literature on the internet. An audiovisual reform originally planned for early 2020 including the merger of the CSA with the HADOPI has been indefinitely pushed back.

The Data Protection Authority (CNIL) and the French Competition Authority (FCA) also exert a significant influence in the sector.

These authorities may deliver opinions upon request by the government, Parliament or other independent administrative authorities, and, at the exception of HADOPI, also render decisions and opinions that may have a structural impact on these sectors. The National Frequency Agency (ANFR) is also an important agency in charge of inter-ministerial spectrum management and use as well as the supervision of independent radio networks (see Section IV).

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 legislation governing the law applicable to data protection is the GDPR[4] 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 from 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.

No specific licences or authorisations are required to become a telecoms operator. Public networks and electronic communication services to the public can be freely established and provided, subject to prior notification to the ARCEP (Articles L32-1 and L33-1 of the CPCE). The ARCEP may register on its own initiative any actor who failed to declare itself.[5]

4 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).

5 Article L33-1 I of the CPCE.

The use of RFs, however, requires a licence granted by ARCEP (Article L42-1 of the CPCE). The frequencies allotted to 5G networks are expected to be subject to limited exemptions in order to encourage its deployment upon the transposition of the EECC.

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 in principle, but is subject to extensions and various derogations.[6] Broadcasting services that are not subject to the CSA's 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 prior declaration.[7]

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.[8] However, according to Article L151-1 et seq. of the French Monetary and Financial Code, foreign (EU or non-EU) investment in strategic sectors (such as security, public defence, cryptography or interception of correspondence),[9] is subject to a prior authorisation by the French Ministry of Economy. Any transaction concluded without prior authorisation is null and void, and criminal sanctions (imprisonment of up to five years[10] and a fine amounting to up to twice the amount of the transaction) are also applicable. The list of sectors subject to prior authorisation has been steadily expanding over the last few years and today include online general press services and activities relating to the integrity, security and continuity of the operation of networks and ECSs.

Specific ownership restrictions applicable to the media sector

French regulations impose media ownership restrictions to preserve media pluralism and competition. 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.[11]

6 See Articles 28 to 32 of the Law of 30 September 1986, which determine the CSA's allocation procedures.

7 Articles 33 to 34-5 of the Law of 30 September 1986.

8 Article L33-1 III of the CPCE.

9 Article R151-3 of the French Monetary and Financial Code.

10 Article L165-1 of the French Monetary and Financial Code.

11 Articles 39-I and 39-III of the Law of 30 September 1986.

Regulation of the media sector is currently evolving in reaction to a number of changes in French media ownership. For example, Law No. 2016-1524 of 14 November 2016 requires media outlets to provide yearly information on their capital ownership and governing bodies,[12] and reinforces the powers of the CSA over French media governance with the creation of ethics committees.[13]

Regarding the radio sector, a single person cannot retain networks of which the coverage exceeds 150 million inhabitants or 20 per cent of the aggregated potential audience.[14] This regulation is, however, expected to be amended in order to take into account local pluralism challenges.

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.[15] In addition, such licence may not 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.[16] 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.[17] Specific rules restricting cross-media ownership also apply.[18]

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 specific to the media sector. Merger control rules are enforced by the FCA.[19]

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.[20] Companies active in radio or TV are subject to merger control procedures before the FCA, in addition to a non-binding opinion from the CSA.[21]

Finally, 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.[22]

12 Article 19 of the Law No. 2016-1524 of 14 November 2016.
13 Article 11 of the Law No. 2016-1524 of 14 November 2016.
14 Article 41 of the Law of 30 September 1986.
15 Article 40 of the Law of 30 September 1986.
16 Article 14 of the Law of 14 November 2016.
17 Article 40 of the Law of 30 September 1986.
18 Article 41-1 to 41-2-1 of the Law of 30 September 1986.
19 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.
20 Article L36-10 of the CPCE.
21 Article 41-4 of the Law of 30 September 1986.
22 Article 42-3 of the Law of 30 September 1986.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

Under the CPCE, ECSs other than public voice telephony may be provided freely.[23]

DSL networks are subject to asymmetrical regulation. Regarding ADSL networks, alternative operators must be provided with direct access to the copper pair infrastructure of France Télécom-Orange, the historical operator, following local loop unbundling.

Internet service providers (ISPs) can operate freely, but must file a prior declaration with ARCEP.[24] A failure to comply with this obligation constitutes a criminal offence.[25]

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. A liability exemption regime for hosting service providers is also set out by the same law, expressly excluding a general obligation to monitor the information they transmit or store or the obligation to look for facts or circumstances indicating illicit activity. Nevertheless, knowledge that obviously illicit content is stored will trigger the obligation to remove or render inaccessible such content. In that respect, the question of the qualification as 'hosting service provider' is still widely debated before French courts.[26] A hosting service provider will benefit from the liability exemption regime 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 content (e.g., determining or verifying the content published, broadcasted or uploaded), the provider will qualify as a website publisher and would be fully liable for any unlawful or harmful content published, broadcast or uploaded on its website.[27]

---

23 Article L32-1 of the CPCE.

24 Article L33-1 of the CPCE.

25 Article L39 of the CPCE.

26 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 a priori the content they host but need to ensure 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 Auféminin.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, will give significant importance to judges' discretion. In that respect, see Cass., Com,. 3 May 2012, No. 11-10.507, *Christian Dior Couture*, No. 11-10.505, *Louis Vuitton Malletier* and No. 11-10.508, *Parfums Christian Dior*, in which the Supreme Court confirmed an earlier decision of the Paris Court of Appeals that did not consider eBay as a 'host provider', and therefore refused to apply the liability-exemption regime. See, in contrast, *Brocanteurs v. eBay*, Paris Court of Appeals, Pôle 5, ch 1, 4 April 2012, No. 10-00.878, in which second-hand and antique dealers accused eBay of encouraging illegal practices by providing individuals with the means to compete unfairly against professionals, and in which the Paris Court of Appeals considered eBay as a host provider able to benefit from the liability-exemption regime. The Court of Appeals based its decision on the fact that eBay had no knowledge or control of the adverts stored on its site. If the seller was asked to provide certain information, it was for the purpose of ensuring a more secure relationship between its users. The issue is also debated in the context of online forums. The Supreme Court ruled on 3 November 2015 that publishing directors are responsible for 'personal contribution spaces' from the moment they become aware of their content and must be held criminally liable for failing to take down defamatory comments (Cass., Crim., 3 November 2015, No. 13-82645).

27 See judgment of the High Court of Paris, 4 December 2015, *Goyard St-Honoré v. LBC France*.

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',[28] 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).

The transposition of the EECC is expected to extend the coverage of universal services to high-speed internet.

These services must be provided under strictly defined pricing and technical conditions taking into consideration difficulties faced by certain categories of users, such as low income populations, and provide equal access across geographical locations. 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.[29]

ARCEP determines the cost of the universal service and, determines the amount of the other operators' contributions to the financing of USOs through a sectoral fund when the provision of USOs represents an excessive burden for the operator in charge. In principle, every operator contributes to the financing, with each contribution being calculated on the basis of the turnover achieved by the operator in its electronic communications activities.[30]

iii 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 is how much control internet stakeholders can rightfully exert over traffic. This implies examining operators' practices on their networks, as well as their relationships with some content and application providers.

The Digital Republic Law[31] introduced the principle of net neutrality into the national legal framework and granted ARCEP with new investigatory and sanctioning powers to ensure compliance (see also Section VI.i).[32] In particular, ARCEP is now in charge of implementing net neutrality in accordance with Regulation No. 2015/2120 of

28 Article 1(2) of Directive No. 2002/22/EC.

29 See Ministerial Order of 27 November 2017 designating Orange (JORF No. 0282 of 3 December 2017).

30 Article L35-3 of the CPCE.

31 Law No. 2016-1321 of 7 October 2016 for a Digital Republic.

32 Articles 40 to 47 of Digital Republic Law.

25 November 2015 establishing measures concerning open internet access.[33] 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.[34]

ARCEP has been taking on a more active role regarding net neutrality since the adoption of the Digital Republic Law. For example, ARCEP has been publishing an annual report on the state of the internet in France, identifying various threats that could undermine the internet's proper functioning and neutrality, and setting out the regulator's actions to contain these threats. The most recent issue addresses data interconnection, transition to IPv6,[35] the quality of fixed internet access, net neutrality, open platforms and the environmental impact of networks.[36]

Pursuant to the Law of 21 June 2004, ISPs have a purely technical role regarding content, and do not have a 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, intervening when requested 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.[37]

Finally, French e-consumers benefit from consumer law provisions and 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.[38] Moreover, consumers must be provided with effective means for requesting the cessation of unsolicited communications.[39] 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 in order to refuse advertising material.[40] All telephone operators also have the obligation to offer their users the possibility to register on an opposition list.[41] 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.[42]

33 Article 40 of Digital Republic Law.

34 Article 43 of Digital Republic Law.

35 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.

36 2020 report: 'The state of internet in France', ARCEP report, June 2020 (available at https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet_edition-2020_250620.pdf).

37 See Articles L331-25, L336-3 and R335-5 of the Intellectual Property Code.

38 See Article L34-5 of the CPCE.

39 See Article L34-5 of the CPCE.

40 See www.bloctel.gouv.fr.

41 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.

42 See Ministerial Order of 25 February 2016 designating SA Opposetel (JORF No. 0050 of 28 February 2016).

iv Privacy and data security

Substantial changes in the legal framework regarding security in telecommunications have been made in the past few years.

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 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 pre-identified individuals likely to be connected to a terrorist threat.[43]

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.[44] This regime, which entered into force on 1 January 2015,[45] authorises the collection of 'information or documents' from operators as opposed to the collection of simply 'technical data' 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.[46] 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.[47] Law No. 2016-731

43 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.

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

45 Article 20 IV of the LPM.

46 See Article 6-1 of Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy as introduced by Article 12 of Law No. 2014-1353 of 13 November 2014 reinforcing regulations relating to the fight against terrorism.

47 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

of 3 June 2016[48] allows police officers, with the authorisation and under the control of a judge, to access, remotely and without consent, the correspondences stored in electronic communications available through identification.[49] Police officers can also be authorised, by a judge and under his or her control, to use a technical method, 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.[50] This Law also extended 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.[51]

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.[52] Exceptions are provided, 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 facilitates the detection of infringements, the collection of evidence and the search for criminal activities by facilitating the creation of police files and coordination. The National Agency for the Security of Information Systems (ANSSI), a branch of the Secretariat-General for Defence and National Security created in 2009, is in charge of cybersecurity threats.[53]

Morevover, 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,[54] and recognises that the CNIL has jurisdiction over the control of video protection systems.[55]

With regard to the detection of cyberattacks, Law No. 2018-607 of 13 July 2018[56] created Article L33-14 of the CPCE that involves operators in the detection of cyberattacks.

---

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.

48 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.

49 Articles 706-95-1 to 706-95-3 of the French Criminal Proceedings Code added by Article 2 of Law No. 2016-731 of 3 June 2016.

50 Articles 706-95-4 to 706-95-10 of the French Criminal Proceedings Code added by Article 3 of Law No. 2016-731 of 3 June 2016.

51 Article 706-102-1 of the French Criminal Proceedings Code amended by Article 5 of the Law No. 2016-731 of 3 June 2016.

52 See Articles L34-1 and D98-5 of the CPCE.

53 See Decree No. 2009-834 of 7 July 2009 as modified by Decree No. 2011-170 of 11 February 2011.

54 See Article L. 251-2 of the French Internal Security Code.

55 See Article L. 253-2 and L. 253-3 of the French Internal Security Code.

56 Law No. 2018-607 of 13 July 2018, Military Planning Law 2019–2025 (LPM).

Pursuant to this article, electronic communications operators are entitled to use technical 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.[57]

In terms of personal data protection, obligations were reinforced with the entry into application of the GDPR.[58] 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.[59]

v The implementation of the Network and Information Security Directive

With regard to cybersecurity, the Network and Information Security Directive (NISD)[60] 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, distribution of electricity and gas). The Prime Minister can designate operators as an OES if they provide at least one of the enumerated services.[61] The operator is notified of the Prime Minister's intent to designate it as an OES and can formulate observations.[62]

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.[63]

Nevertheless, the French implementing law excludes from its scope certain types of entities already subject to information system security regulations, such as operators for

57 Article 45 of the 1978 Data Protection Law.

58 See Article 32 of the GDPR.

59 Available at https://www.cnil.fr/en/new-guide-regarding-security-personal-data.

60 Directive No. 2016/1148 of 6 July 2016.

61 Article 3 of Decree No. 2018-384 dated 23 May 2018.

62 Article 3 of Decree No. 2018-384 dated 23 May 2018.

63 Article 10 of Law No. 2018-133 of 26 February 2018.

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.[64]

Both OESs and DSPs shall appoint a representative in charge of the contact with the ANSSI.[65] For DSPs, this representative acts in the name of the provider for compliance with its obligations set forth of the NSID framework.[66] DSPs shall keep an updated list of all networks and information systems necessary for the provision of their services within the European Union.[67]

OESs must comply with security measures defined in the Order of 14 September 2018 adopted for its implementation.[68] 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.[69] DSPs shall refer to Article 2 of the Commission Implementing Regulation of 30 January 2018 for the security measures that should be implemented.[70] Documents attesting to this implementation should be made available to the ANSSI in case of control.[71]

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.[72]

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[73] and from €75,000 to €100,000 for DSPs.[74]

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.[75]

64 Article 2 of Law No. 2018-133 of 26 February 2018.
65 Articles 5 and 16 of Decree No. 2018-384 dated 23 May 2018.
66 Article 16 of Decree No. 2018-384 dated 23 May 2018.
67 Article 17 of Decree No. 2018-384 dated 23 May 2018.
68 Article 10 of Decree No. 2018-384 dated 23 May 2018.
69 Article 12 of Law No. 2018-133 of 26 February 2018.
70 Article 18 of Decree No. 2018-384 dated 23 May 2018.
71 Article 19 of Decree No. 2018-384 dated 23 May 2018.
72 Articles 7 and 13 of Law No. 2018-133; Articles 11, 12, 20 and 21 of Decree No. 2018-384 dated 23 May 2018.
73 Article 9 of Law No. 2018-133 of 26 February 2018.
74 Article 15 of Law No. 2018-133 of 26 February 2018.
75 Article L42-3 of the CPCE.

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 or notification to ARCEP, which may refuse such assignment. [76] 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,[77] and in December 2011, licences for the 800MHz were awarded to the same operators except Free Mobile,[78] 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. 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.[79] 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.[80]

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.[81] On 16 July 2018, the French government officially

76 Article R20-44-9-2 et seq, of the CPCE.

77 ARCEP, Decision No. 2011-1080 of 22 September 2011.

78 ARCEP, Decision No. 2011-1510 of 22 December 2011.

79 See ARCEP press release of 2 August 2018.

80 ARCEP, Decisions No. 2017-0734 (*Bouygues Telecom*) and No. 2017-0735 (*SFR*) of 13 June 2017.

81 See ARCEP press release of 30 September 2015.

launched its 5G roadmap.[82] 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, followed by the launch of the allocation procedure in late 2019.[83] As of April 2020, Bouygues Telecom, Free Mobile, Orange and SFR had qualified to participate in the auction for allocation of frequencies.[84] The auction for the award of 3,490–3,800MHz band was closed on 1 October 2020.[85]

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 the selection procedures, which have always been in the form of calls for applications to date.

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.[86]

Private radio broadcasters must, in principle, dedicate at least 40 per cent of their musical programmes to French music.[87]

82 See: https://www.economie.gouv.fr/files/files/Actus2018/Feuille_de_route_5G-DEF.pdf.

83 See ARCEP Draft Decision of 15 July 2019 proposing the procedure for awarding the 3,490–3,800MHz band in Metropolitan France.

84 See ARCEP press release of 2 April 2020.

85 See ARCEP press release of 1 October 2020.

86 Articles 7 and 13 of Decree No. 90-66 of 17 January 1990.

87 Article 28 2°-*bis* of the Law of 30 September 1986.

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.[88]

Law No. 2018-1202 of 22 December 2018[89] 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 disturb public order or alter polls' reliability. Operators must implement easily accessible and visible systems that will allow users to report such false information, including when they are financed by third parties.

Decree No. 2020-984 dated 5 August 2020 relaxed certain rules regarding the broadcast of films, increasing the maximum number of hours allotted per year.

ii Advertising

Advertising in television broadcasting is subject to strict regulations in France.[90] In particular, advertising must not disrupt the integrity of a film or programme, with 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.

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

Media owners are also subject to transparency requirements in order to protect advertisers of digital advertisement. According to Article 2 of the Decree No. 2017-159 dated 9 February 2017, 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.

Decree No. 2020-983 dated 5 August 2020 introduced a relaxation of certain rules regarding publicity by authorising segmented advertisement and advertisement for the movie industry on television.

iii Online representation of content

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.[91]

88 Article 56 of the Law of 4 August 2014.

89 Law No. 2018-1202 of 22 December 2018 regarding the fight against the manipulation of information.

90 Decree No. 92-280 of 27 March 1992.

91 Directive 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market.

France 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.[92]

It introduces new provisions under the French Intellectual Property Code 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 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. The Law specifies 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'.

VI THE YEAR IN REVIEW

i The transposition of the European Electronic Communications Code and the Audiovisual Media Services Directive

A legislative bill transposing both the EECC and the AMSD is currently being debated before the National Assembly.[93] According to the proposed bill, major revisions required under the EECC, such as the regulation of OTT services, new consumer protection obligations to be imposed on electronic communications providers, as well as those required under the AMSD, such as the regulation of online video platforms and the investigatory powers of the CSA, are to be adopted through ordinance.[94] The same bill, however, aims to directly transpose requirements regarding the expansion of universal services to cover high-speed internet access and voice services.[95]

92 Law No. 2019-775 of 24 July 2019.

93 Bill including various provisions for the application of the law of the European Union in economic and financial matters (ECOM1935457L).

94 ibid., Articles 24 *ter* and 26.

95 ibid., Article 27.

ii Hate speech regulations

Following the adoption of Law No. 2018-1202 of 22 December 2018[96] with regard to 'fake news', another law regarding content regulation, Law No. 2020-766 of 24 June 2020 regarding hateful content on the internet has been enacted. Law No. 2020-1202 created additional obligations for platform operators to delete child pornography and terrorist content within one hour when notified by the relevant authority, and to delete any hateful content that is 'obviously illicit' within 24 hours when notified by any end user. However, these obligations were found to be unconstitutional and invalidated by the French Constitutional Court.[97]

iii Additional 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.[98]

This decision was appealed by Google, but subsequently confirmed by the French Supreme Administrative Court.[99]

The CNIL continues to act as an active regulatory authority, and has recently imposed its first sanction as a lead supervisory authority (Article 60 of the GDPR) in July 2020.[100]

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.[101] This guidance was partially struck down by the French Supreme Administrative Court,[102] prompting the adoption of amended guidelines and new recommendations.[103]

The modified guidance largely reiterates the data protection principles already applied by the CNIL on previous occasions. 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, and withdrawal of consent must be as easy as giving consent.

96 Law No. 2018-1202 of 22 December 2018 regarding the fight against the manipulation of information.

97 Cons. Const. 18 June 2020, No. 2020-801.

98 CNIL Decision No. SAN - 2019-001 of 21 January 2019 imposing a pecuniary sanction against GOOGLE LLC.

99 Conseil d'Etat, 19 June 2020, req. No. 430810.

100 CNIL decision No. SAN – 2020-003 of 28 July 2020 regarding SARTOO SAS corporation.

101 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).

102 Conseil d'Etat, 19 June 2020, req. No. 434684.

103 CNIL decision No. 2020-091 of 17 September 2020 adopting guidelines on the application of Article 82 of the amended law dated 6 January 1978 modified to the reading or writing operations in a user's terminal (in particular cookies and other tracking devices) and abrogating decision No. 2019-093 of 4 July 2019; CNIL decision No. 2020-092 of 17 September 2020 adopting a recommendation proposing the practical modalities of compliance for the use of 'cookies and other tracking devices'.

'Cookie walls' as well as whether audience management cookies or performance cookies may be exempted from the opt-in consent requirement are now subject to a case-by-case review. The CNIL also recommends operators give users the opportunity to periodically renew their consent, for example, every six months.

Further clarifications on information obligations are provided in the new guidance documents. The identity of every third-party cookie provider must now be communicated to users, as well as greater details regarding the cookies' functionalities.

The CNIL announced that website providers will have until March 2021 to comply with the new guidelines.

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

The saga surrounding the implementation of Article 15 of the Copyright Directive under French law continues. As the national law did not prohibit the assignment of a licence free of cost, Google decided to withdraw longer displays of copyrighted content unless the rights holders agreed to give free authorisation. In April 2020, the FCA ordered Google to enter into good faith negotiations with publishers to decide on remuneration for the display of copyrighted content in Google News or Search.[104] Google lodged an appeal before the Paris Court of Appeal, which confirmed the FCA's order in a decision dated October 2020.

vi The creation of a national Pole of Expertise on Digital Regulation (PEReN)

On 31 August 2020, the creation of a national Pole of Expertise on Digital Regulation (PEReN) was announced.[105] The PEReN will be in charge of providing expertise regarding the regulation of digital platforms, in particular regarding the technical aspects including data analysis, data sharing, algorithmic processing and data science.

VII CONCLUSIONS AND OUTLOOK

With the national transposition of the EECC and the AMSD still underway and the unsettled questions surrounding the Digital Services Act remaining at the European Parliament, significant changes are expected in the French TMT regulatory framework in the year to come. The inclusion of the OTT services under the telecommunications regulations, new regulations regarding platforms, and implementation of provisions transposing the Copyright Directive are only few of the moving pieces that can have a large impact on the legal landscape. Content regulation and the reshuffling of regulatory authorities are two other areas that should also be closely monitored.

104 FCP decision 20-MC-01 of 9 April 2020 on requests for interim measures by the Syndicat des éditeurs de la presse magazine, the Alliance de la presse d'information générale and others and Agence France-Presse.

105 Décret No. 2020-1102 du 31 août 2020 portant création d'un service à compétence nationale dénommé 'Pôle d'expertise de la régulation numérique' (PEReN)

Appendix 1

ABOUT THE AUTHORS

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 proven expertise in complex commercial litigation matters and clients in different industry sectors namely in IT and other technology-related sectors. 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 former global co-chair of the technology industry group within the firm and aims at unlocking the global platform around data protection issues globally.

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 cited in *Chambers Europe* and *The Legal 500 Paris* as 'exceptional', 'whose negotiating skills and expertise are remarkable', as 'very sharp and down-to-earth' and with 'very good knowledge of the industry'. He advises high-profile French and international groups on large outsourcing, telecommunication and system integration projects.

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
www.lw.com

Chapter 7

GERMANY

Joachim Grittmann[1]

I OVERVIEW

With an annual business volume of approximately €260 billion in 2018, the ICT sector did not only increase business volume by 3.6 per cent compared to 2017; it is also one of the largest economic sectors in Germany, employing already more than 1.2 million people.[2] ICT has become a driving force in Germany's economy, contributing to 4.8 per cent of the national gross value-added services in 2018.[3]

By focusing on key issues such as convergence, mobility, data protection and internet security, the government has tried to advance the information society through targeted policies to modernise legal and technical frameworks and to promote research and market-oriented development over the past decade. As part of this overall effort, the federal government has adopted specific programmes and strategies tailored to the needs of the ICT sector. On 20 August 2014, it concluded the Digital Agenda 2014–2017, focusing on a strategy for the digital future of Germany,[4] which was extended by the Digital Strategy 2025[5] in 2016. In the current coalition agreement, politicians have set the goal of supplying the whole of Germany via gigabit networks by the end of 2025.[6]

The Digital Agenda further includes topics such as digital security and the Strengthening Industry 4.0 initiative. Beyond that, ethical aspects in the ICT sector are increasingly moving into the political spotlight.[7]

---

1 Joachim Grittmann is a counsel at Latham & Watkins LLP.

2 www.bmwi.de/Redaktion/DE/Artikel/Branchenfokus/Wirtschaft/branchenfokus-informationstechnik-und-telekommunikation.html.

3 https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/ikt-branche-2018.pdf?__blob=publicationFile&v=6, p. 3.

4 www.bundesregierung.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf?__blob=publicationFile&v=6.

5 www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-strategie-2025,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.

6 See also https://www.bmvi.de/DE/Themen/Digitales/Breitbandausbau/Breitbandfoerderung/breitbandfoerderung.html.

7 On 18 July 2018, the German Federal Government set up the Data Ethics Commission (DEK), which is responsible for ethical standards and guidelines. A first report was published in 2019; see https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/datenethikkommission/ datenethikkommission- node.html.

II REGULATION

i The regulators

All television and radio broadcasters are subject to state control. Public service broadcasters are supervised by internal committees: content-related supervision is carried out by the respective broadcasting council. The respective administrative board, which is appointed by the broadcasting council, supervises all management decisions made by the director. Private broadcasters, in contrast, are subject to external supervision. The competent authority is the respective state media authority of each German state,[8] whose responsibilities – apart from supervision – include granting authorisations and assigning transmission capacities.[9] They also have a wide range of powers to supervise broadcasters, such as warnings, prohibitions, or withdrawals and revocations of licences.[10]

The state media authorities work together in a committee concerning licensing and supervision as well as in the development of private broadcasting on fundamental questions, primarily with a view to the equal treatment of private TV and radio broadcasters.[11]

The state media authorities are also responsible for the compliance of private TV and radio broadcasts with basic programming principles. They supervise the observance of regulations on advertising limitations, the protection of minors and the protection of pluralism. Their tasks are carried out by several committees.

The main regulator in the area of telecommunications is the federal legislator due to the competence regarding telecommunications. Important federal laws are the Telecommunications Act (TKG) and, for telemedia services, the Telemedia Act (TMG).

The compliance of telecommunications companies with the TKG is monitored by the Federal Network Agency (BNetzA). The Agency ensures the liberalisation and deregulation of the telecommunications, postal and energy markets through non-discriminatory access and efficient use-of-system charges. It is responsible, inter alia, for securing the efficient and interference-free use of frequencies and protecting public safety interests. Apart from regulation, the BNetzA performs a number of other tasks related to the telecommunications market such as administering frequencies and telephone numbers.

The Federal Commissioner for Data Protection and Freedom of Information (BfDI) is responsible for the supervision of data protection at telecommunications companies insofar as they provide telecommunications services.[12]

8 Four states have joint media authorities: Berlin and Brandenburg as well as Hamburg and Schleswig-Holstein.

9 Section 50 et seq. of the Inter-State Broadcasting Treaty (RStV).

10 Section 38(2) of the RStV.

11 The goals and remits of this cooperation are laid down in the Contract on the Cooperation of the Media Authorities in the Federal Republic of Germany. The focus is on promoting programming diversity, and thus freedom of information and opinion in private television and radio. This involves, in addition to controlling media power by means of licensing limitations and licence monitoring, the promotion of media literacy among viewers and listeners.

12 Whereas other data processing activities in the ICT area is are supervised by local data protection authorities.

ii Main sources of law

The use and distribution of media and telecommunications are first of all protected by fundamental rights. The Basic Law (GG) guarantees the freedom of information, the freedom of the press for journalists and publishers, as well as the freedom of broadcasting and film (Article 5(1)) and the freedom of art (Article 5(3)). Furthermore the GG guarantees the secrecy of telecommunications.

Broadcasting law is the responsibility of the 16 federal states. They have agreed on a fundamental treaty regulating the legal framework, the State Treaty on Broadcasting (RStV). The 22nd amendment to the RStV came into effect on 1 May 2019.[13] However, the RStV will be replaced by the State Treaty on Media (MStV), which has already been passed. This serves primarily to adopt the Audiovisual Media Services Directive 2010/13/EU and is scheduled to come into force at the end of 2020.

Further legal sources, at the level of the federal states, are various other interstate treaties, such as the Interstate Treaty on the Protection of Minors in Broadcasting and in Telemedia (JMStV).

In addition, broadcasting is regulated in the TMG, which includes in particular the transmission of media via the internet.

Telecommunication law lies in the shared competence between the EU and the Member States.[14] The EU has issued several regulations and directives relating to this matter.[15]

Germany adopted the most important regulations in particular in the TKG. The next reform of the TKG will be comprehensive and will adopt the EECC requirements.

iii Regulated activities

Private and public television broadcasting is governed by the RStV, which outlines the side-by-side existence of public and private broadcasting. All private broadcasters require a licence for the purpose of providing broadcasting services.[16] According to the RStV, the provider of an electronic information and communications service – if it is categorised as a broadcast – requires a licence as well.[17] If the competent state media authority determines that this is the case, the provider, after being notified of this classification, must at his or her choice either submit a licence application within three months or change the service in a way that it is no longer qualified as a broadcast.

When providing telecommunication or network services, operators have to adhere to the TKG. The TKG does not generally oblige telecommunications services or network

13 See https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Rundfunkstaatsvertrag_RStV.pdf.

14 Article 4(2) lit. h, 170 et seq. TFEU.

15 e.g., Roaming Regulations (EU) 531/2012, the Universal Service Directive 2002/22/EC, the Access Directive 2002/19/EC, European Electronic Communications Code Directive (EU) 2018/1972 (EECC), which has to be adopted by the Member States by 21 December 2020 (Article 124 EECC).

16 Section 20(1) RStV.

17 Section 20(2) RStV.

providers to apply for a licence; however, it requires them to notify the BNetzA when they start to provide the services or the network.[18] It is not unequivocal in each case which services are exempt from a notification.[19]

iv Ownership and market access restrictions

German law provides for certain restrictions on foreign investments. The Federal Ministry of Economics and Technology (BMWi) may prohibit transactions that might interfere with German or foreign interests according to Section 4 of the Foreign Trade Law (AWG) and Section 55 et seq. of the Foreign Trade Law Ordinance (AWV). The scope of the foreign investment control has developed in the last years by stipulating a list of particularly sensitive business areas which relate to critical infrastructures[20] and which, depending on certain threshold values, explicitly cover specific ICT activities.

The TKG imposes certain obligations on telecommunications service providers and network operators. Agreements relating to telecommunications services and network access can be negotiated freely[21] with providers and operators, unless one party has significant market power (in which case, price terms and access obligations are regulated by the TKG; a provider with significant market power is not able to choose its customers freely).[22]

The RStV contains special ownership control provisions[23] that are designed to achieve media-plurality objectives. These rules apply in addition to the general merger control regime under German and European competition law and are administered by the Commission on Concentration in the Media. Section 11d (2) No. 3 RStV further states that public broadcasting companies are not entitled to offer non-broadcasting-related print media. Criteria to evaluate content are to what extent the offer meets a democratic, social and cultural need of society, whether the offer will contribute to journalistic competition and the financial costs.

Since 2012, proceedings concerning the Tagesschau-App have been ongoing. Publishing houses claimed that the Tagesschau-App provides a high amount of non-broadcasting-related textual content and therefore has a competition-distorting effect. On 30 April 2015, the Federal Court of Justice (BGH) held that not only the concept of the App has to comply with the RStV, but also the specific content, which is subject to full judicial review.[24] If broadcasting and non-broadcasting elements are implemented, it is necessary to determine the focus. On 30 September 2016, the Higher Regional Court of Cologne (OLG Köln) came to the conclusion that the app content on the relevant day was not sufficiently broadcasting-related but equivalent to print media and hence not permitted.[25] In 2018, the BGH did not accept the appeal of the decision, ultimately bringing the case before the Federal Constitutional Court (BVerfG).[26]

18 Section 6 TKG.

19 The BNetzA publishes a list of notified undertakings at regular intervals: https://www.bundes-netzagentur.de/EN/Areas/Telecommunications/Companies/Notification/ NotificationRequirement-node.html.

20 Listed in the BSI-Kritis Ordinance, https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/bsi-kritis-ordiance-poster.pdf?__blob=publicationFile&v=4.

21 e.g., access, payment terms, currency and billing.

22 See Sections 21 and 28 TKG.

23 Section 25 et seq. RStV.

24 BGH ruling of 30 April 2015 – I ZR 13/14 – GRUR 2015, 1228 et seq.

25 OLG Köln ruling of 30 September 2016 – 6 U 188/12 – GRUR 2017, 311().

26 MMR-Aktuell 2018, 402395.

v Transfers of control and assignments

The German merger control provisions are enforced by the Federal Cartel Office (BKartA). The current legislation can be found in Chapter VII of the Act Against Restraints of Competition (GWB), which deals with the control of concentrations affecting the German market. In addition, Section 101 et seq. of the TFEU and the EC Merger Regulation apply.[27]

The filing of merger notifications in Germany is mandatory if the turnover thresholds according to Section 35(1) of the GWB are met and none of the *de minimis* exemptions apply.[28] If the statutory conditions for prohibition are fulfilled, the BKartA will prohibit the merger or order the divestment or disposal of certain assets of a completed merger.

Mergers that are subject to merger control may not be completed before either the BKartA has cleared the transaction or the relevant waiting periods of one month (first phase) or four months (first and second phases together) after submission of a complete notification have expired without the BKartA having prohibited a transaction.

There are no legal deadlines for a notification of a concentration, but notifiable concentrations must not be completed before clearance. Therefore, it is advisable to submit a notification well before the envisaged completion date. It is possible to file a pre-merger notification even prior to the signing of the transactional documents. Furthermore, parties should not forget to submit the mandatory post-completion notice to the BKartA, which needs to be filed without undue delay following completion of the transaction.[29] In principle, all parties involved in a merger are responsible for filing.

Submission of an incorrect or incomplete filing, failure to submit a post-merger completion notice, or cases of incomplete, incorrect or late notices, constitute administrative offences and can lead to a fine of up to €100,000.

The BKartA can also consider services provided without remuneration and scaling effects in its assessment of market share or market power, and the threshold for merger control is a transaction value of €400 million.[30]

27 Council Regulation (EC) No. 139/2004 of 20 January 2004 on the control of concentrations between undertakings, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32004R0139.

28 Two *de minimis* exemptions apply under the following conditions:

a one party to the merger achieved less than €10 million turnover during the preceding fiscal year (in the case of the target including the seller and all its affiliates, provided that the seller controls the target and, in the case of the acquirer, including all its affiliates) (Section 35, Paragraph 2); or

b the relevant market (which must have been in existence for at least five years) had a total annual value of less than €15 million in the previous calendar year (*de minimis* market clause, Section 36, Paragraph 1).

29 See *Getting the Deal Through – Merger Control*, https://gettingthedealthrough.com/area/20/ jurisdiction/11/ merger-control-germany.

30 Cf. Section 18 (3a) and Section 35 (1a) GWB; cf. also Seeliger/deCrozals, ZRP 2017, 37.

III TELECOMMUNICATIONS & INTERNET ACCESS

i Internet and internet protocol regulation

All IP-based services are regulated under the TMG.[31] Commercial rules for telemedia are covered in the TMG, while aspects relating to journalistic content are regulated in the RStV[32] and the JMStV. Telemedia services are permission-free and generally do not need to be registered.

Telecommunications services and telemedia services are mutually exclusive; therefore, telecommunications are excluded from the scope of the TMG. In practice, the distinction is often difficult to make. When granting access to the internet, a distinction must be made according to the services and functions offered by the provider. If the provider restricts itself to the exclusive data transmission of third-party content from the internet to the user and does not prepare any content, this constitutes a telecommunications service and thus not a telemedium.

ii Universal service

Broadband availability continues to increase steadily throughout Germany. At the end of 2019, about 92 per cent of households connected with broadband connections of at least 50Mbit/s. Over 43 per cent of households have gigabit (1,000Mbit/s) connections. Bandwidths of at least 200Mbit/s are available for about 75 per cent of households. While the increasing use of super-vectoring technology has contributed to increased availability in the bandwidth classes up to 200Mbit/s, the expansion of cable TV networks (CATV) based on the new DOCSIS 3.1 technology and the expansion of FTTB/H fibre optic networks are driving growth in the higher bandwidth classes. However, LTE coverage can still be improved in Germany. The network operators had promised to provide LTE network coverage of 98 per cent (by population) nationwide by the end of 2019. In each federal state, 4G coverage had to be at least 97 per cent. According to a recent inquiry by the BNetzA from May 2020, this proof could not be provided by the network operators in all federal states.[33]

The federal government intends to give a further boost to the development of the broadband network by, for example, capitalising on synergies in the construction of infrastructure, using the digital dividend[34] and formulating regulations that foster investments. Various initiatives exist at the federal, state and local levels.[35]

Moreover, the federal government encourages projects to pursue industry solutions. For example, small and medium-sized telecommunications companies can borrow funds on privileged terms and with adequate risk pricing through the corporate financing programme of Germany's state-owned development bank.[36]

31 Adopted on 18 January 2007 and last amended on 11 July 2019.

32 Section 54 et seq. RStV.

33 While some states are nearly 100% covered, others have only 80.7% coverage or even less: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_ Institutionen/Frequenzen/OeffentlicheNetze/Mobilfunknetze/mobilfunknetze-node.html.

34 That is digitisation ending up in freeing up spectrum and usually resulting in its reallocation.

35 e.g., the German broadband initiative, the Netalliance Digital Germany initiative and Zukunftsoffensive Gigabit Germany; the Netalliance Digital Germany initiative started on 7 March 2014.

36 www.kfw.de/inlandsfoerderung/Unternehmen/Erweitern-Festigen/Breitbandnetze-finanzieren.

In any event, the existing federal and state loan guarantee scheme is generally available to companies in the telecommunications sector to prevent economically desirable broadband projects from failing as a result of the lack of suitable financing.

White areas[37] are shrinking rapidly, partly thanks to ongoing investment by the network operators. The reduction has also largely been achieved thanks to the hosting of action programmes offered by the federal states, local authority broadband initiatives in those areas, and the nationwide activities of associations such as the German Association of Internet Enterprises,[38] the Association of the Providers of Telecommunications and Value-Added Services[39] and the Association of Towns and Municipalities.[40]

The next revision of the TKG is expected to make a further contribution to broadband expansion.[41] For example, the federal government is planning a right to fast internet access based on criteria defined by the BNetzA. In addition, certain sanctions will be laid down in the event that a network operator fails to deliver the guaranteed transmission rates. In order to drive the expansion forward, the revision also aims to implement the newly permitted, more comprehensive regulatory incentive mechanisms from the EECC.[42]

iii Restrictions on the provision of service

An amendment of the TKG in 2012 initially introduced the concept of net neutrality. The federal government was authorised to draft a regulation that sets out, inter alia, the requirements for non-discriminatory data transmissions.[43] However, with the entry into force of the European Net Neutrality Regulation,[44] a national regulation was no longer pursued and the TKG provision was repealed. Article 3 of the Net Neutrality Regulation provides, inter alia, that providers of internet access shall treat all traffic equally, but permits reasonable traffic management measures provided these are transparent, non-discriminatory and proportionate, and are not founded on commercial considerations. The BEREC[45] published guidelines for the implementation of the obligations of national regulatory authorities.

An example of controversial restrictions on network provisioning is the reduction of the internet speed on mobile phone plans. In Germany, mobile phone plans usually only grant few gigabytes[46] of traffic with full speed. Having exceeded this data amount, Internet-speed will be reduced to 16 or 32kbit/s. For some years, mobile network carrier offered so called 'passes', which exclude certain music streaming services or social media services from this amount of data.[47] In 2018, the BNetzA prohibited certain conditions of a zero-rating mobile tariff option, which has been challenged by the provider. The Administrative Court of Cologne referred questions to the European Court of Justice

37 White areas are rural areas in Germany that still lack high-speed internet connections.

38 www.eco.de.

39 www.vatm.de.

40 www.dstgb.de.

41 https://www.heise.de/news/TKG-Novelle-Verzoegerung-beim-Recht-auf-schnelles-Internet-4865581.html.

42 https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/fortentwicklung-telekommunikationsregulierung-1546632.

43 See former Section 41a(1) of the TKG.

44 European Net Neutrality Regulation 2015/2120/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2120.

45 Body of European Regulators for Electronic Communications.

46 Usually 1 to 15 GB.

47 Known as 'zero-rating' or 'zero tariff'.

(CJEU), which has not been answered yet.[48] In a second case, regarding the reduction of internet speed by a provider, the same Court also referred a question to the CJEU concerning the conformity with Article 3 of the Roaming Directive.[49] In a recent ruling, the CJEU states that 'the requirements to protect internet users' rights and to treat traffic in a non-discriminatory manner preclude an internet access provider from favouring certain applications and services by means of packages enabling those applications and services to benefit from a "zero tariff" and making the use of the other applications and services subject to measures blocking or slowing down traffic'.[50]

Finally, the UWG provides restrictive provisions regarding unsolicited calls, emails and text messages.[51] Making first contact with consumers by such measures requires, as a general principle, the explicit approval of the consumers.[52]

iv Privacy and data security

Privacy

The protection of personal data in the ITC area is governed by (1) the EU General Data Protection Regulation (GDPR), (2) the Federal Data Protection Act (BDSG) as well as (3) sector-specific telecommunications and telemedia laws. The regulation is supervised by the BfDI, data protection authorities on federal states level and partly the BNetzA.

In a 1983, the BVerfG developed a right to privacy as an element of the general right to free development of one's personality, which is protected under Article 2(1) in conjunction with Article 1(1) GG. Until 2018, the protection of individuals regarding the processing of their personal data was laid down in local data protection law, especially the BDSG.

With the enactment of the GDPR further strengthening individual rights and meeting the challenges of globalisation and new technologies, the BDSG was also heavily amended and revised with effect from 25 May 2018. The GDPR is a uniform framework laying down principles for legitimate data processing in the EU and the EEA. Compared to the predecessor Data Protection Directive (95/46/EC), the GDPR entails significantly stricter requirements for data protection. The GDPR introduced substantial sanctions for non-compliance and, depending on the nature of the infringed provision, may consist of civil liabilities, criminal sanctions or administrative fines. Administrative fines can amount to €20 million or up to 4 per cent of the total worldwide annual revenue, whichever is higher, for each violation.

In addition, both the TKG and the TMG provide sector-specific privacy rules. The TMG provides a legal framework as regards online privacy including requirements for the collection and further processing of usage and location data. The TKG provides rules for telecommunication service provider including requirements for collection and further processing of traffic and location data. Section 88 TKG stipulates provisions pertaining to the telecommunication secrecy (content data and partly traffic data). With the announced

48 Administrative Court of Cologne decision of 19 November 2019 – 9 K 8221/18 – https://www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/Archiv/2019/26_191119_01/index.php.

49 Administrative Court of Cologne decision of 20 January 2020 – 9 K 4632/18 – https://www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/03_200121/index.php.

50 CJEU Press Release No. 106/20: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-09/cp200106en.pdf.

51 Section 7 UWG.

52 Fines can be as high as €300,000; see Section 20(1) and (2) UWG.

renewal of the telecommunications laws it is discussed whether the TMG and TKG data protection rules may be consolidated in a new sector-specific act for electronic communication, telemedia and telecommunications.

Data security

Data security in Germany is governed by the Law on the Federal Office for Information Security (BSIG), sector-specific regulations in the TKG as well as the the GDPR. A major amendment of the BSIG has been made in 2015, aiming at an improvement in the IT security of critical infrastructure[53] including ICT infrastructure. Parts of the BSIG strengthen the position of the Federal Office for Information Security (BSI) as described below, while other sections impose obligations on private entities maintaining critical infrastructure that are relevant for common welfare.

The BSI is a superior federal authority with wide-ranging tasks of threat prevention in IT systems. The BSI tasks include developing criteria, procedures and tools to test and evaluate the security of information technology systems and components. Therefore, the BSI is the central reporting office for disruptions and attacks on IT systems in private enterprises.

The BSIG especially imposes obligations on private enterprises to safeguard IT security, such as the duty to report disturbances in IT systems to the BSI. Private enterprises that are subject to these obligations are, in particular, operators of critical infrastructure in the energy, like the IT and telecommunication sectors. Within two years of the BSIG coming into force, they had to upgrade their IT systems to make them state of the art, and from then on must prove their compliance once every two years through security audits or certificates.[54]

Operators of telecommunication services have the duty to inform their customers of any IT security risk, and to provide information on solutions for these problems.[55] Telemedia services operators must ensure that their users are protected from attacks on IT security through state-of-the-art technical and organisational means.[56]

The EU Commission has adopted several measures to prepare Europe against cyber incidents. In particular, the Directive on Security of Network and Information Systems (NIS Directive) was the first EU-wide legislation on cybersecurity.[57] It includes measures to ensure a high common level of network and information security across the EU. The NIS Directive was implemented into German law on 29 June 2017.[58]

On 27 March 2019, the German Federal Ministry of the Interior proposed a new bill for an IT Security Act 2.0 (IT-SiG 2.0). The IT-SiG 2.0 aims, inter alia, to further strengthen the BSI by transferring new competences. It also prescribes additional obligations

53 Further defined in the BSI KRITIS Ordinance; see above Fn. 19.

54 Section 8a BSIG.

55 Section 109a(4) TKG.

56 Section 13(7) TMG.

57 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

58 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148. Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6 Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, BGBl, 2017, 1885, https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s1885.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1885.pdf%27%5D__1600694321765.

on manufacturers, providers and operators of critical infrastructure while introducing stricter penalties. A new draft of the bill was published in May 2020 further strengthening the position of the BSI.[59]

The BNetzA has published a revised catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data pursuant to Section 109 TKG (Version 2.0).[60]

Data retention for the purpose of inner security

Since the BVerfG rendered data retention of traffic data as intended under the TKG of 2007 to be unlawful,[61] the question of whether and to what extent data retention is in line with national and European law has been discussed widely. The CJEU decided similarly that European Directive 2006/24/EC setting out the framework for data retention is invalid.[62] After two drafts of a German data retention act in 2011 and 2013 were not adopted, a new law came into force on 18 December 2016.[63] However, further legal proceedings prevented the retention of traffic data. In proceedings for interim relief before the Higher Administrative Court of Münster, a telecommunications service provider obtained a temporary exemption from the retention obligation.[64] In response to this decision of 22 June 2017, the BNetzA declared that until final clarification in the main proceedings, telecommunications providers who do not comply with the retention obligation as of 1 July 2017 will not be held responsible under supervisory law. In its ruling of 20 April 2018, the Cologne Administrative Court followed the Higher Administrative Court. The Court found that the plaintiff – a telecommunications service provider – is not obliged to retain the telecommunications connection data of its customers in the context of data retention because the statutory provisions are not compatible with EU law. On 25 September 2019, the Federal Administrative Court (BVerwG) decided to refer the final interpretation of the Data Protection Directive for Electronic Communications (Directive 2002/58/EC) to the CJEU.[65] Pending final clarification in Luxembourg, data retention in Germany remains suspended. In addition, several constitutional complaints against the 2015 law are currently pending before the BVerfG in Germany.

Where the journey before the CJEU could take us is shown by the Opinion of the Advocate General of 15 January 2020 in similar proceedings. The Advocate General considers the current rules in France, the United Kingdom and Belgium violating EU law. From his point of view, the retention of telephone and internet connection data to be lawful only to a very limited extent.[66]

59 https://intrapol.org/wp-content/uploads/2020/05/200507_BMI_RefE_IT-SiG20.pdf.

60 The draft has been notified to the EU Commission: https://ec.europa.eu/growth/tools-databases/tris/de/search/?trisaction=search.detail&year=2020&num=496.

61 BVerfG ruling of 2 March 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 – BeckRS 2010, 46771.

62 CJEU ruling of 8 April 2014 – C-293/12 and C/594/12 – BeckEuRS 2014, 393023.

63 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, BGBl 2015, 2218, www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&bk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%2527bgbl115s2218.pdf%2527%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s2218.pdf%27%5D__1471357640831.

64 Higher Administrative Court of Münster decision of 22 June 2012 – Az. 13 B 238/17 – NVwZ-RR 2018, 43.

65 BVerwG ruling of 25 September 2019 – Az. 6 C 12/18 – NVwZ 2020, 1108.

66 https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-01/cp200004en.pdf.

Enforcement of law in social networks

With effect from 1 January 2018, the Network Enforcement Act (NetzDG) was implemented to secure and improve the enforceability of penalties against unlawful contact on significant social media platforms. Social network providers are obliged to combat fake news and hate speech by blocking, and to remove unlawful content. Furthermore, it is required that a transparent, accessible and effective procedure for users to report unlawful content has to be established under which social network providers have to report biannually.[67]

Protection of children

Youth protection provisions applicable to the media can primarily be found in the Law for the Protection of the Youth (JuSchG) and the JMStV.

The Federal Department for Media Harmful to Young Persons (BPjM) is the authority responsible for protecting children and adolescents from media[68] that might contain harmful or dangerous content under the JuSchG. The BPjM can act only at the request of other administrative institutions. Once an official request has been filed, the BPjM is obliged to process the complaint. Possible measures in the event of a violation are a prohibition on publication, blocking the provider and fines of up to €500,000.

The JMStV forms the legal basis for assessing content distributed in broadcast or media services. The compliance of broadcast and media services with the JMStV is controlled by the Commission for the Protection of Minors in the Media (KJM). The JMStV distinguishes between illegal content and content that impairs the development of minors: illegal content must not be distributed via broadcasting or media services. Content that is rated as impairing the development of minors (e.g., a severe depiction of violence) is subject to access restrictions. In the event of a breach of the provisions of the JMStV, the KJM decides on the sanctions to be imposed against the respective media content provider.[69]

IV SPECTRUM POLICY

i Development

Originally, frequencies in Germany were used – with a few exceptions – by Germany's federal mail service, Deutsche Bundespost. Since 1996, however, the markets for network and telephony have been fully liberalised.

Today's development goes hand in hand with the population's increasing demand for mobile communication services. Not least because of the technical possibilities opened up by, inter alia, UMTS and LTE, demand for more bandwidth will continue to rise in line with increasing mobility. Growing demand and technological innovation both call for the availability of an adequate frequency spectrum. The next generation of mobile network – 5G

67 Failure to comply with the obligations may result in fines of up to €50 million.

68 The types of media monitored include, inter alia, videos, books, computer games and websites.

69 The measures depend on the severity of the breach, and can range from a complaint against the content provider to fines. The issue may even be handed over to the State Prosecutor.

– is already being realised. Since the current allocations for the 800MHz, 1,800MHz and 2.6GHz frequencies will expire by 31 December 2025, there is a public inquiry being carried out to guarantee early availability of suitable frequencies for high-performance networks.[70]

ii Flexible spectrum use

The use of a spectrum requires its prior allocation.[71] The TKG states that the allocation of spectra shall be regulated by a Spectrum Regulation, and requires the Federal Council's consent.[72] Based on the allocation of frequencies and the specifications set out in the Spectrum Regulation under Section 53 TKG, the BNetzA shall divide the spectrum ranges into spectrum uses and related terms of use.[73] Spectra for wireless access to telecommunication networks must be assigned in a technologically and service-neutral manner.[74]

The TKG provides the framework for a flexible use of allocated spectra. Owners of an allocated frequency have the possibility to trade their frequency, and to let third parties use their frequency, for example, by way of a lease, co-use or in the form of a joint use via spectrum pooling. It is necessary, however, that the BNetzA releases such forms of use for flexible use and specifies the corresponding conditions.[75]

iii Broadband expansion through spectrum auctions

A few rural areas in Germany still lack high-speed internet connections. Thus, the federal government concentrates on the development of the broadband network towards a fibre-optic network with planned investments of €100 billion by 2025.[76]

If the BNetzA finds that the number of available spectra is not sufficient for their allocation, it can order that the allocation of frequencies be preceded by a procurement procedure.[77] Often, the procurement is held in the form of a spectrum auction, which is organised by the BNetzA.[78]

On 12 June 2019, the latest auction of mobile broadband spectrum ended following 497 bidding rounds over seven weeks.[79] The auction of 5G-frequencies in the fields of 2 and 3.6GHz aggregated a total amount of approximately €6.5 billion.

70 Frequency Compass (Frequenzkompass), https://www.bundesnetzagentur.de/DE/ Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OeffentlicheNetze/Mobilfunknetze/mobilfunknetze-node.html.

71 Section 55(1) TKG.

72 Section 53(1) TKG.

73 Section 54(1) TKG.

74 Section 54(2) TKG.

75 Section 62(1) and (2) TKG; also see Scherer/Heinickel, NVwZ 2012, 585 (591f).

76 https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/netzallianz-digitales-deutschland.pdf?__blob=publicationFile.

77 Section 55(10) TKG.

78 Section 61 TKG.

79 After the merger of Telefónica and E-Plus in the summer of 2014, only four operators (Drillisch, Telefónica, Telekom and Vodafone) were allowed to bid.

V MEDIA

i Regulation of media distribution generally

Media distribution is currently mainly regulated by the RStV.[80] The regulation differs according to the different persons involved. In the future, the focus will be primarily on the intermediaries.

Various aspects of regular distribution are regulated, such as product placement. For example, Sections 7, 15 and 44 of the MStV deal with permissible and impermissible product placement. According to these provisions, product placement is generally prohibited and may only be carried out with a clear indication and without significant influence on the editorial responsibility and independence of the content.[81]

ii Internet-delivered video content

In future, internet-delivered video content will be more strictly regulated at the level of intermediaries and slightly less regulated at the level of content creators. The new MStV stipulates that intermediaries (in particular very large video platforms) will operate completely non-discriminatorily in the future. To ensure this, increased transparency requirements and obligations to state reasons are established. The European Commission also released the Guidelines on Video Sharing Platforms 2020/C 223/02.[82]

The need for a broadcasting licence according to the RStV for streamers or influencers is a particularly controversial and difficult topic. Up to now, the legal framework of these broadcasting licences has been almost exclusively designed for TV broadcasts, from which online streaming usually differs significantly. The requirements for the need of a broadcasting licence have so far been – for online streaming – relatively low. A live-stream ('linear') with more than 500 potential viewers and editorial design[83] as well as regular broadcasting is sufficient.[84] In the new MStV in particular the spectator requirement is raised to 20,000 persons. In addition, such offers, which have only a small meaning for the formation of opinion, are in the future excluded from the requirement.

VI THE YEAR IN REVIEW

In 2019, the CJEU ruled on two noteworthy cases, which originate in the increased regulation by the BNetzA. Both concern whether or not over-the-top services (OTT) are electronic communications services. OTT services use the internet to provide special communication services such as email or internet-calls (VoIP), regardless of the internet provider.

80 The RStV will soon be replaced by the MStV.

81 For example, a private broadcaster recently broadcast a certain format for one week under the theme of a current motion picture. During the broadcast, excerpts of the new film were shown and scenes were re-enacted. The State Media Authority declared a violation of the RStV, which was confirmed by the Administrative Court of Cologne in a ruling of 9 June 2020 – 6 K 14278/1 – https://www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/29_200617/index.php.

82 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2020.223.01.0003.01.ENG&toc=OJ:C:2020:223:TOC.

83 Even the insertion of comments or the editing of the video may be sufficient.

84 https://www.medienanstalt-nrw.de/themen/rundfunklizenzen.html.

The first decision[85] concerned the SkypeOut internet telephone service, which made it possible to call telephone numbers connected to the 'normal' telephone network via the internet from inside the Skype application (VoIP). The Court ruled that a 'service which allows the user to call a fixed or mobile number covered by a national numbering plan from a terminal via the public switched telephone network (PSTN) of a Member State constitutes an "electronic communications service"'. Therefore, SkypeOut is subject to regulations by the BNetzA under the TKG.

The second decision[86] concerned the email service provider Gmail by Google. Both the BNetzA and the administrative court considered Gmail to be a telecommunications service although the service was free of charge and the services took place in the 'open internet'. The administrative court argued, that the individual procedural steps (transmission via the open internet, storage on Gmail servers) could not be evaluated separately from each other. The CJEU, however, ruled that the decisive criterion was not the functional usage of (third-party) infrastructure but responsibility for the data transmission. While SkypeOut must (necessarily) guarantee the connection between the internet and the public telephone network through a gateway, Gmail only provides a service that depends on data transmission on a foreign network (the internet) without (technically) guaranteeing this transmission. Therefore Gmail may not be considered a telecommunications service.

VII CONCLUSIONS AND OUTLOOK

The ICT sector in Germany is highly important and fast growing, entailing a fast-paced legal and policy environment. Convergence presents an abundance of challenges for policymakers, industry and society. Cooperation on a European and global level is vital for most German ICT policy issues, including telecommunication and frequency policies, ICT research, anti-spam measures as well as consumer, copyright and youth protection in the context of new media.

85 CJEU ruling of 5 June 2019 – C-142/18 – ECLI:EU:C:2019:460.

86 CJEU ruling of 13 June 2019 – C-193/18 – ECLI:EU:C:2019:498.

Appendix 1

ABOUT THE AUTHORS

JOACHIM GRITTMANN

Latham & Watkins LLP

Joachim Grittmann is counsel in the Frankfurt office of Latham & Watkins LLP and practises in the firm's litigation and trial department. His practice involves all aspects of public law matters for a variety of public and non-public clients. He has broad experience in administrative and regulatory law, including telecommunications and media laws as well as data protection laws. A special focus of his activities is the interface of administrative and data protection law, especially with regard to the activities of data protection supervisory authorities. Joachim is also co-author of one of the leading commentaries on the GDPR and the BDSG (Taeger/Gabel).

Joachim has been an attorney since 2001 and since 2013 has been counsel at Latham & Watkins LLP in Frankfurt. Joachim Grittmann is also a Master of Public Administration and an Associate Professor for public law at the University of Heidelberg (including lawyer-oriented legal education).

LATHAM & WATKINS LLP

Reuterweg 20
60323 Frankfurt
Germany
Tel: +49 69 6062 6000
Fax: +49 69 6062 6700
joachim.grittmann@lw.com
www.lw.com

Chapter 10

JAPAN

Stuart Beraha, Hiroki Kobayashi, Takaki Sato and Benjamin Han[1]

I OVERVIEW

The media and telecommunications environment in Japan has continued its rapid development throughout 2019 and 2020. While the country has already achieved a broadband penetration rate of 100 per cent, numerous measures have been (and continue to be) implemented to enhance the nation's telecommunications networks.

i Japan's covid-19 response

As in many other countries, the covid-19 pandemic has significantly impacted several aspects of Japanese society, including work life and business operations. Despite the near-100 per cent broadband penetration and near-universal 3G/LTE, and increasingly 5G, coverage throughout Japan, Japanese businesses have lagged behind the government's pandemic-related goal of having 70 per cent or more of each company's employees work from home. That said, many companies have taken this opportunity to re-evaluate their notions of a 'traditional office', which typically has been characterised by long hours at the office and packed commutes, and the necessity of office space, particularly in metropolitan areas like Tokyo where office space is in short supply.

ii Society 5.0

Additionally, the Japanese government has begun pursuing its 'Society 5.0' initiative: the digitisation of the entire society by integrating digital innovations (like artificial intelligence (AI) and big data analysis) into the physical (real) world. In furtherance of this initiative, the Japanese government has pursued a number of programmes and measures in the telecommunications space.

For example, the government is now strongly pushing the rollout of 5G and other cutting-edge technology that is capable of transferring data at even higher rates than is currently possible with LTE. 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 launched 5G telecommunication services in 2020.

In addition, to combat the spread of covid-19, the Japanese government released the Contact-Confirming Application (COCOA), a social tracing app developed by Microsoft that allegedly does not store personally identifiable information but allows a user to report

1 Stuart Beraha and Hiroki Kobayashi are corporate partners, and Takaki Sato and Benjamin Han are corporate associates at Latham & Watkins Gaikokuho Joint Enterprise.

if he or she has tested positive for covid-19 and notifies any phone with the app installed if it has been in the vicinity of such user's phone. The app reached 4.4 million users in its first week, but registrations have reportedly slowed substantially since its debut.

Society 5.0 will inevitably result in a significant increase in personal data communication, both domestic and cross-border. The security of such data is a key concern with respect to such communication, which the government has addressed through various regulations. That said, the government seeks to strike a balance between the protection of personal data and the potential economic benefits of big data analysis. One approach that the government has been exploring is the creation of a personal-data-store-type regime known as personal information banks, which would entail personal data being collected by a trusted entity (i.e., the 'personal information bank') and such entity providing service providers with access to such data in accordance with the data subject's instructions.

iii Recent digitisation efforts

The Japanese government is also pursuing a number of efforts aimed at digitising government services and making them more easily accessible to residents. For example, the MIC has pursued 'Open Data' initiatives with respect to governmental data, encouraging all governmental agencies (including municipal ones) to allow citizens to easily access and use governmental data in digital format for free. However, as of the end of 2019, 63 per cent of municipal governments have taken no measures to address the Open Data initiative.

Additionally, to allow Japanese residents to access more government services online or more conveniently, the Japanese government has rolled out personal identification cards known as 'My Number' cards. Among other services, My Number card holders are able to make certain tax filings online (electronically authenticated with My Number card data) and receive family, tax, residency and other records at convenience stores (which are ubiquitous in most Japanese cities) rather than at their local city hall or ward office. That said, despite being introduced in 2015, the adoption of My Number cards has been sluggish – reportedly only 17 per cent of Japanese residents have My Number cards as of July 2020 and the government's incentive programme that rewards ¥5,000 of cashless payment credit (e.g., PayPay credit) to registrants has attracted less than 10 per cent of expected applicants as of September 2020.

Even where residents have received My Number cards, there have been hiccups in the implementation of programmes attempting to leverage the system. Notably, the Japanese government offered an online application option for the Japanese government's ¥100,000 special covid-19 stimulus payment to residents with My Number cards. However, local municipal offices were flooded by requests to reset My Number card passcodes (required to log into the government's application page) from residents who forgot them and many residents reported having trouble accessing the application page even with correct passcodes – in some cases, it was simply quicker for residents to post a physical application. Additionally, even when residents were able to submit an application online, all applications were reportedly reviewed by government officials by hand, meaning an online application was not necessarily processed any more quickly than a physical application.

The government is nevertheless expected to continue pursuing data and digitisation initiatives. Yoshihide Suga, prime minister of Japan, voiced a commitment to further digitise government services and 'allow people to receive government services 24 hours a day, 7 days a week so long as they have a My Number card.' In furtherance of this goal, Prime Minister

Suga has instructed the Digital Transformation Minister, Takuya Hirai, to establish a new governmental agency named the Digital Agency. The bill establishing the Digital Agency will be submitted to the legislature in January 2021.

Under the current bureaucratic system, the responsibility for digitisation measures is scattered among several governmental agencies, based on whether such measures relate to the sectors within such agency's purview. Some have said that such decentralised responsibilities partially account for the slow progress of Japan's digitisation efforts, particularly when compared to other countries. For example, agencies have implemented different IT systems and data formats, rather than coordinate standardised systems and formats. This disparity reportedly made it more difficult for governmental agencies to share covid-19 data.

While the final details regarding the Digital Agency will depend on the bill that is ultimately passed by Japan's legislature, the Digital Agency will seek to consolidate responsibility and authority for digitisation efforts into one centralised agency. The aim is to facilitate more efficient implementation of digitisation efforts and help agencies share data and coordinate more smoothly by standardising IT systems and formats.

Other initiatives that the Digital Agency is planning to pursue include consolidation of various identification cards into the My Number card (e.g., public health insurance cards). This will enable citizens to reduce the number of identification cards that they must carry to receive services. Additionally, Digital Transformation Minister Hirai announced that he seeks to have the Digital Agency serve as a 'control tower' to expedite digitisation in the private sector as well as the public sector. Few public details about this initiative are available at the time of writing.

iv Expansion of telecommunications market access and competition

The government is also increasingly prioritising the expansion of market access and competition within the Japanese telecommunications industry. For example, the government is looking to equalise competition between Japanese service providers and non-Japanese service providers. In 2020, telecommunication regulations were amended to ensure the government may enforce such regulations equally between domestic and foreign service providers.

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. In addition, digital platform businesses have recently drawn additional scrutiny from government regulators who are concerned with the fairness of transactions. In 2020, a new law was enacted to ensure fairness of digital platform businesses, mainly via disclosure requirements.

v Digital piracy prevention initiatives

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's approach did not result in legislation. Instead, the Agency for Cultural Affairs (ACA) addressed this issue by amending the Copyright Act.

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:

a the Wire Telecommunications Act, which governs facilities for wired signal transmission, such as wired telephony, wired broadband networks and cable television;

b the Radio Act, which governs facilities for wireless signal transmission, such as mobile phones, terrestrial and satellite television broadcast infrastructures and high-powered WiFi networks;

c the Telecommunications Business Act, which regulates telecommunications and media businesses; and

d 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 the 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 restrictions, 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 the typical review process for licence renewals or new applications.

Further, the Telecommunications Business Act was amended in May 2015 to require the major telecommunications companies[2] 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,[3] KDDI and SoftBank – until Rakuten Mobile entered the market in October 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

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 Corporation is 33.93 per cent owned by the Japanese Ministry of Finance as of 30 June 2020. NTT DOCOMO is a publicly traded subsidiary of NTT Corporation, but on 29 September 2020, NTT Corporation announced that it plans to take NTT DOCOMO private by making a tender offer for, and purchasing, all of NTT DOCOMO's publicly traded shares (around 34 per cent of NTT DOCOMO's outstanding common shares) for around ¥4.25 trillion. NTT Corporation expects that the buyout will be completed by the end of the fiscal year ending 31 March 2021.

filing and waiting periods unless the acquiring investor satisfies criteria for exemption from such prior filing requirement.[4] When there are no national security concerns present, this is ordinarily a pro forma requirement.

III TELECOMMUNICATIONS & 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[5] 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. Notwithstanding such funding assistance, NTT East and NTT West have operated at a deficit in their landline businesses due to the burden of owning and maintaining all of the facilities necessary to provide services to the entirety of Japan, even to rapidly depopulating areas. To reduce this burden, the NTT Act was amended in May 2020 to permit NTT East and NTT West to use wireless telecommunication facilities owned by other telecommunications companies to fulfil their duties of providing universal service.

4 Regulated transactions include an acquisition of 1 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 33.93 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.

Currently, there is no similar law requiring universal broadband service, but the MIC's Information and Communications Council announced in December 2019 that it is considering extending universal service requirements to include broadband service. Notwithstanding the lack of a formal requirement for universal coverage, as of 2015, the broadband infrastructure (3.5G, satellite internet, 3.9G, DSL, optics fibre/FTTH, etc.) penetration rate in Japan has already reached 100 per cent, and super-broadband infrastructure (optical fibre/FTTH, 3.9G and other infrastructure with data transmission speed over 30Mb per second, including DSL, FWA, satellite, BWA, etc.) penetration rate has similarly reached 99.98 per cent. That said, rolling out optical fibre will be especially important to enable the proliferation of 5G. Optical fibre's nationwide penetration rate is 98.8 per cent as of March 2019 but it is below 95 per cent in a few prefectures. The MIC is planning to complete installing optical fibre in all cities, towns and villages that desire it by March 2022.

Rakuten Mobile: a new mobile network operator service provider

Rakuten KK, a major e-commerce platform operator, has long had the largest market share of all mobile virtual network operators (MVNOs) in Japan. Its recently established subsidiary, Rakuten Mobile, was approved to become Japan's fourth mobile network operator (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 planned to launch MNO services by October 2019, but the launch was delayed because of delays in installing base stations. In the interim, Rakuten Mobile offered free service to around 5,000 customers in limited areas like Tokyo and Osaka while its full network service was being rolled out. Rakuten Mobile launched MNO services in April 2020, and seeks to attract customers by offering a competitively priced unlimited data plan – Rakuten reported that it has received over 1 million applications for the service as of 30 June 2020. However, data usage is capped at 5GB when roaming in areas where Rakuten has not yet built out its own network and relies instead on KDDI's network (i.e., areas outside certain major metropolitan areas like Tokyo, Nagoya and Osaka). Furthermore, Rakuten has only launched its 5G network in around 20 locales, which is limited compared to the other MNO providers.

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[6] since June 2014. The goals of the SAQ2 JAPAN Project include:

a increasing the number of free Wi-Fi hotspots and improving the accessibility of these hotspots to the public;

b facilitating the availability and installation of Japanese SIM cards for foreign mobile phone users in Japan;

6 SAQ is an acronym for selectable, accessible and quality.

c reducing international roaming fees applicable to foreign mobile phone users in Japan; and

d 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 190,000 public Wi-Fi access points across Japan,[7] 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.[8] This NTT group affiliate also continues to install additional Wi-Fi access points.

In preparation for hosting the Olympic Games in Tokyo that were originally scheduled to take place in 2020, 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 app[9] 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

7 As of March 2020.

8 This application was prepared primarily for foreign visitors' use, but Japanese residents are also able to use the application.

9 Omotenashi means hospitality.

10 Normally, users can only use the Wi-Fi network of the service provider to which they are currently subscribed.

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, and severe typhoons during the fall of 2019. 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 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 originally scheduled to take place 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. The MIC further loosened the restrictions to allow Japanese residents to use foreign mobile phones for R&D purposes via an amendment to the Radio Act. Under the amended Radio Act, which came into force in force in November 2019, Japanese residents are permitted to use foreign mobile phones for R&D purposes for up to 180 days, though the user is required to file a prior notification with the MIC and this exception only allows users to connect devices that have received certain foreign certifications to Wi-Fi or Bluetooth.

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.

iii 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 and launched commercial MNO services in April 2020. 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 the government has 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 2018, approximately 751 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 2020 the number of active MVNOs has increased to 1,128. Correspondingly, there were 24.65 million MVNO subscribers by March 2020, up from 7.17 million in December 2013. However, despite this recent increase in MVNO activity, MVNO service subscribers still only constituted 13.2 per cent of all mobile service subscribers as of March 2020.

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

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.

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 regulations implementing 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.

The MIC also seeks to address another competition issue – the cost of complying with the Telecommunication Business Act may differ between Japanese enterprises and foreign ones. The cost difference is primarily owing to the difficulty of extraterritorial enforcement of the act, resulting in uneven enforcement between domestic and foreign enterprises. Under the current Telecommunication Business Act, a foreign company is not subject to extraterritorial enforcement unless the company has an establishment or a facility in Japan, even if it provides services to Japanese consumers. To address this gap, the MIC amended the Telecommunication Business Act in May 2020 to extend its extraterritorial enforcement to foreign enterprises that provide services to Japanese customers that are equivalent to those provided by domestic enterprises that are regulated by the Telecommunications Business Act. These amendments are expected to be in full force by May 2021. The amended Telecommunication Business Act requires such foreign telecommunication companies to register with the MIC and to designate a local representative in Japan to ensure that the MIC can realistically enforce sanctions. This Amendment also aims to enhance the protection of Japanese consumer's privacy rights. As a consequence of extraterritorial application, even foreign telecommunication companies must comply with the obligation to protect the consumer's right to 'secrecy of communication', which is protected even more stringently than personal data under Privacy Act. However, foreign telecommunication companies may face difficulty in complying with these 'secrecy of communication' requirements because the regulations do not always clearly identify what categories of data fall within those requirements in the context of digital communication (which may include header-data, IP addresses, location data, etc.), despite the MIC's issuing guidelines that provide some (incomplete) clarity as to this issue. Foreign telecommunication companies should monitor how discussions develop with respect to understanding these requirements and the MIC will hopefully issue further guidelines as recommended by Information and Communications Council.

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.

As a result of a study conducted by the Working Group on Consumer Protection Rules based on the MIC's collection and analysis of consumers' complaints trends the MIC has recognised that there are widespread consumer complaints about solicitations made by telecommunication business providers that intentionally mislead consumers as to the identity of such provider or omit the purpose of communication (e.g., to solicit customers to enter into subscription contracts they may not desire). Some consumers were induced to enter into agreements with small-sized enterprises that misleadingly portrayed themselves as larger, more well-known enterprises, while others switched service providers under the mistaken belief that they were just switching to a different subscription plan provided by their existing service provider. To address these issues, the MIC amended the Telecommunication Act to require telecommunication service providers and distributers to clearly state their identity and the purpose of a communication prior to each communication for solicitation. The amendment came into full force and effect in October 2019.

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.

Further amendments to the Privacy Act were passed in June 2020. The amendments pertain to various matters, including the enhancement of data subject rights, narrowing the scope of permissible opt-out transfer of personal data, creating a new category of 'pseudonymised data' with less cumbersome requirements, heightening filing duties upon data breach, strengthening extraterritorial enforcement, etc. Regulations implementing the new amendments and guidelines are expected to clarify how to manage day-to-day data operation in compliance with the amendment by around June 2022, at which time the amendment is likely to come into full force and effect.

The Japan Fair Trade Committee (JFTC) has also approached personal data protection from the perspective of competition law. In December 2019, the JFTC issued guidelines on abuse of market dominance in the context of digital platforms collecting personal data from platform users. This suggests that in the JFTC's view, abuse of market dominance could occur in the business-to-consumer context, rather than solely in the business-to-business context. Whether a digital platform provider has 'market dominance' is a fact-intensive inquiry. The JFTC guidelines list types of behaviour constituting 'abuse,' which mainly consist of violations of the Privacy Act. However, it should be noted that the guidelines are non-exhaustive – other behaviour may constitute 'abuse' even if it does not violate the Privacy Act. Also, certain 'abusive' behaviour covers collection of information which is related to a person but not identifiable. Such unidentifiable information is not protected by the Privacy Act, but the JFTC may still seek to protect it.

At the same time, in the furtherance of the Society 5.0 initiative, which will be facilitated by easier data circulation, the government has sought to establish systems by which data subjects can provide personal data in exchange for services, while being protected against illegitimate use of such data. As a result, the personal information bank (PIB) regime has been adopted. Under this regime, a PIB enters into a contract with a data subject under which the PIB is authorised to manage the data subject's personal data, and when necessary, to collect personal data which the data subject already provides to other companies (such as e-commerce platform, SNS, etc.). When a company desires to use the personal data managed by the PIB, the PIB is authorised to determine whether to give the consent to such usage on behalf of the data subject following the general policy specified by the data subject. The data subject also has the right to opt-out of usage. There are no constraints on the kinds of benefits that may be offered to data subjects in exchange for access to their personal data. Accordingly, the PIB may offer benefits to incentivise the data subjects to participate in its service.

A PIB is not legally required to obtain any governmental licence to operate its data business, but a PIB may obtain certification from the Information Technology Federation of Japan (ITFJ) if desired, primarily to demonstrate the PIB is reputable. The MIC and METI issued the latest guidelines setting forth the criteria that an applicant must satisfy to obtain such certification in October 2019. As of April 2020, five PIBs have obtained the ITFJ certification and one PIB has launched data services.

Protection of digital platform users

As illustrated by the JFTC's approach to digital platform operators' collection and processing of personal data, Japanese regulators have taken great interest in protecting users (both of marketplace participants and customers). For this purpose, the Ministry of Economy, Trade and Industry (METI), JFTC and MIC pushed for the Act For Transparency of Digital Platformer Transaction (the Platformer Act). The Platformer Act was enacted in June 2020, and is expected to be in full force around June 2021.

METI is expected to specify the digital platform businesses that will be subject to the Platformer Act (specified platformer). The list of specified platformers has not been released, but foreign digital platform businesses operating in Japan are likely to be treated similarly to Japanese digital platform businesses because officers of METI explicitly announced that Platformer Act will apply to both foreign and domestic digital platform businesses. Specified platformers will be subject to three types of obligations: (1) disclosure requirements; (2) requirements to establish procedures and structures to effectively communicate with marketplace participants and to handle inquires and complaints from marketplace participants; and (3) requirements

to submit annual reports to METI on the compliance status and self-assessment thereof with respect to compliance with the requirements of (1) and (2). In order to comply with the disclosure requirements, a specified platformer may need to disclose items that are not included in typical terms of use, including the criteria used to determine the ranking of products, and the criteria for banning participation in a marketplace.

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.

Although the IPSHQ did not reach a consensus, the ACA approached this issue from the perspective of the Copyright Act and successfully pushed for an amendment thereto, whereby an operator of piracy sites is subject to a criminal penalty of imprisonment up to five years or fines of up to ¥5 million or both, and a person posting a hyperlink to infringing content on a piracy site is subject to imprisonment up to three years or fines of up to ¥3 million. In addition to the ban on piracy sites, the ACA addressed illegal downloads of infringing content. Before the amendment, the statutory ban on illegal downloads pertained only to a limited category of infringing contents: music and movies. The amended Copyright

Act will ban downloads of all the categories of infringing contents, including books, theses and computer programs. The ban on piracy sites will come into full force and effect on 1 October 2020. The extension of infringing content categories come into full force and effect on 1 January 2021.

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.

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 266 million as of March 2020 (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, and 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, Y!Mobile, 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/per 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 bandwith. In this round, Rakuten Mobile, a major online shopping platform operator 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 within two years. For the purpose of expediting 5G spreading, the MIC also started granting subsidies to corporations for of the installation of optical fibre. These four major providers have launched 5G telecommunication services in 2020, but the coverage differs from carrier to carrier – as noted above, Rakuten's 5G network currently only covers around 20 locales. The MIC seeks to make the spectrum currently used for 4G also available for 5G, and is making efforts to

establish a framework to do so. Also, separate from its goal of nationwide 5G coverage, the MIC has started to grant 'Local 5G' spectrum authorisations. The first round of Local 5G authorisation was granted to 13 organisations (including Fujitsu, Tokyo University, etc.). Local 5G is intended to be used only within a narrow and limited area such as the grantee's specific building or land.

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.

The government is now focusing on 5G, which will enable data transmission speeds of up to 10Gb per second. As described above, 5G spectrum was allocated to NTT DOCOMO, KDDI, Softbank, and Rakuten Mobile in 2019. These four providers have launched the 5G telecommunication service in 2020 with varying scopes of coverage as of the time of this writing.

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.

iv 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 the then 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 February 2019 indicated that there were 17.5 million fee-based video delivery service users in 2018, and the number was expected to increase to 23.6 million by 2021.

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 V.i 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

Throughout 2019 and 2020, 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.

In particular, the MIC is heavily stressing the importance of 5G technology in connection with its Society 5.0 initiative. This focus is illustrated by the prominence of 5G-related topics in the MIC's latest annual White Paper in 2020. Society 5.0 will be a digital data-driven society, and the MIC is fully aware of the need to strongly facilitate the utilisation of data in Japan. According to the MIC's international comparative survey, Japanese companies have been the least proactive in using digital data for business purposes, while Japanese data subjects have been the most reluctant to provide personal data (in each case, of the surveyed countries). The Personal Information Bank regime may be a potential way to tackle these problems.

VII CONCLUSIONS AND OUTLOOK

The Japanese government is pursuing a number strategies to digitise government services, such as making government data available online, rolling out the My Number card system to make certain services accessible online or more conveniently and creating the Digital Agency to consolidate digitisation efforts. The effectiveness of such efforts has varied, but the efforts are expected to continue given the government's announced commitment to digitise Japanese governmental services.

The government has also taken steps to expand market access and competition in the Japanese telecommunications industry by making it easier to enforce regulations equally between Japanese service providers and non-Japanese service providers, and adding regulations to eliminate or regulate anticompetitive business practices like SIM card locking and automatic customer contract renewals.

Lastly, further steps have been taken to address media piracy in Japan, including amendments to the Copyright Act that subject operators of piracy sites to criminal penalties and expand the categories protected by the Copyright Act.

In sum, 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.

Appendix 1

ABOUT THE AUTHORS

STUART BERAHA

Latham & Watkins Gaikokuho Joint Enterprise

Stuart Beraha is a partner in the corporate separtment of Latham & Watkins' Tokyo office and leads the firm's data and technology transactions practice in Asia. Mr Beraha has been based in Tokyo for over 20 years, and has broad experience in technology, content, branding and other intellectual property development, licensing and partnering transactions. His work in the telecommunications industry has included patent and technology licensing matters for mobile device and infrastructure manufacturers, licensing and commercial arrangements for digital platform business operators, various aspects of submarine cable landing and related arrangements, and a wide range of other commercial and IP-related transactional matters. Mr Beraha is admitted to the New York bar and registered in Japan as a Gaikokuho-Jimu-Bengoshi (registered foreign lawyer, New York Law).

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.

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.

BENJAMIN HAN

Latham & Watkins Gaikokuho Joint Enterprise

Benjamin Han is an associate in the corporate department of Latham & Watkins' Tokyo office and a member of the data and technology transactions practice. Mr Han assists in the representation of leading Japanese and multinational companies on a variety of intellectual property and commercial matters, including intellectual property licensing, sale, and other transactions, joint development, joint venture, strategic alliance and outsourcing arrangements, and product manufacturing, supply and distribution arrangements. Mr Han has assisted in the representation of clients in a variety of industries, including companies in the semiconductor, pharmaceutical and telecommunications sectors. Mr Han is admitted to practise in California.

LATHAM & WATKINS LLP

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
stuart.beraha@lw.com
hiroki.kobayashi@lw.com
takaki.sato@lw.com
benjamin.han@lw.com
www.lw.com

Chapter 16

SAUDI ARABIA

Brian Meenagh, Alexander Hendry, Avinash Balendran, Homam Khoshaim and Lojain Al-Mouallimi[1]

I OVERVIEW

Technology, media and telecommunications are key pillars underpinning the objectives and themes of Saudi Arabia's Vision 2030 programme.[2] This is seen through significant investment in technology-enabled megaprojects such as NEOM,[3] Qiddiya[4] and the Red Sea Project[5] and the creation of new government agencies within the last 12 months, including the Saudi Data and Artificial Intelligence Authority and its sub-entities, the National Data Management Office, the National Information Center and the National Center for AI, that are dedicated to the furtherance of a technology-enabled society. As noted in the sections below, Saudi government policy is firmly in support of investment in and deployment of technology and telecommunications products and services.

Key trends we are seeing in Saudi Arabia include:

a Encouragement of foreign direct investment (FDI) into Saudi Arabia – particularly in the technology sector with dedicated resources within government agencies focusing on FDI into the technology sector.[6]

b The rollout of 5G – 5G spectrum has been available to retail customers since mid-2019 with the Saudi Ministry of Communications and Information reporting in February 2020 that Saudi Arabia had 6,500 5G towers in operation and noting that Saudi Arabia had received a Government Leadership Award from the Mobile World Congress for its efforts in developing national digital infrastructure.[7]

c Growth of e-commerce – in late 2019, the United Nations Conference on Trade and Development E-Commerce Index (UNCTRAD B2C E-Commerce Index) identified Saudi Arabia as being one of the top 10 developing countries in the e-commerce sector[8] and the Ministry of Commerce published specific regulations applicable to e-commerce service providers in Saudi Arabia[9] and the issue of these regulations coincide with a significant growth in electronic and mobile commerce activity.

---

1 Brian Meenagh is a partner, and Alexander Hendry and Avinash Balendran are associates at Latham & Watkins LLP. Homam Khoshaim and Lojain Al-Mouallimi are associates at the Law Office of Salman M Al-Sudairi.

2 https://vision2030.gov.sa/en.

3 https://www.neom.com/en-us/.

4 https://qiddiya.com/.

5 https://www.theredsea.sa/en.

6 https://investsaudi.sa/en/sectors-opportunities/information-technology/.

7 https://www.mcit.gov.sa/en/media-center/news/232692.

8 https://unctad.org/system/files/official-document/tn_unctad_ict4d14_en.pdf.

9 https://www.lw.com/thoughtLeadership/COVID-19-and-Online-Transactions-in-Saudi-Arabia.

Migration to cloud-based services – like most technologically mature economies, enterprises in Saudi Arabia are seeking to utilise cloud-based services. In parallel, the Communications and Information Technology Commission and the National Cybersecurity Authority have issued regulations and guidance applicable to the use of cloud computing services in Saudi Arabia.

II REGULATION

i The regulators

The technology and telecommunications sector in Saudi Arabia is principally regulated by two bodies: the Ministry of Communications and Information Technology (MCIT)[10] (formerly, the Ministry of Post, Telegraph and Telephone) and the Communications and Information Technology Commission (CITC).

A small number of other authorities have more discrete remits. Recently, Saudi Arabia has expanded regulation into the field of cybersecurity, which has led to the creation of the National Cybersecurity Authority (NCA)[11] and the National Cyber Security Center (NCSC), both overseen by the Ministry of Interior (MOI).[12]

The key regulators for media and media protection in Saudi Arabia are the Ministry of Media (MoM)[13] and General Commission for Audiovisual Media (GCAM).[14]

Further details on each regulator are set out below.

Technology and telecommunications

Key regulators

The MCIT is responsible for making general policies and development programmes and representing Saudi Arabia in domestic, regional and international bodies in the technology and telecommunications sector.

The CITC is responsible for issuing licences in accordance with the Telecom Act and implementing approved plans and programmes for the supervision and management of the technology and telecommunications sector. Decisions made by the CITC can be appealed to MCIT.

Other relevant regulators

a The Saudi Authority for Data and AI (SDAIA): the SDAIA and its sub-entities the National Data Management Office (NDMO), the National Information Center (NIC), and the National Center for AI (NCAI) work on providing a data-driven and AI-supported government and economy, and to own the national data and AI agenda to help achieve Vision 2030's goals.[15]

b The National Centre for Digital Certification (NCDC): established in 2001 and transferred to the remit of the MCIT for management in 2005, the NCDC is primarily

10 https://www.mcit.gov.sa/en.

11 https://nca.gov.sa/en/index.html.

12 https://www.moi.gov.sa/.

13 https://www.media.gov.sa/en.

14 https://www.gcam.gov.sa/en.

15 https://sdaia.gov.sa/.

responsible for the management of public key infrastructure (i.e., a set of roles, policies, and procedures needed to create, manage, and distribute digital certificates and manage public-key encryption).[16]

c The National Digital Transformation Unit (NDTU): established in 2017, the NDTU aims to develop and further the digitisation of citizen services in partnership with the private sector. A notable example of this in 2017 was the setting up of FekraTech, an interactive platform that enables citizens to participate in Saudi Arabia's national digital transformation by submitting digital solutions to existing challenges; the NDTU worked alongside the Ministry of Health for the initiative's initial project, whereby individuals proposed solutions to a number of health-related issues.[17]

d The Saudi Authority for Intellectual Property (SAIP): established in 2018 with the aim of organising, supporting, sponsoring, protecting and promoting intellectual property in Saudi Arabia in accordance with global best practices.[18]

Cybersecuity regulators

The MOI oversees numerous bodies that work to maintain Saudi Arabia's security and manage its internal affairs. Its objectives and responsibilities include:

a achieving security and stability, providing safety for Saudi Arabia citizens and protection against crime;

b reinforcing security relationships with neighbouring Arab and GCC countries, to maintain safety in Saudi Arabia and abroad, to control crime and drug smuggling, and exchange security information; and

c reinforcing security cooperation with neighbouring countries to protect cultural possessions and achievements, supporting internal and external security, controlling crime, terrorism and drug smuggling, and developing Arab security institutions.

In addition to the above responsibilities, all cybercrimes must be reported to the MOI.[19] Prosecutions are led by the Bureau of Investigation and Prosecution.

The NCA was established by royal decree in October 2017 as the body responsible for the protection and promotion of cybersecurity matters in Saudi Arabia. In October 2017, it issued a set of minimum standards to be applied by various national agencies to reduce the risk of cyber threats; these controls considered governance, strengthening cybersecurity, enhancing external cybersecurity, in addition to cloud computing, and industrial control systems and ultimately became consolidated in the NCA's Essential Cybersecurity Controls (ECC – 1 : 2018)[20] and Cloud Cybersecurity Controls (CCC – 1: 2020).[21]

The NCA has both regulatory and operational functions related to cybersecurity and it works closely with public and private entities to improve the cybersecurity posture of the country in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities in alignment with Vision 2030.

16 https://www.ncdc.gov.sa/?lang=en.

17 https://ndu.gov.sa/en/.

18 https://www.saip.gov.sa/en/.

19 Please see here for further information https://www.saudi.gov.sa/wps/portal/snp/individuals/servicedetails/6166.

20 https://nca.gov.sa/en/pages/ecc.html.

21 https://nca.gov.sa/files/ccc-en.pdf.

The NCA also oversees the NCSC and Saudi CERT. The NCSC has a national role in monitoring, analysing cyber risks and threats, and sharing information with government entities and critical national infrastructures. While Saudi CERT's primary mission is to raise cybersecurity awareness in Saudi Arabia.

Media

The MoM is the governmental body tasked with the regulation of Saudi Arabia's media, and Saudi Arabia's communications with other countries.

GCAM is responsible for the regulation of audiovisual media transmission in Saudi Arabia. It reports to the MoM, but is a separate legal entity, with independent finance and administration.

ii Main sources of law

Technology and telecommunications

The key relevant laws in the technology and telecommunications sector are as follows:

a The Telecom Act (issued under the Council of Ministers resolution No. (74), dated 05/03/1422H (corresponding to 27 May 2001), and approved pursuant to the Royal Decree No. (M/12), dated 12/03/1422H (corresponding to 3 June 2001).[22]

b The Communication and Information Technology Commission Ordinance (the CITC Ordinance) (issued under the Council of Ministers resolution No. (74), dated 05/03/1422H (corresponding to 27/05/2001), and amended pursuant to the Council of Ministers resolution No. (133), dated 21/05/1424H (corresponding to 21 July 2003).[23]

c The E-Commerce Law 2019 (Royal Decree No. M/126 dated 07/11/1440H (corresponding to 10 July 2019)).[24]

The CITC's role has expanded beyond telecommunications and it has issued a variety of regulations and consultations[25] in a number of sectors in the technology and digital space, including:

a the Cloud Computing Regulatory Framework (version 2, revised in February 2019) (the Cloud Regulations): the Cloud Regulations outline the rights and obligations of cloud service providers (CSPs) and users of cloud services (i.e., cloud customers); they only apply to CSPs who own cloud infrastructure in Saudi Arabia or have a direct contractual relationship with customers based in Saudi Arabia;[26]

b the Regulation for the Reduction of Spam (the Spam Regulations): the Spam Regulation requires telecommunications service providers to reduce spam messages transmitted across their networks, including by implementing prevention and monitoring mechanisms. Spam messages are defined as certain types of electronic messages sent without any opt-out mechanism;

22 https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA%20_001_E_%20Telecom%20Act%20English.pdf.

23 https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_002_E_CITC%20Ordinance.pdf.

24 An English translation is not yet available.

25 https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/default.aspx.

26 https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf.

c CITC Decision No. 395/1439 dated 3/11/1439H (corresponding to 14 August 2018);[27]
d the Internet of Things Regulatory Framework, issued in September 2019;[28]
e Rules and Conditions for MVNO Services and IoT-VNO Services Provision: these update the conditions and licensing requirements related to the request for a licence to provide mobile virtual network operator services. They set out the conditions and licensing requirements relating to the provision of the services by internet of things virtual network operators;[29]
f the Saudi Domain Name Registration Regulation[30] and related guidelines and rules;[31]
g the regulations, guidelines and rules for the registration of Saudi country-code top-level domains. They are issued by the Saudi Network Information Centre (SaudiNIC),[32] part of the CITC; and
h the Rules and Technical Standards for ICT Infrastructure Deployment in New Developments: these are intended to facilitate the implementation and roll-out of telecom networks.[33]

Additional regulatory documents issued by CITC relating to the technology and telecoms sector can be found on the CITC website.[34]

Cybersecurity

The key relevant cybersecurity laws are as follows:

a Royal Decree No. 5/11/8697 dated 26/8/1370 H (corresponding to 2 June 1951) (the Law Establishing the Ministry of Interior);
b the Anti-Cyber Crime Law (issued under the Council of Ministers Decision No. 79, dated 7/3/1428 H (corresponding to 26 March 2007), and approved by Royal Decree No. M/17, dated 8/3/1428 H (corresponding to 27 March 2007) (the Cyber Law); [35] and
c the Cloud Regulations.

There are also a number of sector-specific cybersecurity rules and requirements, for example, for the finance sector, the SAMA Cyber-Security framework (version 1, May 2017).

Media

The key laws regulating media and media protection are as follows:

a the Publications Law promulgated by Royal Decree No. M/32 dated 03/09/1421H (corresponding to 29 November 2000);

27 https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/ReductionofSPAM/Documents/IT%20008%20E%20-%20Regulation_For_The_Reduction_of_SPAM_Eng.pdf.
28 https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf.
29 https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Licenses/LicensingRegulatoryFrameworks/Documents/PL-SP-021-A-MVNO-EN.pdf.
30 https://www.nic.sa/en/view/regulation.
31 https://nic.sa/en/cat/rules.
32 https://www.nic.sa/en/.
33 https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/ICTInfrastructure.aspx.
34 https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/default.aspx.
35 https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf.

b the Electronic Publications Regulations published on 20/04/1432H (corresponding to 25 March 2011);
c the Press Institutions Law promulgated by Royal Decree No. M/20 dated 08/05/1422H (corresponding to 29 July 2001) (the Press Institutions Law);
d the General Commission for Audiovisual Media Regulations promulgated by Royal Decree number 33/M dated 25/03/1439H (corresponding to 13 December 2017) (the GCAM Regulations);
e the GCAM Implementing Regulations promulgated by Minister of Media resolution No. 16927 dated 04/03/1440H (corresponding to 12 November 2018) (the GCAM Implementing Regulations); and
f the Copyright Law promulgated by Royal Decree No. M/41 dated 02/07/1424H (corresponding to 30 August 2003).

Publications and press institutions

For the implementation of media laws in relation to publications, the Ministry of Media applies:

a the Law of Printing and Publication and its implementing regulations, regulating print and publication activities; and
b the Implementing Regulations For Electronic Publishing, regulating the practice of electronic publishing in Saudi Arabia.

Audiovisuals

For the implementation of media laws in relation to audiovisuals, the GCAM has issued the implementing regulations governing the following matters:

a importing and selling receivers;[36]
b licensing visual and audible media content production companies;[37]
c establishing a representative offices of tv channels;[38]
d importing, distributing, selling and renting visual and audible media content;[39]
e establishing studios;[40]
f audiovisual broadcasting services over telecommunication networks;[41]
g TV and radio competitions;[42]

36 http://ncar.gov.sa/Documents/Details?Id=FcuO0O65mqv6hUJyQTqGoQ%3D%3D. An English translation is not yet available.
37 http://ncar.gov.sa/Documents/Details?Id=1MYbzcTWDtG73jvEANk3PQ%3D%3D. An English translation is not yet available.
38 http://ncar.gov.sa/Documents/Details?Id=hd7cqmBdRYVl%2BtMCCV63%2Bg%3D%3D. An English translation is not yet available.
39 http://ncar.gov.sa/Documents/Details?Id=H72YTNxW3IS3MwUVeYZEeA%3D%3D. An English translation is not yet available.
40 http://ncar.gov.sa/Documents/Details?Id=I9s%2BthH2KdfE7gG%2FG4b8WQ%3D%3D. An English translation is not yet available.
41 http://ncar.gov.sa/Documents/Details?Id=kC0xTcvz6I6QmCgfWZN5uw%3D%3D. An English translation is not yet available.
42 http://ncar.gov.sa/Documents/Details?Id=W5xSXAHO2EIvFCmaJWItzg%3D%3D. An English translation is not yet available.

h SNG services;[43]
i audio social communication services;[44]
j visual broadcasting via closed circuit services;[45]
k on-demand video services issued by the GCAM;[46] and
l videogame participation.[47]

iii Regulated activities

Generally, each relevant regulator maintains its processes for issuing its licences pursuant to its own regulations, rules and policies. However, more regulators are adopting the use of a unified e-licence issuing system named 'Meras'[48]. Meras allows applicants to submit online applications to obtain licences issued by regulators participating in the Meras platform. We expect that any remaining licences requiring in-person attendance will be phased out in favour of online submissions, either through the relevant regulator or through the Meras platform.

Technology

The Telecom Act provides a legal foundation for supervising and managing the telecommunications sector in Saudi Arabia. It also outlines certain objectives for the sector. These include:

a providing advanced and adequate telecommunications services at affordable prices;
b ensuring the provision of access to the public telecommunications networks, equipment and services at affordable prices;
c ensuring the creation of a favourable atmosphere to promote and encourage fair competition in all fields of telecommunications;
d safeguarding the public interest and user interest as well as maintaining the confidentiality and security of telecommunications information; and
e ensuring the transfer and migration of telecommunications technology to keep pace with its development.

Any entity seeking to provide telecommunications services must submit a licence application to the CITC.

The CITC Ordinance establishes the CITC as the regulatory authority for all matters relating to the telecommunications sector in Saudi Arabia. It includes reference to the CITC's responsibilities, board composition and membership, governance, and sources of finance.

The CITC is responsible for a wide variety of roles, including:

43 http://ncar.gov.sa/Documents/Details?Id=RDTW06ZGhCgAIfarI62%2FTw%3D%3D. An English translation is not yet available.
44 http://ncar.gov.sa/Documents/Details?Id=nIWrewmfgu7D5ZyZWrZDQg%3D%3D. An English translation is not yet available.
45 http://ncar.gov.sa/Documents/Details?Id=N8zzTS1L9PIVRyIvZKih7Q%3D%3D. An English translation is not yet available.
46 http://ncar.gov.sa/Documents/Details?Id=0bYan%2FrPJGJntHUNchtwcQ%3D%3D. An English translation is not yet available.
47 http://ncar.gov.sa/Documents/Details?Id=1DpjOttTK1WQLvvDHlDHzg%3D%3D. An English translation is not yet available.
48 https://meras.gov.sa/en/about/.

a issuing the necessary licences in accordance with all relevant laws;
b ensuring the implementation of the conditions specified in such licences;
c implementing approved policies, plans and programmes for developing the telecommunications sector;
d achieving the orderly expansion of the telecommunications infrastructure and telecommunications services provided to the users in an effective and reliable manner; and
e encouraging reliance on market forces for the provision of telecommunication services.

Cybersecurity

CSPs that exercise direct or effective control over data centres or critical cloud infrastructure hosted in Saudi Arabia are required to register with the CITC.

Media

Publications

Pursuant to the Publications Law, it is necessary to obtain a licence from the MoM to:

a to print, publish, distribute publications or engage in any other publication services;
b import, sell or rent movies or video tapes;
c produce, sell or rent computer programs;
d engage in any press services; and
e carry out photography services.

These activities are restricted to Saudi nationals. In addition, the holder of a licence may transfer, lease or share ownership of such licence after obtaining the approval of the MoM. Furthermore, the Electronic Publications Regulations stipulates that it is required to obtain a licence from the MoM in order to carry out electronic publication. Such licence is also restricted to Saudi nationals.

The author, publisher, printer or distributor must obtain the MoM's approval prior to circulating a publication. The MoM will not approve a publication that prejudices Islam, the Saudi regime, the interests of the country or public morals and customs.

Press institutions

The Press Institutions Law stipulates that in order to establish a press institution that carries out the business of publishing magazines and newspapers, an application shall be submitted by the founders of the institution accompanied with the details of the business and the founders to the MoM. The number of founders shall not be less than 30 and all must be Saudi nationals.

The Minister of Media and Information can only grant a licence after the approval of the Council of Ministers. Both the general manager and chief editor of the press institution must be Saudi nationals. The headquarters of the press institution shall be in the city specified by the licence. Some of its publications may be issued in other cities pursuant to approval of the MoM.

Audiovisuals

In order to obtain, renew or cancel a licence from the GCAM, the approval of the Council of Ministers is required based on the recommendation of GCAM.

There are three types of licences that can be obtained from GCAM: media activity licenses, cinema licences and broadcasting and distribution licences.

iv Ownership and market access restrictions

Typically only those activities listed in the Ministry of Investment (MISA) negative list are prohibited for foreign investors. The MISA negative list is narrow and does not touch upon any of the activities listed in this chapter. However, we note that each regulator has broad discretion when it comes to issuing their licences. Separate from the MISA negative list, each regulator may apply foreign ownership restrictions whether based on its own regulatory framework, policies, security concerns, other interests or solely at its discretion.

v Transfers of control and assignments

Any merger or acquisition transaction shall be subject to the antitrust regime of Saudi Arabia, as implemented by the General Authority for Competition.[49] From an operational perspective and depending on the type of licence, the requirements for licences transfers may range from no action required, notification to the relevant regulator, to obtaining regulator consent (including re-application).

III TELECOMMUNICATIONS & INTERNET ACCESS

i Internet and internet protocol regulation

The regulation and classification of internet and IP-based services are handled by the same authorities and pursuant to the same broader set of legislation governing the telecommunications sector in Saudi Arabia.

There are, however, specific regulations targeting internet and IP-based services in place – for example, see the references in the above sections to the E-Commerce Law and Cloud Regulations as well as the various regulations issued by the CITC and referred to above.

i Universal service

Saudi Arabia has encouraged the development of telecom and broadband infrastructure and adopted the same under its Vision 2030. Prior to the strategies adopted under Vision 2030, the CITC issued the Universal Access and Universal Service Policy[50] (the Policy) in July 2007, which aims to enable 100 per cent of the population to obtain, at a minimum, 'public access to a defined ICT service at a defined quality through reasonably available and affordable public or community facilities' and to subscribe to and use a defined ICT service at a defined quality on an individual or household basis.[51]

ii Restrictions on the provision of service

Service providers are regulated broadly under the Telecom Act.

49 https://gac.gov.sa/index_en.asp.

50 https://www.citc.gov.sa/en/RulesandSystems/bylaws/Documents/LA%20007_%20%20E_%20%20The%20Universal%20Access%20and%20Universal%20Service%20Policy.pdf.

51 Article 1 of the Universal Access and Universal Service Policy.

In addition to that, the CITC has issued regulations that speak to the rights, obligations and terms of ICT service providers and users (the Service Providers Regulations)[52] issued in 2017, and the SPAM Regulations (see above), which aim to reduce unsolicited calls and messages. Both sets of regulations apply to all service providers licensed by the CITC and any users thereof.

Under the Service Providers Regulations, the following general principles must be clearly stated in Arabic and English on any service contracts between a provider and user:

a the minimum age of the applicant is 15;

b service providers may refuse to offer monthly cellular subscriptions to users who have proven to have outstanding balances whether with the same service provider or another; and

c service providers may require that applicants applying for monthly cellular subscriptions provide insurance in certain circumstances.

Contracts must include:

a price list including details related to each service offered and information related to any down-payment requirements;

b details related to the service offered and specifications thereof;

c details of the conditions and obligations of the user and consequences of breach of such conditions and obligations as well as details of any discounts or offers;

d details of any restrictions or exceptions related to the service offered and any additional fees which would apply if such restrictions or exceptions were triggered;

e the duration of the contract and renewal mechanism;

f dates of invoices;

g the mechanism adopted for amending or cancelling the service; and

h situations in which the service provider may suspend or cancel the service.

In addition, the Service Providers Regulations state that each service provider must offer its services to any users applying for the services being offered, and each service must be offered in a consistent manner to all users. This includes maintaining the same prices for services offered, quality of service, time during which the services are offered, and any other conditions imposed by the CITC.

Under the Service Providers Regulations, all user information is considered confidential and service providers are obliged to maintain such confidentiality and seek all measures for the purposes of securing user information and prohibiting access, publication, sharing or use thereof. Service providers are also prohibited from disclosing user information unless such disclosure is mandated under another applicable law, is based on the user's consent, or is provided based on a request from the CITC. Furthermore, the same level of data security must be mirrored in the internal policies of service providers and monitored accordingly.

Service providers are also obligated to maintain the confidentiality of user phone calls and any information transmitted to and from the user or information received through one of the service providers' public networks. They must also prohibit access to such information by any employee or affiliate.

52 https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/Termstoprovide/Pages/default.aspx.

iii Privacy and data security

The Basic Law of Governance of 1992 (Royal Order No. A/91 of 1992) (the Basic Law)[53] specifies a number of rights that promote self-expression.

For example, Article 40 of the Basic Law specifies that privacy of telegraphic and postal communications, and telephone and other means of communication, shall not be violated.

Furthermore, it specifies that there shall be no confiscation, delay, surveillance or eavesdropping, except in cases provided by the law.

Article 8 of the Publications Law also guarantees freedom of expression in different forms of publication.[54]

Although the Basic Law and the Publications Law grant rights promoting self-expression, they are subject to other limits and qualifications laid down by applicable law that aim to protect national interests. Examples of those limits include (without limitation):

a Article 62 of the Basic Law, which states that if there is an imminent danger threatening the safety of Saudi Arabia, the integrity of its territories or the security and interests of its people, or is impeding the functions of official organisations, the King may take urgent measures to deal with such a danger.

b Article 6 of the Cyber Law, which criminalises the production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through the information network or computers. The penalty for committing any of the foregoing crimes is imprisonment for a term not exceeding five years; and a fine not exceeding 3 million riyals.

c An Antiterrorism Law introduced in November 2017, which maintains broad definitions of what can be considered a terrorist act. The foregoing law does not restrict the definition of terrorism to violent acts. Other conduct it defines as terrorism includes 'disturbing public order', 'destabilizing national security or state stability', 'endangering national unity' and 'suspending the basic laws of governance', all of which may encompass any form of expression.[55]

Saudi Arabia does not have a comprehensive general data protection law. Shariah principles (i.e., Islamic principles derived from the Holy Quran and the Sunnah) are the primary source of data protection law in Saudi Arabia – these principles generally protect the privacy and personal data of individuals.

The general right to privacy is also reflected in Article 40 of the Basic Law, which mentions privacy as a right that is related to the dignity of an individual and guarantees the privacy of telegraphic, postal and other types of communication. It also prohibits surveillance and eavesdropping unless permitted by law.

In addition, there is:

53 https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/16b97fcb-4833-4f66-8531-a9a700f161b6/1.

54 https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/ecaaec43-8ff9-46b8-b269-a9a700f16e66/2.

55 'Terrorist crime' means any act committed, individually or collectively, directly or indirectly, by a perpetrator, with the intention to disturb public order, destabilise national security or state stability, endanger national unity, suspend the Basic Law or some of its articles, undermine state reputation or status, cause damage to state facilities or natural resources, attempt to coerce any of its authorities into a particular action or inaction or threaten to carry out acts that would lead to the aforementioned objectives or instigate such acts; or any act intended to cause death or serious bodily injury to a civilian, or any other person, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act.

a sectoral legislation that contains data protection obligations for organisations operating in the financial services, healthcare and telecommunications sectors in Saudi Arabia;
b legislation that contains data protection obligations (e.g., the Cloud Regulations and the Internet of Things Regulatory Framework); and
c extraterritorial data protection legislation that may apply to Saudi companies and individuals by virtue of their overseas activities (e.g., the General Data Protection Regulation (EU) 2016/679 and Personal Data Protection Act BE 2562 (2019)).

For example, Article 3 of the Cyber Law states that anyone who spies on, intercepts or receives data transmitted through an information network or a computer without legitimate authorisation; or invades an individual's privacy through the misuse of camera-equipped mobile phones etc., shall be subject to imprisonment for a period not exceeding one year; or a fine not exceeding 500,000 riyals or both.[56]

Article 3.5.2 of the Cloud Regulations states that cloud service providers are not liable for unlawful content or infringing content that has been uploaded, processed or stored on the cloud service providers' systems. However, Article 3.5.4 of the Cloud Regulations states that cloud service providers must remove such unlawful or infringing content or render it inaccessible within the country after written notice by the CITC or any other authorised entity.[57]

Article 3.5.3 of the Cloud Regulations states that nothing in the same shall be interpreted as a legal obligation on cloud service providers to monitor their systems for unlawful or infringing content. However, Article 3.5.5 of the Cloud Regulations states that cloud service providers may, at their own initiative or following a third-party request, remove from their system or render inaccessible in Saudi Arabia (or any other jurisdiction) any unlawful or infringing content. The foregoing right is exercisable on the condition that such removal is in accordance with the provisions of the cloud contract and the cloud service provider provides adequate notice to the affected customer.

According to the Cloud Regulations:

a unlawful content means software, text, files, audio, video, images, graphics, animations, illustrations, information, personal, business or other data, in any format, whether provided by the customer or a third party, that is unlawful under Saudi laws; and
a infringing content means content, whether provided by the customer or a third party, that infringes a person's intellectual property rights.

Other than the general right to privacy in the Basic Law, at the time of writing we are not aware of any specific legislation protecting children online in Saudi Arabia. However, we note that parents in Saudi Arabia are increasingly using parental control apps to regulate the time that their children spend online.[58]

In addition to the discussion in Section II.i about how cybersecurity concerns are being addressed, the Cyber Law aims to ensure information security, the protection of rights pertaining to the legitimate use of computers and information networks, and the protection of public interest, morals and the national economy.

56 https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf.

57 https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf.

58 '33% of parents in Saudi Arabia worry about harmful online content', *The Saudi Gazette*, 1 April 2020.

IV SPECTRUM POLICY

i Development

The following pieces of legislation regulate this area.

a The Telecom Act: the regulation of radio spectrum usage is one of the main functions of the CITC pursuant to the Telecom Act. Under the Telecom Act, an essential objective of spectrum management is to promote optimal spectrum use by achieving optimum utilisation of this resource, ensuring the creation of a favourable atmosphere to promote and encourage fair competition in all fields of telecommunications, ensuring effective and interference-free usage of frequencies, ensuring clarity and transparency of procedures, ensuring principles of equality and non-discrimination, and ensuring the development of telecommunications technology.

b The National Spectrum Strategy 2025: the CITC has recently published a National Spectrum Strategy 2025[59] that describes the CITC's priorities with respect to the development of Saudi Arabia's spectrum policy going forward. The Spectrum Strategy states that Saudi Arabia has already achieved considerable success in assigning spectrum to public mobile networks that utilise International Mobile Telecommunication standards to provide mobile broadband services, and notes the creation of a dedicated subcommittee in 2019 under the auspices of the CITC to focus on 5G spectrum matters within the National 5G Taskforce.

ii Flexible spectrum use

Under the Spectrum Strategy, a comprehensive review of fixed point-to-point links is contemplated in order to determine the most optimal band plans with the overall objective being to review and optimise a total of 5.4GHz of legacy spectrum by 2025.

Currently, the Spectrum Strategy notes that Saudi Arabia has made notable progress on addressing issues related to the International Mobile Telecommunication (IMT) field, which resulted in it being ranked among the leading nations in awarded IMT spectrum. Furthermore, the Spectrum Strategy also speaks of enabling space spectrum in which the focus would be on championing Saudi Arabia's emerging space industry in international discussions and within Saudi Arabia. This will enable the CITC to work on satellite coordination requests and resolve such requests in a timely manner, thereby allowing existing and future satellite services access to spectrum and manage trade-offs with IMT allocations.

iii Broadband and next-generation services spectrum use

The Spectrum Strategy recognises a number of ways in which the growing need for spectrum for broadband services and next-generation services, among others, is addressed. The Spectrum Strategy states that it aims to identify and resolve existing inefficiencies while overcoming hurdles that prevent international harmonisation and optimal spectrum utilisation. Moreover, there is a push for 5G+ deployment in order to position Saudi Arabia among the leading nations in unlocking innovative high-performance use cases and applications based on 5G.

59 https://www.citc.gov.sa/ar/services/spectrum/Documents/National%20Spectrum%20Strategy_E.pdf.

iv Spectrum auctions and fees

Auctioning spectrum

As of the third quarter of 2020, the CITC has auctioned spectrum to licensed mobile networks operators within Saudi Arabia.

In 2017, the CITC issued a press release stating that it had awarded large blocks of contiguous spectrum, ideal for deployment of next-generation broadband networks across Saudi Arabia to four MNOs.[60] This was the first spectrum auction in Saudi Arabia and the first time spectrum in the 700MHz band has been allocated in the MENA region.

The auction raised 5.8 billion riyals for 50MHz in the 700MHz band and 66MHz in the 1,800MHz band.

We are not aware of any plans to auction spectrum to non-licensed entities.

Spectrum fees

Currently, spectrum users must be licensed by the CITC and such licence is accompanied by a fee to be paid to the CITC calculated in accordance with the CITC's Spectrum Fees of Frequency Usage Policy.[61]

V MEDIA

i Regulation of media distribution generally

In addition to the key laws regulating media and media protection specified in Section II.ii, the following laws are also relevant in regulating media and media protection in Saudi Arabia:

a the National Committee for Regulating Digital Media Content formed pursuant to a Council of Ministers resolution dated 23/03/1435H (corresponding to 24 January 2014);
b the Media Policy in Saudi Arabia issued by the MoM;[62] and
c the General Commission for Audiovisual Media age classification guide.

The media sector may be broadly categorised into the following subsectors: publications, press institutions and audiovisuals. As per the question, this entry predominantly focuses on audiovisuals.

ii Service obligations

In order to engage in broadcasting and other audiovisual media activity in Saudi Arabia, an appropriate licence needs to be obtained. The types of licences contemplated in the licence manual that accompanies the GCAM Implementing Regulations include:

a media content production, and operating media production studios;
b advertising agencies;
c operating cinemas;
d satellite distribution;
e terrestrial transmission;
f satellite uplink stations;

60 https://www.citc.gov.sa/en/MediaCenter/PressReleases/Pages/2017060601.aspx.
61 https://www.citc.gov.sa/en/RulesandSystems/Bylaws/Pages/FinancialSpectrumPolicy.aspx.
62 An official English translation is unavailable on the MoM's website.

g linear and non-linear (e.g., video on demand and over the top) broadcasting;
h radio broadcasting;
i IPTV and cable television;
j media audience measurement; and
k importation, distribution, sale and lease of:
- audiovisual media content;
- cinematic movies, videos and TV shows; and
- receivers and accessories.

Licensees are required to pay the applicable fees and comply with the requirements specified in the licence. Furthermore, licensees are required to (among others):

a comply with the GCAM's policies with regard to prioritising the use of Kingdom resources, including human resources; and
b participate in capacity building in respect of local content production capabilities.

Licensees may need to comply with technical specifications for equipment relating to transmission and reception of media content, and with the allocation of frequencies and associated technical procedures and standards for frequency use.

iii Content restrictions

The Copyright Law protects original and derivative works created in the fields of literature, art and sciences, irrespective of their type, means of expression, importance or purpose of authorship.

The Copyright Law is intended to prevent third parties from copying the protected work. The protection period for sound works, audiovisual works, films, collective works and computer programs is 50 years from the date of the first show or publication of the work, regardless of republication. The protection period for broadcasting organisations shall be 20 years from the date of the first transmission of programs or broadcast materials, and the protection period for the producers of sound recordings and performers shall be 50 years from the date of performance or its first recording, as the case may be.

Cabinet Resolution No. 163 dated 10/24/1417 AH prohibits users within Saudi Arabia from publishing or accessing illegal, harmful or anti-Islamic content on the internet.

Previously, the Internet Service Unit operated a data link that connected Saudi Arabia to the international internet. Users would subscribe to any number of local internet service providers and all web traffic would have been forwarded through servers at the Internet Service Unit. The foregoing structure has been modified, and we understand that multiple data service providers act as a proxy between the internet service providers and the international internet. The CITC is now responsible for administering the internet filtering service, which was previously under the Internet Service Unit's domain.

The CITC provides such services in cooperation with the Permanent Internet Security Committee, and provides a list of banned websites to the data service providers.

Alternatively, users may submit a request to block a particular website where they deem such a website or material to contain undesirable content. Once a user has submitted the web-based form it is reviewed by a team of CITC employees, which determine whether the user's request is justified.

The data service providers are responsible for ensuring that the websites are banned on their internet gateways. If a data service provider fails to comply with the CITC's instructions, it may result in a fine of up to 5 million riyals.[63]

In terms of the content that is filtered, websites and materials that are inconsistent with Islam, for example, materials relating to pornography, gambling and drugs would be classified as harmful content.

The CITC regulates network operators, and the ICT and postal sector. The Telecom Act provides the legal framework for organising this sector.[64]

The GCAM regulates the audiovisual sector[65] and the MoM supervises all means of visual, audio and written communication content in Saudi Arabia.[66]

Pursuant to the Publications Law, a licence from the MoM is required to carry out, among other things, the following activities to print, publish, distribute publications or engage in any other publication services, to import, sell or rent movies or video tapes, to produce, sell or rent computer programs, to engage in any press services and to carry out photography services.

The activities mentioned above are restricted to Saudi nationals. In addition, the holder of a licence may transfer, lease or share ownership of such licence after obtaining the MoM's approval.

The author, publisher, printer or distributor must obtain the MoM's approval prior to circulating such publication. The MoM will not approve a publication that prejudices Islam, the Saudi Arabia regime, the interests of the country or public morals and customs.

As such, we understand that traditional media outlets would fall under the remit of the Publications Law.

As described more fully above, there are three types of licences that can be obtained from the GCAM: media activity licences; cinema licences; and broadcasting and distribution licences. As such, we understand that emerging platforms are more likely to fall within the GCAM Regulations and GCAM Implementing Regulations.

iv Internet-delivered video content

There is limited information on how the move from broadcast video distribution to internet video distribution has affected consumers and the ability of internet service providers to control, and be compensated for, the content being transmitted over their networks.

However, according to the CITC's 2017 Annual Report, the penetration rate of internet services has soared over the past years from 64 per cent in 2014 to around 82 per cent by the end of 2017 and, accordingly, the demand for internet and broadband services has risen.[67]

Furthermore, '96% of people inside the country use the internet, compared to just 2% in the year 2000, while 99% of the country's area has internet access.'[68] As such, it is

63 Freedom of the Net 2019, Saudi Arabia, Freedom House.

64 https://www.citc.gov.sa/en/AboutUs/AreasOfwork/Pages/default.aspx.

65 https://www.gcam.gov.sa/en/AboutUs#Tab1.

66 https://www.my.gov.sa/wps/portal/snp/pages/agencies/agencyDetails/AC164/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zivQIsTAwdDQz9LQwNzQwCnS0tXPwMvYwNDAz0g1Pz9L30o_ArAppiVOTr7JuuH1WQWJKhm5mXlq8f4ehsaGaiX5DtHg4AfoZqHw!!/.

67 Page 136 of the CITC's 2017 Annual Report: https://www.citc.gov.sa/en/mediacenter/annualreport/Documents/PR_REP_013Eng.pdf.

68 'How Saudi Arabia is deploying ICTs against COVID-19 — and beyond', *The Saudi Gazette*, 25 July 2020.

reasonable to presume that the move from broadcast video distribution to internet video distribution has not had a significant negative impact on consumers as 96 per cent of the population in Saudi Arabia has some form of access to the internet.

VI THE YEAR IN REVIEW

In January 2020, the CITC launched a competition to award licences to new MVNOs in Saudi Arabia.[69] The process at the time of writing and is expected to conclude in the fourth quarter of 2020.

In July 2020, Saudi Arabia hosted a meeting of G20 Digitial Economy Ministers.[70] The meeting brought together all G20 members as well as the OECD and the International Telecommunication Union as knowledge partners and focused on a number of areas that are relevant to the creation of global digital economies (i.e., trustworthy artificial intelligence, cross-border data flows, smart cities, the development of a common framework for measuring the digital economy and maintaining digital security and trust).

In August 2020, the CITC issued a cybersecurity regulatory framework for ICT and postal sector service providers.[71] The framework is intended to increase the cybersecurity maturity of such service providers and mainly concerns organisations that are licensed or registered by the CITC or subject to its regulation in Saudi Arabia.

In October 2020, the CITC launched a regulatory sandbox for delivery applications.[72] The regulatory sandbox is designed to 'support, enable, and sustain the growth of Saudi Arabia's delivery app ecosystem, for the benefit of all sector stakeholders, including consumers, producers, and delivery drivers'.

Also in October 2020, and as noted above, the NCA issued the final draft of its Cloud Cybersecurity Controls – CCC-1:2020.[73]

VII CONCLUSIONS AND OUTLOOK

The technology, media and telecommunications sectors are core to the future economic development of Saudi Arabia and, accordingly, it is likely that we will see further legislative and regulatory developments with respect to these sectors over the next few years.

Looking ahead, we would not be surprised to see further legislation or regulation in one or more of the following areas:

a Implementation of a national data privacy regime: in 2020 we saw the implementation of new privacy regimes in Abu Dhabi, Dubai and Egypt. It would be consistent with both regional trends and Saudi Arabia's desire to grow its digital economy to see a dedicated privacy law and privacy regulator put in place in Saudi Arabia.

69 https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Licenses/LicensingRegulatoryFrameworks/Documents/MVNO-RFA-EN.pdf.

70 https://www.mcit.gov.sa/en/media-center/news/301563 and https://g20.org/en/media/Documents/G20SS_Declaration_G20%20Digital%20Economy%20Ministers%20Meeting_EN.pdf.

71 https://www.citc.gov.sa/en/mediacenter/pressreleases/Pages/20200410.aspx and https://www.citc.gov.sa/en/RulesandSystems/CyberSecurity/Documents/CRF-en.pdf.

72 https://www.citc.gov.sa/en/mediacenter/pressreleases/Pages/20200410.aspx.

73 https://nca.gov.sa/files/ccc-en.pdf.

b Reform to national intellectual property laws and registration authorities: the Saudi Authority for Intellectual Property was launched in 2018 and has been busy in 2020 with various public consultations on changes to Saudi Arabia's intellectual property regime.[74] These changes are aligned to the Authority's stated mission (i.e., 'promoting the competitiveness of the national economy, supporting the growth of the intellectual property culture in Saudi Arabia') and will be of significant interest to technology, media and telecommunications companies that seek to generate, protect and license intellectual property in Saudi Arabia.

c Promotion and support for further foreign direct investment in the TMT sector: the Saudi Arabian General Investment Authority was converted into the MISA in 2020 and we expect that throughout 2021 and beyond, the MISA will seek to implement further measures, including potential regulatory reform, to promote Saudi Arabia as a world-class investment destination.

In short, we expect the next few years to be a very exciting time to be a TMT lawyer operating in Saudi Arabia.

74 https://www.saip.gov.sa/en/public-opinions/.

Appendix 1

ABOUT THE AUTHORS

BRIAN MEENAGH

Latham & Watkins LLP

Brian Meenagh is a partner at Latham & Watkins and leads its Middle East data and technology transactions practice. He represents companies, financial institutions, and government entities in a range of complex transactions involving data, technology and intellectual property assets, both in the Middle East and internationally. Brian serves a diverse client base ranging from startups to governments to many of the world's leading financial services, healthcare and technology companies and has particular experience advising on multi-jurisdictional transactions involving businesses in the Middle East.

ALEXANDER HENDRY

Latham & Watkins LLP

Alexander Hendry is a senior associate in Latham & Watkins' data and technology transactions practice. He specialises in the negotiation and drafting of complex technology contracts for commercial transactions and collaborations, and giving strategic advice on large-scale, business-critical, first-of-their-kind technology projects. He advises clients across the globe on legal and commercial issues relating to technology, outsourcing, fintech, commercial contacts, intellectual property, and data privacy. Alexander has practised in the United Kingdom, Asia and the Middle East.

AVINASH BALENDRAN

Latham & Watkins LLP

Avinash Balendran is an associate in Latham & Watkins' data and technology transactions practice, based in Dubai. Avinash has experience advising clients across a range of sectors including healthcare, private equity, and financial services on a variety of technology and commercial issues. Avinash is also a certified information privacy professional/Europe and has experience advising companies on GDPR compliance projects, on technology-related regulatory issues in the United Arab Emirates and Saudi Arabia, and drafting and negotiating complex commercial contracts through working on a number of landmark deals in the Middle East.

HOMAM KHOSHAIM

Law Office of Salman M Al-Sudairi

Homam Khoshaim is a senior associate in the Law Office of Salman M Al-Sudairi, based in Riyadh. He advises on a broad range of transactions, including M&A, emerging companies, venture capital, joint ventures, initial public offerings and other equity capital markets transactions and corporate advisory work. He also has specialised knowledge in antitrust and competition, payments and emerging financial services, and entertainment, sports and media matters. Homam is a New York qualified attorney and a solicitor of England and Wales.

LOJAIN AL-MOUALLIMI

Law Office of Salman M Al-Sudairi

Lojain Al-Mouallimi is an associate in the Law Office of Salman M Al-Sudairi, based in Riyadh. Lojain advises Saudi Arabian and international clients on a broad range of corporate, commercial and bankruptcy issues. Lojain was previously with the Olayan Group where she focused on compliance, M&A and litigation. She holds a juris doctor degree from the University of Notre Dame and is a certified mediator in the state of Indiana.

LATHAM & WATKINS LLP

ICD Brookfield Place, Level 16
Dubai International Financial Centre
PO Box 506698
Dubai
United Arab Emirates
Tel: +971 4 704 6300
Fax: +971 4 704 6499

Law Office of Salman M Al-Sudairi
Al-Tatweer Towers, 7th Floor, Tower 1
King Fahad Highway, PO Box 17411
Riyadh 11484
Saudi Arabia
Tel: +966 11 207 2500
Fax: +966 11 207 2577

brian.meenagh@lw.com
alexander.hendry@lw.com
avinash.balendran@lw.com
homam.khoshaim@lw.com
lojain.al-mouallimi@lw.com
www.lw.com

Chapter 19

UNITED KINGDOM

John D Colahan, Gail Crawford and Lisbeth Savill[1]

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 2020–21 Annual Plan (updated in September 2020).[2] They include improving broadband and mobile coverage across the UK, protecting consumer rights, supporting UK broadcasting by maintaining a media environment that supports society, protection of consumers online, enabling strong and secure networks, sustaining the universal postal service during the covid-19 pandemic, and increasing diversity and inclusion. Legislation and government guidance on changes to law with effect from 1 January 2021 should also be noted.

European and national law and standards currently govern the UK data protection framework (and equivalent standards will continue to apply following Brexit) 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)[3] (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).

---

1 John D Colahan, Gail Crawford and Lisbeth Savill are partners at Latham & Watkins LLP. The authors would like to acknowledge the kind assistance of their colleagues Rachael Astin, Alexandra Luchian, Amy Smyth, Sarah Miller, Katie Henshall and Emma Pianta in the preparation of this chapter.

2 Ofcom's Plan of Work 2020/21 available at https://www.ofcom.org.uk/__data/assets/pdf_file/0029/194753/statement-ofcom-plan-of-work-2020-21.pdf.

3 Directive (EU) 2016/1148.

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.[4]

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.

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.[5] Ofcom's main duties include:

a ensuring optimal use is made of the radio spectrum;
b ensuring the UK has a wide range of electronic communications services;
c ensuring a wide range of high-quality television and radio services are provided by a range of different organisations, appealing to a range of tastes and interests;
d ensuring people are protected from harmful or offensive material, unfair treatment and invasion of privacy on television and radio;
e 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
f ensuring the universal service obligation on postal services is secured in the UK.

Ofcom's priorities and major work areas for 2020 and 2021 were published on 30 April 2020,[6] and updated on 29 September 2020.[7]

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:

a the Wireless Telegraphy Act 2006;
b the Digital Economy Act 2010;
c the Consumer Rights Act 2015;

4 See Ofcom statement, Renewal of the co-regulatory arrangements for broadcast advertising, 4 November 2014, available at https://www.asa.org.uk/news/renewal-of-co-regulatory-arrangement-for-broadcast-advertising.html.

5 Section 3(1) of the Act.

6 Ofcom's Plan of Work 2020/21 available at https://www.ofcom.org.uk/__data/assets/pdf_file/0029/194753/statement-ofcom-plan-of-work-2020-21.pdf.

7 September 2020 update available at https://www.ofcom.org.uk/__data/assets/pdf_file/0018/203724/pow-2020-21-sept-update.pdf.

d the GDPR and the Data Protection Act 2018, and following the end of the Brexit transition period, the UK-GDPR;
e the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011);
f European Regulation 2017/003 (e-Privacy Regulation), once it takes effect;
g the NISD and the NIS Regulation;
h the Freedom of Information Act 2000;
i the Investigatory Powers Act 2016;
j the Enterprise Act 2002;
k the Copyright, Designs and Patents Act 1988 (CDPA);
l the Digital Economy Act 2017 (DEA);
m the Competition Act 1998;
n the Consumer Rights Act 2015;
o the European Electronic Communications Code Directive,[8] establishing the European Electronic Communications Code; and
p the European Union (Withdrawal) Act 2018.

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[9] and the corresponding UK implementing legislation, the Data Protection Act 1998, and introduces more stringent standards and an enhanced enforcement regime.

In April 2018, the government announced in the Modernising Consumer Markets Green Paper[10] 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).[11] The recommendations in the Furman Report included:

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);

8 Directive 2018/1972 establishing the European Electronic Communications Code.

9 Directive 95/46/EC.

10 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/699937/modernising-consumer-markets-green-paper.pdf.

11 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

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 1 July 2020, the CMA published its final report concluding the market study into online platforms and advertising. The CMA concluded that it will not be launching a market investigation, as a market investigation would risk cutting across broader regulatory reform and that launching a market investigation at this time would be inappropriate given the disruption caused by the covid-19 pandemic. The CMA also concluded that existing laws are not suitable for effective regulation and recommended that the UK government introduce legislation for what the CMA described as 'a new *ex ante* pro-competition regulatory regime to govern the behaviour of major platforms funded by digital advertising'. The CMA has launched a Digital Markets Taskforce in conjunction with Ofcom and the ICO to advise the UK government on designing the regulatory regime. The Taskforce will focus on the test that might be used to identify firms with strategic market status (SMS), which online activities may be regulated, and the remedies that could be applied for harm. Stakeholders were invited to send their responses and complete questionnaires by 31 July 2020. The Taskforce intends to provide advice to the UK government by the end of 2020; 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 CMA acknowledged in its final report published on 1 July 2020 that many of the concerns identified in digital markets are international in nature and, as such, has engaged with other international competition authorities with a view to developing a consensus. The CMA has stated that it intends to advocate proactively for *ex ante* regulation for platforms.

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.

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 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.[12]

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.[13]

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

12 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.

13 The CMA and Ofcom have signed a memorandum of understanding in respect of their concurrent competition powers in the electronic communications, broadcasting and postal sectors. This is available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/502645/Ofcom_MoU.pdf.

confirmed by the Competition Appeal Tribunal.[14] 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. 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.[15]

Following the 2017 National Security and Infrastructure Investment Review Green Paper,[16] 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.[17]

In June 2020, in the context of the covid-19 pandemic, the UK government announced that it would introduce a new public interest consideration under the Enterprise Act 2002 under which the UK Secretary of State can intervene in transactions on public health emergencies grounds.[18]

In July 2020, the UK's merger regime for transactions in the defence and technology sectors was further amended to include three additional categories of enterprises (artificial intelligence, advanced materials and cryptographic authentication) to which the lower £1 million threshold and lower share of supply threshold apply.[19]

v 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

14 *Lebedev Holdings Limited and Another v. Secretary of State for Digital, Culture, Media and Sport* [2019] CAT 21, judgment available at https://www.catribunal.org.uk/sites/default/files/2019-08/1328_Lebedev_Judgment_160819.pdf.

15 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).

16 Available at https://www.gov.uk/government/consultations/national-security-and-infrastructure-investment-review.

17 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 Bidco Ltd (CMA case page available at: https://www.gov.uk/cma-cases/connect-bidco-inmarsat-merger-inquiry?utm_source=65f2270a-d8f3-472d-ae23-ed623f071cd0&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate).

18 See https://www.legislation.gov.uk/uksi/2020/627/pdfs/uksi_20200627_en.pdf.

19 The Department for Business, Energy and Industrial Strategy's guidance to the changes is available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902531/Enterprise_Act_2002_guidance_on_changes_to_the_turnover_and_share_of_supply_tests_for_mergers__Orders_2020_.pdf.

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.[20]

A further initiative as part of the European Digital Strategy is the Digital Services Act package announced by the European Commission to strengthen the Single Market for digital services and foster innovation and competitiveness of the European online environment, based on two main pillars: framing the responsibilities of digital services and *ex ante* rules covering large online platforms acting as gatekeepers. In June 2020, the Commission initiated a public consultation to identify specific issues that may require EU-level intervention that closed on 8 September 2020.[21]

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. 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.[22] 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.[23] In its mid-term review, the Commission identified online platforms as one of three emerging challenges, and proposed

20 Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53056.

21 Available at https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

22 Available at https://ec.europa.eu/digital-single-market/en/news/online-platforms-new-rules-increase-transparency-and-fairness.

23 'Online Platforms and the Digital Single Market; Opportunities and Challenges for Europe' SWD (2016) 172 available at https://ec.europa.eu/digital-single-market/en/news/communication-online-platforms-and-digital-single-market-opportunities-and-challenges-europe; page 8 of https://eur-lex.europa.eu/resource.html?uri=cellar:a4215207-362b-11e7-a08e-01aa75ed71a1.0001.02/DOC_1&format=PDF.

the implementation of actions to tackle these challenges.[24] 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 take an initial step in regulating online platforms, and 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, or the Platform to Business Regulation[25]) includes measures seeking to reduce unfair trading practices, increase transparency, resolve disputes more effectively as well as establishing an EU Observatory on the Online Platform Economy to monitor the impact and implementation of the new rules.[26] The new Regulation came into force on 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 applies 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.[27] For this reason, the Regulation does not affect online television, films, streamed sports, music, e-books or games. However, the Commission has stated its intention to 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; this review is expected to be released in 2021.

Telecoms

The current European Commission telecoms and connectivity proposals include:

a recasting the Framework, Authorisation, Access and Universal Services Directives as one directive, the European Electronic Communications Code;

b upgrading BEREC to a fully fledged EU agency;

c a 5G Action Plan for the development and deployment of 5G networks in Europe; and

d a WiFi4EU initiative to aid European villages and cities roll out free public Wi-Fi.

24 Available at https://ec.europa.eu/digital-single-market/en/news/digital-single-market-commission-calls-swift-adoption-key-proposals-and-maps-out-challenges.

25 Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1150.

26 Available at https://ec.europa.eu/digital-single-market/en/news/commission-decision-group-experts-observatory-online-platform-economy.

27 Available at https://ec.europa.eu/digital-single-market/en/news/geo-blocking-regulation-questions-and-answers.

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.[28] Ofcom confirmed in August 2020 that it would auction more airwaves through a bidding process due to start in January 2021.[29]

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 21 December 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

28 See: https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/results-auction-mobile-airwaves.

29 See: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020/plans-for-spectrum-auction.

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 budget of over €130 million has been allocated to implement free Wi-Fi across the EU, and 29,195 municipalities have registered to the initiative.[30] 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 & 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.

From April 2016, the Regulation on Open Internet Access[31] 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).

30 See: https://ec.europa.eu/digital-single-market/en/news/overview-wifi4eu-winners and https://wifi4eu.ec.europa.eu/#/home.

31 Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN.

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. Ofcom's latest annual report on its approach to assessing compliance with the Regulation on Open Internet Access was published in July 2020.[32] Ofcom's report covers monitoring the quality of internet access services; safeguarding open internet access; transparency measures; and complaints and remedies. The Regulation on Open Internet Access requires NRAs, such as Ofcom, to issue such reports annually.

ii 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.[33] 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.[34] Consumers and businesses are now able to request connections since 20 March 2020.[35]

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.

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. Among the provisions of the DEA is a maximum penalty for online copyright infringement of 10 years. 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

32 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0033/197709/net-neutrality-report-2020.pdf.

33 Available at http://www.legislation.gov.uk/uksi/2018/445/made.

34 Available at https://www.ofcom.org.uk/consultations-and-statements/category-1/delivering-broadband-universal-service.

35 See https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/broadband-uso-advice.

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, 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.

In March 2018, the government launched the Creative Industries Sector Deal, which included various specific commitments of interest concerning the tackling of online infringement of copyright. As part of the deal, funding was committed to extend the Get it Right from a Genuine Site campaign.[36]

The availability of defences for online intermediaries in respect of unlawful content is currently governed primarily at a European level by the E-Commerce Directive,[37] as implemented into UK law by the Electronic Commerce (EC Directive) Regulations 2002 and applicable case law (although the implementation of the new Copyright Directive will bring changes to the current EU regime). The E-Commerce 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,[38] as amended by the ePrivacy Directive;[39] 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),[40] which is currently partway through the European legislative review process. However, no draft has yet been agreed by the Member States in the Council, and negotiations on the latest draft are ongoing.

The GDPR continues to be directly applicable in the UK during the Brexit transition period (31 January 2020 to 31 December 2020), alongside the DPA. Following the end of that transition period, the DP Brexit Regulations[41] will come into force to put in place the UK's post-Brexit data protection regime. The retained EU GDPR and the UK's 'applied GDPR' (i.e., the EU GDPR as applied via the DPA in areas otherwise outside the scope of the EU GDPR) are effectively merged to create the UK-GDPR. The DPA continues

36 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/695097/creative-industries-sector-deal-print.pdf.

37 Directive 2000/31/EC.

38 Directive 2002/58/EC.

39 Directive 2009/136/EC.

40 Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

41 The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

to apply, subject to amendments made by the DP Brexit Regulations to ensure the proper functioning of the DPA in conjunction with the UK-GDPR. In effect, the UK regime will therefore retain the standards of the EU GDPR following Brexit, but the UK-GDPR will not automatically incorporate any changes made to the EU GDPR in the future. Following the end of the transition period, in certain circumstances an organisation in the UK may need to comply with both the EU GDPR and the UK-GDPR/DPA. This would be the case if the UK organisation is either processing personal data about European individuals prior to 31 December 2020 (in which case the EU GDPR will continue to apply to that ongoing processing), or if it has operations in or provides services to individuals in the EU and is caught by the EU GDPR's extraterritorial application.

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 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.

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;[42] 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).

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:

a 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);

b 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

c 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 legal bases for the transfer of personal data from the EU and the UK (following the end of the Brexit Transition Period) to countries outside the EU/UK, of which one has recently been invalidated (the Privacy Shield, successor to the Safe Harbor) and another is subject to ongoing challenge (standard contractual clauses, also known as model clauses).

42 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.

Under the historic Safe Harbor agreement, if a US recipient of personal data was self-certified under the US Safe Harbor regime, personal 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, and included additional safeguards for the protection of personal data.

In the meantime, in May 2016, Max Schrems filed a complaint with the Irish Data Protection Commissioner concerning the legal status of data transfers to the US 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.[43] 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. By July 2019, the Privacy Shield had undergone two joint reviews by the US and European authorities: both of which ultimately concluded that the Privacy Shield remained an effective mechanism for the transfer of personal data to the US, though made several proposals for improvement. In the *Schrems II* case, the Advocate General delivered his non-binding opinion on 19 December 2019,[44] which questioned the validity of the Privacy Shield and also challenged the adequacy of the standard contractual clauses to transfer personal data to the US. In its judgement of 16 July 2020,[45] the CJEU invalidated the Privacy Shield with immediate effect, meaning that it can no longer be relied on to ensure compliance with the GDPR for relevant existing or future data exports to the US. The CJEU held that the standard of protection afforded to personal data under the GDPR and European fundamental rights laws could not be guaranteed by the Privacy Shield, primarily due to what it held to be a lack of proportionality of specific US national security laws, as well as a lack of effective and enforceable rights for data subjects.

In relation to the standard contractual clauses, the CJEU held that the model clauses remain valid as a mechanism for personal data transfer outside the EU/UK, but that they cannot be used if the legislation in the third country does not enable the recipients to comply with their obligations. Further, the CJEU found that reliance on the standard contractual clauses alone was not necessarily sufficient in all circumstances, and that each data transfer (to any third country, including onwards transfers) must be assessed on a case-by-case basis to ensure adequate protection for the data. If, in the relevant context, the standard contractual

43 Available at www.dataprotection.ie/docs/25-05-2016-Statement-by-this-Office-in-respect-of-application-for-Declaratory-Relief-in-the-Irish-High-Court-and-Referral-to-the-CJEU/1570.htm.

44 Available at http://curia.europa.eu/juris/documents.jsf?num=C-311/18.

45 *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems* [2020] C-311/18.

clauses are assessed to insufficiently protect individuals' data, additional safeguards should be put in place. Finally, the CJEU made clear that, if a competent supervisory authority believes that the standard contractual clauses cannot, in relation to a specific data transfer, be complied with in the recipient country and the required level of protection cannot be secured by other means, such supervisory authority is under an obligation to suspend or prohibit that transfer (unless the data exporter has already done so itself).

Following the CJEU's decision, the Irish Data Protection Commissioner is required to consider the specific case of Facebook's relevant transfers of data to the US: proceedings are ongoing.

This decision of the CJEU applies to data transfers from the UK to third countries outside of the EEA during the Brexit transition period, and is binding on UK courts. The government and ICO are expected to release further guidance on the UK approach to data transfers to the US and more widely following the end of the transition period. After 1 January 2021, the UK will become a third country for the purposes of data transfers from the EEA, and the third country transfer restrictions under the GDPR will apply, unless and until an adequacy decision is granted by the European Commission in favour of the UK; this is currently under negotiation, during which a number of potential issues have been raised around the UK's surveillance and communications interception regimes.

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.[46] Further, the data subject must have the right to withdraw consent at any time.[47] The ePrivacy UK Regulations apply the GDPR standard of consent for the purposes of those Regulations, including in relation to cookies. In July 2019, the ICO updated its guidance on cookies,[48] 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

46 General Data Protection Regulation: Recitals 26, 30 and 32.

47 General Data Protection Regulation: Article 7(3).

48 Available at https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/.

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 user 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 Code acts to expand the scope of the ePrivacy Directive to OTT communications providers, who will therefore come within the remit of the various restrictions on uses of content, traffic and location data set out in the ePrivacy Directive (and national implementing legislation such as the ePrivacy UK Regulations).

The Draft ePrivacy Regulation (which is not yet in final form and therefore subject to further changes) aims to develop 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 (as already achieved in effect by the Code), 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 establishing that 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;

e 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

f 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 for the Council to reach agreement on a proposed text; the latest draft under discussion was published by the Croatian Council presidency in February 2020. 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 (including the latest draft released in February 2020), the ePrivacy Regulation is expected to come into force two years after its finalisation and publication date. Given the criticism of the current 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. As the ePrivacy Regulation will not enter into force prior to the end of the Brexit transition period (30 December 2020), the Regulation will not be directly applicable in the UK; the ePrivacy UK Regulations will continue to apply as UK national law, subject to amendments introduced by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419 (which primarily ensure the proper functioning of the ePrivacy UK Regulations alongside the amended DPA and UK-GDPR from 1 January 2021).

Enforcement

The ICO is responsible for the enforcement of, amongst other legislation, 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). As a result of Brexit, the ICO remains responsible for the enforcement of these UK regimes, but is outside the scope of any related European associations (for example, the European Data Protection Board).

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 2019 and 2020,[49] the ICO has particularly focussed its investigation and enforcement efforts on the following topics: improving data security practices, reducing unlawful access, and addressing compliance concerns about the use of new surveillance technology. The ICO's actions in the past year were a mix of Data Protection Act 1998 (DPA 1998) and DPA matters. Under the DPA 1998, the ICO has issued a number fines in recent years at the level of the maximum available financial sanction (£500,000). The most recent of these fines was imposed against Cathay Pacific Airways, in March 2020, for information security failings resulting in the exposure of customer personal data.[50] Prior to that, in January 2020, the ICO issued a £500,000 fine against DSG Retail Limited following a cyberattack impacting its point-of-sale system that affected over 14

49 Available at https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

50 Available at https://ico.org.uk/action-weve-taken/enforcement/cathay-pacific/.

million people.[51] The ICO issued two similar fines at this level in 2018. 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. Facebook subsequently appealed the fine, and Facebook and the ICO ultimately reached a settlement in October 2019, with Facebook agreeing to pay the £500,000 fine with no admission of liability.[52] 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 is also taking action under the DPA. The ICO issued its first (and only, to date) monetary penalty notice under the DPA in December 2019, imposing a fine of £275,000 against Doorstep Dispensaree Ltd for failing to properly secure health information. The ICO's proposed fines under the GDPR/DPA against British Airways and Marriott International, both announced in July 2019, remain its most significant proposed sanctions. These investigations are ongoing and the final level of fines imposed is not yet known. On 8 July 2019, 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 an ongoing, European-wide trend of data protection supervisory authorities starting to utilise their increased powers under the GDPR to impose significant fines, and indicate 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 127,940 complaints under the ePrivacy UK Regulations in 2019–2020 (down from 138,368 in 2018–2019). The majority of fines imposed under the ePrivacy UK Regulations relate to automated marketing calls. In March 2020, the ICO issued the highest-ever nuisance calls fine of £500,000 to CRDNN Limited, which was responsible for more than 193 million automated nuisance calls.[53]

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

51 Available at https://ico.org.uk/action-weve-taken/enforcement/dsg-retail-ltd/.

52 Available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/statement-on-an-agreement-reached-between-facebook-and-the-ico/.

53 Available at https://ico.org.uk/action-weve-taken/enforcement/crdnn-limited-mpn/.

person of the data breach without undue delay.[54] 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.[55] As a result of this strengthening of the requirements 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[56] and 11,854 notifications in 2019–2020.[57] The ICO reports that in 95 per cent of the reported cases in 2019–2020, 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.[58]

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). DRIPA included a sunset clause which provided for automatic expiry of its provisions on 31 December 2016, though it was subject to a number of legal challenges prior to (and following) that date. 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).[59] The Court of Appeal referred the case to the CJEU, which held, on 21 December 2016, that the ePrivacy Directive and the Charter of Fundamental Rights

54 General Data Protection Regulation: Articles 33 and 34.

55 General Data Protection Regulation: Article 83(4)(a).

56 Available at https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

57 Available at https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

58 Available at https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

59 *R (Davis & Watson) v. Secretary of State for Home Department* [2015] EWHC 2092.

preclude laws that require a general and indiscriminate retention of data. The CJEU ultimately referred back to the Court of Appeal, which agreed that the DRIPA data retention provisions were incompatible with EU law (in its final judgment delivered on 30 January 2018).[60]

The current regime is governed primarily by the Investigatory Powers Act 2016 (IPA) and RIPA. The IPA overhauls, and in some cases extends, the scope of RIPA, and also repeals Part One of RIPA (which covered the interception and acquisition of communications data). The IPA has been rolled out by various different statutory instruments, the latest of which brought all remaining provisions into force on 22 July 2020.[61] The remaining provisions of RIPA (i.e., those not repealed by the IPA) remain effective, and broadly cover direct surveillance, covert human intelligence, and obtaining electronic data protected by encryption. 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);

f 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;

g 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);

h 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;

i provides local government with some investigatory powers (e.g., to investigate someone fraudulently claiming benefits), but not access to internet connection records;

j creates a new criminal offence for unlawfully accessing internet data; and

60 *Secretary of State for the Home Department v. Watson* [2018] EWCA Civ 70.

61 The Investigatory Powers Act 2016 (Commencement No. 12) Regulations 2020 (SI 2020/766).

k creates a new criminal offence for a TO or someone who works for a TO to reveal that data has been requested.

Both the RIPA and IPA have been subject to legal challenges in recent years (following the claims brought against DRIPA). In April 2018, the UK High Court ruled that the then-current provisions of 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.[62] 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. In *Privacy International v. UK*,[63] the CJEU recently reiterated that national law derogations from European fundamental rights of privacy must be strictly necessary and proportionate. It determined that UK legislation[64] authorising the acquisition and use of bulk communications data by the UK security and intelligence agencies for national security purposes did not meet the required proportionality standards or provide for sufficiently objective criteria to define how those authorities exercise their powers. Following this preliminary ruling from the CJEU, proceedings have been referred back the UK courts.

On 13 September 2018, the European Court of Human Rights ruled in the case of *Big Brother Watch and Others v. the United Kingdom*[65] 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[66] requested that the case be referred to the Grand Chamber at the European Court of Human Rights, where it was heard in July 2019:[67] judgment is expected before the end of 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.

62 *R (on the application of National Council for Civil Liberties (Liberty)) v. Secretary of State for Home Department* [2018] EWHC 975.

63 *Privacy International* (case C-623/17).

64 The Telecommunications Act 1984 and RIPA.

65 ECHR 299 (2018).

66 The Court heard three cases simultaneously: (1) *Big Brother Watch and Others v. United Kingdom* (Case No. 58170/13); (2) *10 Human Rights Organisations and Others v. United Kingdom* (Case No. 24960/15); and (3) *Bureau of Investigative Journalism and Alice Ross v. United Kingdom* (Case No. 62322/14).

67 Hearing recording available athttps://echr.coe.int/Pages/home.aspx?p=hearings&w=5817013_10072019&language=en&c=&py=2019

Protection for children

Under the GDPR, children are defined as vulnerable natural persons who merit specific protection with regard to their personal data.[68] 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.[69] 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.[70] The ICO published its Age Appropriate Design Code[71] in January 2020, and it came into force on 2 September 2020 with a 12-month transition period. The Code is a statutory Code of Practice under the DPA, setting out guidance on the application of the GDPR and DPA in the context of children's personal data and children's use of digital services. It is made up of 15 standards focussing on providing default settings which ensure an automatic high level of data protection safeguards for online services likely to be accessed by children. The standards cover topics such as: data sharing; data minimisation; transparency; parental controls; nudge techniques; and profiling.

On 8 April 2019, the Home Office and DCMS published an Online Harms White Paper[72] for public consultation, which builds on the proposed measures set out in the government's Green Paper titled Internet Safety Strategy, published in May 2018.[73] The White Paper proposes a new compliance and enforcement regime intended to combat online harms, including measures aimed at protecting children. The regime is designed to force online platforms to move away from self-regulation and sets out a legal framework to tackle users' illegal and socially harmful activity. The proposals extend to all organisations that provide online platforms allowing user interaction or user-generated content. The government issued its initial response to the White Paper consultation on 11 February 2020, which set out preliminary details of the proposed new regulatory regime to govern content posted on online platforms, and confirmed that an active 'duty of care' will be introduced, requiring organisations to prevent certain content from appearing on their platforms. The governments initial response also indicated that it is minded to appoint Ofcom as the new regulator of harmful content and conduct online. A full government response is expected in 2020.

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.

68 General Data Protection Regulation: Recitals 38 and 75.

69 General Data Protection Regulation: Article 8.

70 General Data Protection Regulation: Article 17.

71 Available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.

72 Available at https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.

73 Available at https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper.

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[74] and an Education for a Connected World Framework,[75] which together aim to assist, among other organisations, schools and child services providers to integrate digital resilience into education and other child settings and to identify the specific skills children need to manage online risks. 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.[76] 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,[77] 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.[78] 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),

74 Available at https://www.gov.uk/government/publications/digital-resilience-framework.

75 Available at https://www.gov.uk/government/publications/education-for-a-connected-world.

76 Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

77 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805677/National_Cyber_Security_Strategy_Progress_Report.pdf.

78 Available at https://ec.europa.eu/digital-single-market/en/what-radio-spectrum-policy.

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 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,[79] the majority of which related to phishing 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[80] and the Authorisation Directive,[81] 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.[82]

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

79 Available at https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

80 Directive 2002/21/EC.

81 Directive 2002/20/EC.

82 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0028/68239/statement.pdf.

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 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.

iii Broadband and next-generation mobile spectrum use

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.[83] The technology has provided more capacity at faster speeds for mobile services on smartphones such as video streaming, email and social networking sites. On 24 July 2020, Ofcom announced that it is reviewing its existing regulations further to support growing demand from UK customers.[84]

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 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.

In July 2019, the UK published a consultation paper in relation to the proposed approach to implementation of the European Electronic Communications Code Directive.[85] 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. The UK government conducted a consultation on the implementation of the Code in mid-2019, and published its response in July 2020.[86]

83 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0032/98159/5p8-Regs.pdf.

84 See: https://www.ofcom.org.uk/consultations-and-statements/category-2/improving-spectrum-access-for-wi-fi.

85 Available at https://www.gov.uk/government/consultations/implementing-the-european-electronic-communications-code.

86 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902879/Government_response_EECC.pdf.

The response after the consultation confirmed that the UK government will ensure that UK law remains operable after implementing the Code, and that it would grant a 12-month period for the telecoms industry to implement the most onerous measures. Ofcom is due to publish a statement setting out the detailed approach in autumn 2020.

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.

Ofcom confirmed on 3 August 2020 that another 5G spectrum auction will take place in January 2021, as the 2018 5G auction will not cover the anticipated demand for 5G once it is commercially available.[87]

Ofcom 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.[88] 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.[89] Ofcom confirmed in its report published on 13 March 2020 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.[90] 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.

87 https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020/plans-for-spectrum-auction.

88 Available at https://www.ofcom.org.uk/consultations-and-statements/category-1/award-700mhz-3.6-3.8ghz-spectrum.

89 Available at https://www.ofcom.org.uk/consultations-and-statements/category-3/defragmentation-spectrum-holdings.

90 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0020/192413/statement-award-700mhz-3.6-3.8ghz-spectrum.pdf and https://www.ofcom.org.uk/__data/assets/pdf_file/0034/199717/statement-sut-modelling-700mhz-3.6-3.8ghz-spectrum.pdf.

vi 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.

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 grappling with new business models to monetise content and frameworks to provide sufficient protection for the rights of content creators and consumers alike. The Commission's DSM Strategy has had implications for the UK media sector (subject to changes to national law as a result of Brexit). covid-19 has caused huge disruption to content production, but has helped to drive uptake of new digital media offerings.

i Superfast broadband and media

Fast broadband underpins the accessibility to consumers of internet-delivered content services. As demand for internet data in the UK accelerates, so do calls for the UK's broadband infrastructure to be upgraded.

In January 2020, Ofcom proposed new regulations to assist in fuelling full-fibre infrastructure for the whole of the UK. As part of this, Ofcom opened a consultation which closed on 1 April 2020, with results to be published in early 2021. As part of the UK's commitment to superfast broadband, the government announced that 96 per cent of UK households now have access to superfast broadband (speeds of 24Mbps or more) coverage and plans have been announced to develop the Superfast Broadband Programme until 2026 as part of the UK Next Generation Network Infrastructure Deployment Plan.[91]

91 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/418567/UK_Next_Generation_Network_Infrastructure_Deployment_Plan_March_15.pdf.

Since 2017, full-fibre coverage in the UK has trebled.[92] The focus has now shifted to exploring ways to take superfast broadband to the most remote and hardest-to-reach places in the UK. On 19 May 2019, the government launched the Rural Gigabit Connectivity programme, established to trial a model to deliver full-fibre broadband to premises in rural and remote areas.[93] This is consistent with the DEA, which provided for a USO whereby consumers may request a minimum download speed of 10Mbps by 2020. In August 2020 the government announced that almost half a million premises now have access to gigabit technology.[94] In March 2020, the government announced a £5 billion commitment through to March 2021 to fund gigabit-capable deployment to the remaining 20 per cent of the UK (representing up to 6 million households).[95]

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. The revised Directive entered into force on 19 December 2018[96] and Member States and the UK (during the UK/EU transitional period) were due to implement the revisions to the AVMSD into national law by 19 September 2020, although a number of Member States and the UK missed the deadline. In the UK, the Audiovisual Media Services Regulations 2020 (UK AVMS Regulations) were made on 30 September 2020 and amend the existing UK Broadcasting Acts and the Act.[97] Most of the regulations come into force on 1 November 2020, with the remainder to come into force on 6 April 2021.

The revisions to the AVMSD (which are largely reflected in the new UK regulations) 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

92 Available at https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2019/supercharging-investment-in-fibre-broadband.

93 Available at https://deframedia.blog.gov.uk/2019/05/20/200-million-rollout-of-full-fibre-broadband-begins-and-the-guardian-on-ea-eel-research/.

94 See https://www.gov.uk/government/news/gigabit-broadband-rollout-milestone-reached.

95 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/909949/RGC_Key_Information_Document_August_2020_.pdf.

96 Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808&from=EN.

97 Available at https://www.legislation.gov.uk/uksi/2020/1062/contents/made.

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 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.[98]

In July 2020, the Commission published non-binding guidelines on (1) video-sharing platforms (VSPs); and (2) European works.[99] The guidelines intend to help Member States and the UK implement the AVMSD revisions, and offer a practical toolkit to ensure the promotion of European works and to help Member States and the UK assess which online services would fall under the scope of the AVMSD. The guidelines encourage cooperation between the national authorities, especially to gather relevant data, and to limit the risks of divergent interpretations of the tests referred to in the AVMSD. Such cooperation is to be facilitated through the European Regulators Group for Audiovisual Media Services (ERGA) and national authorities should keep ERGA informed in the areas covered by the guidelines. The UK was an active member of ERGA prior to leaving the EU, and Ofcom has said that it will continue to cooperate with ERGA as appropriate under the terms of the Brexit withdrawal agreement and to collaborate with European counterparts to exchange best practices for dealing with common challenges.[100]

Also in July 2020, Ofcom published a 'call for evidence' in relation to the UK's regulation of VSPs and to gather information on the practical and proportionate application of the measures included in the AVMSD.[101] The 'call for evidence' closed on 24 September 2020.

The UK AVMS Regulations define VSPs in accordance with the AVMSD criteria, defining a VSP as a service or dissociable section of a service which meets certain criteria and where the provision of videos to members of the public is (1) the principal purpose of the service; or (2) an essential functionality of the service.

Ofcom is appointed as the regulator for VSPs although Ofcom is given the power to designate another body as regulator should it choose to do so and subject to certain conditions. Pursuant to the UK AVMS Regulations, VSP providers are to notify Ofcom to confirm that they provide a VSP service and Ofcom must maintain a list of VSPs that it regulates and document its reasons for determining jurisdiction. Failure of a VSP provider to notify Ofcom may result in Ofcom imposing a financial penalty on such VSP provider. Ofcom may also require VSP providers to pay a regulatory fee provided that the amount of any such fee (1) represents the appropriate contribution of the VSP provider towards meeting Ofcom's costs as regulator each financial year; and (2) is justifiable and proportionate in respect of each VSP provider.

98 For more information see https://www.lw.com/thoughtLeadership/lw-how-the-updated-ams-directive-will-impact-european-media-services.

99 Available at https://ec.europa.eu/digital-single-market/en/news/commission-releases-guidelines-video-sharing-platforms-and-guidelines-european-works; VSP guidelines – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2020.223.01.0003.01.ENG&toc=OJ:C:2020:223:TOC; European works guidelines – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2020.223.01.0010.01.ENG&toc=OJ:C:2020:223:TOC.

100 Ofcom, Content (international work), https://ofcom.org.uk/about-ofcom/international/content.

101 Available at Ofcom, call for evidence, video-sharing platform regulation, https://www.ofcom.org.uk/consultations-and-statements/category-1/video-sharing-platform-regulation.

Regarding enforcement, the UK AVMS Regulations grant Ofcom a range of formal enforcement powers (broadly, issuing binding enforcement notifications and/or imposing financial penalties). Any enforcement notification must specify a reasonable period during which the VSP provider is required to take the action specified and include reasons for the decision. A financial penalty may be an amount up to five per cent of the offending VSP provider's applicable qualifying revenue or £250,000 (whichever is greater), as Ofcom determines to be appropriate and proportionate.

It is anticipated that Ofcom will also issue its own guidance to (1) help service providers understand whether they meet the definition of VSP and fall under UK jurisdiction; and (2) on the applications of the protective measures as set out by the AVMSD.

With regards to European works, the AVMSD establishes that providers of on-demand audiovisual media services must secure at least a 30 per cent share of European works in their catalogues and ensure prominence of those works. The definition of European works under the AVMSD includes works of countries that are part of the Council of Europe's Convention on Transfrontier Television (ECTT), of which the UK, along with 20 other EU countries, is a member. Therefore, UK-originated works continue to be classified as European works after Brexit. The AVMSD takes precedence among EU Member States, but the UK's position as a party to the ECTT will not be affected by its exit from the EU.

The Commission and the UK government have each published guidance notes on the AVMSD amendments and on the implications of Brexit on the audiovisual media sector.[102] On 1 January 2021, the AVMSD, including the country of origin principle,[103] will cease to benefit services under UK jurisdiction made available in the EU, and the UK will be treated as a third country. However, 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). From 1 January 2021, it would be possible for a media service provider to keep a 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. Furthermore, the ECTT framework will still apply, which provides for freedom of reception and retransmission.[104] This means that, broadly, the EU countries that have signed up to the ECTT must allow freedom of reception to services under UK jurisdiction. The same applies to reception in the UK of services originating from countries that are party to the ECTT. For the seven non-ECTT countries, additional licences and consents will be required, subject to local law requirements. Further, VOD services are outside of the scope of the ECTT 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.

102 The Commission's note is available at https://ec.europa.eu/digital-single-market/en/news/notice-stakeholders-withdrawal-united-kingdom-and-eu-rules-field-audiovisual-media-services; and the UK government's note is available at https://www.gov.uk/government/publications/broadcasting-and-video-on-demand-if-theres-no-brexit-deal/broadcasting-and-video-on-demand-if-theres-no-brexit-deal.

103 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)).

104 Article 4 of Council of ECTT.

Portability Regulation

On 9 December 2015, the Commission proposed a regulation to enable the cross-border portability of online content services.[105] The resulting Portability Regulation was published in the Official Journal on 30 June 2017[106] and came into force on 1 April 2018.[107] 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.

However, the Portability Regulation will cease to apply to UK–EEA travel from 1 January 2021. 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.

From 1 January 2021, content service providers will therefore 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.[108]

Copyright reform

Satellite and Cable Directive

On 14 September 2016, 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); a directive on copyright in 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 new Satellite and Cable Directive[109] entered into force on 7 June 2019, with Member States having two years (until 7 June 2021) to transpose the Directive into national law.

105 Available at https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-627-EN-F1-1.PDF.

106 Available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1128&from=EN.

107 See Corrigendum available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1128R(01)&from=EN.

108 Available at https://www.gov.uk/guidance/cross-border-portability-of-online-content-services-after-the-transition-period.

109 Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2019.130.01.0082.01.ENG.

The Commission's initial proposal was aimed at introducing a cross-border clearance mechanism for digital broadcasting and broadening retransmission rights. This was to be achieved through a combination of extending the country of origin principle[110] to cover online services and amending the collective approach to the exercise of cable retransmission rights, so that they applied to other similar means of retransmission (but excluding transmission via the open internet) as well as cable retransmission.

After a full legislative process, the new Satellite and Cable Directive did indeed extend 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'). 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's clearance regime applies only in respect of (1) radio programmes; and (2) broadcasters' TV programmes that are news and current affairs programmes, or broadcasters' own fully financed productions – it does not for example extend to coverage of sports events or programming acquired or commissioned from third parties.

The new 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, IPTV and internet), provided that where such retransmission takes place over an internet access service, it is carried out in a managed environment (i.e., in which the operator of the service provides a secure retransmission to authorised users). Furthermore, Member States can apply the principle in instances where both the broadcast and the retransmission take place in the same Member State. This means that instead of negotiating individually with every rights holder, operators of retransmission services benefit from collective management of rights and so are able to obtain licences from collective management organisations.

Further, the new Satellite and Cable Directive clarifies the principle of 'direct injection' by confirming that when a broadcaster transmits programmes to a distributor or platform (without the broadcaster itself simultaneously transmitting the programmes to the public), and the distributor or platform then transmits those programme-carrying signals to the public, the broadcaster and distributor or platform 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.

From 1 January 2021, the extent to which UK-based media companies can rely upon the provisions of the Satellite and Cable Directive (whether in the context of existing satellite and cable services' use of country of origin and cable retransmission rights, or in the new online or digital extensions) in respect of broadcasts into the EEA will depend on the nature and terms of the arrangements agreed between the UK and the EU and on how the domestic legislation of each EEA Member State treats broadcasts originating in non-EEA countries. Following the transition period, and as noted in UK government guidance, absent additional agreement these provisions may no longer apply and as such UK-based media companies may need additional rights holders' permissions to access the EU market.[111] In its guidance,

110 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.

111 Guidance available at https://www.gov.uk/guidance/copyright-clearance-for-satellite-broadcasting-after-the-transition-period.

the UK government indicates that in the UK, the country of origin principle will continue to be applied to broadcasts from any country, except where the broadcast is commissioned or uplinked to a satellite in the UK and it originates from a country that provides lower levels of copyright protection. The government guidance also states that UK law will continue to apply existing rules to cable retransmissions of broadcasts originating in an EEA Member State.[112]

Copyright Directive

The Copyright Directive came into force on 7 June 2019 and Member States have until 7 June 2021 to transpose the Directive into national law.

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 collective management organisation (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);

112 Guidance available at https://www.gov.uk/guidance/changes-to-copyright-law-after-the-transition-period.

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).

On 21 January 2020, the UK government confirmed that the UK will not be required to implement the Directive and that it has no plans to do so. Furthermore, the UK government confirmed that any future changes to the UK copyright framework will be considered as part of the usual domestic policy process. Following the EU-wide implementation of the Copyright Directive by 7 June 2021, there may be a significant rift between the EU regime and the UK national regime (e.g., given the implications of Article 17 and its interplay with the existing safe harbour regime as implemented into national UK law), creating a potentially challenging regulatory environment. Companies with an EU and UK presence, such as UK-headquartered companies with operations in the EU or global companies with operations in both the EU and UK, could experience a significant impact.

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,[113] and Member States had to implement the directive by 11 October 2018.[114] 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 from 1 January 2021. 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 following Brexit, the cross-border exchange of accessible format copies with the UK may be restricted. The latest government guidance at the time of writing indicates that the government is on track to ratify the Treaty into national legislation by 1 January 2021.[115]

113 Available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1563&from=EN.

114 Available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017L1564&from=EN.

115 Available at https://www.gov.uk/guidance/access-to-copyright-works-for-visually-impaired-people-after-the-transition-period.

Changes to copyright law from 1 January 2021

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), a government guidance note published on 30 January 2020[116] identifies changes to copyright law that will come into effect following the end of the transition period for the UK's exit from the EU. The guidance sets out how UK copyright law will change, subject to any changes under the future UK–EU relationship, and introduces the Intellectual Property (Copyright and Related Rights) (Amendment) (EU Exit) Regulations 2019 (the IP Exit Regulations) under the powers of the European Union (Withdrawal) Act 2018, due to come into force on 1 January 2021. The IP Exit Regulations remove or correct references to the EU, EEA or Member States in existing UK copyright legislation to preserve the effect of UK law where possible. Reciprocal cross-border arrangements will be amended or brought to an end, as appropriate. The government guidance note does state that, depending on the outcome of any further negotiations between the UK and the EU, the IP Exit Regulations may be amended. The guidance reiterates that most UK copyright works (such as books, films and music) will still be protected in the EU because of the UK's participation in the international treaties on copyright. For the same reason, EU copyright works will continue to be protected in the UK. This applies to works made before and after 1 January 2021. However, note the following changes to copyright law which are relevant to the media sector and in respect of which the government has published guidance:

a Sui generis database rights.[117] 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 for databases created on or after 1 January 2021. UK owners of databases created on or after 1 January 2021 will need to consider whether they can rely on alternative means of protection in the EEA – for example licensing arrangements or copyright protection. The government's guidance states that UK legislation will be amended so that only UK citizens, residents and businesses are eligible for database rights in the UK for databases created on or after 1 January 2021. The government's guidance further states that pre-existing sui generis database rights (whether held by UK or EEA persons) will continue to exist for the remainder of their duration.

b Collective rights management.[118] EU CMOs are required by the EU Collective Rights Management (CRM) Directive to represent, on request, rights holders of any EEA Member State. UK government guidance confirms that from 1 January 2021, 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 musical rights. UK rights holders and CMOs will still be able to request representation, but EEA CMOs may refuse those requests depending on the national law of Member States. The guidance

116 Available at https://www.gov.uk/guidance/changes-to-copyright-law-after-the-transition-period.

117 UK government guidance available at https://www.gov.uk/guidance/sui-generis-database-rights-after-the-transition-period.

118 UK government guidance available at https://www.gov.uk/guidance/collective-rights-management-after-the-transition-period.

further states that in the UK, existing obligations on UK CMOs will be maintained following 1 January 2021 (including those specific to multiterritorial licensing of musical works for online services).

c Orphan works.[119] 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. According to the government's guidance, UK CHIs will not be able to make use of the orphan works exception from 1 January 2021 and UK CHIs may face claims of copyright infringement if they make orphan works available online in the UK or EEA, including works they had made available online before 1 January 2021. As such, UK CHIs will need to remove any orphan works currently made available under the exception, or consider seeking a licence under the UK's orphan works licensing scheme.

iii OTT delivery of content and broadcast TV

Over-the-top internet delivery (OTT) is utilised by a range of content providers in the UK, including public service broadcasters (PSBs) (i.e., BBC iPlayer, ITV Hub, All4 and My5), cable and satellite platforms (e.g., both Virgin Media and Sky offer VOD products) 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). Disney+ launched in the UK in March 2020 and quickly became the third-most-subscribed-to SVoD service (behind Netflix and Amazon Prime Video) according to Ofcom data.

The industry is transforming as the take-up of superfast broadband and connected televisions changes the way in which people watch audiovisual content. People's total television and audiovisual viewing in 2019 was four hours and 52 minutes per day, a figure which remains similar to the levels of total viewing in 2018. Of this, live TV made up 53 per cent (a decrease of 3 per cent since 2018), while the remaining 47 per cent was composed of viewing non-broadcast content such as content available via standalone VOD platforms and YouTube. 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 98 per cent of UK homes having a working TV set in 2020.

Additionally, the covid-19 pandemic has changed consumer viewing behaviour significantly with people spending more time at home viewing content. According to Ofcom, 2020 has seen an accelerated growth in the viewing of online video, particularly OTT subscription services, with people in the UK watching an average 37 minutes per day more than in 2019. Even as lockdown measures eased, people's total viewing time in the UK was on average 11 per cent higher than in the same week in 2019. People's total television viewing in April 2020 (at the peak of lockdown restrictions), was an average per day (across all devices) of 6 hours 25 minutes – a significant increase on the 2019 figures.

119 UK government guidance available at https://www.gov.uk/guidance/orphan-works-and-cultural-heritage-institutions-copyright-after-the-transition-period.

The change in viewing habits is also in part driven by younger viewers, who watch more non-broadcast than broadcast content. SVoD viewing is far more pronounced in this age group, with large content libraries supporting heavy usage. The daily average for 2019 is split into three main parts: live TV (55 minutes - 21 per cent); YouTube (76 minutes – 30 per cent); and SVoD (59 minutes – 23 per cent). Viewing of SVoD by adults aged 16–34 has increased by a total of 12 minutes per day, continuing similar growth trends of previous years.

The continued growth of online video has ensured that total commercial revenue, encompassing TV and online, remained flat compared to 2019. Before the outbreak of covid-19, traditional commercial TV revenues were continuing the downward trend of previous years, with both digital multichannel and commercial PSBs seeing a decline in total revenue in 2019. Revenue from pay-TV subscription services remained flat comparatively to 2018 levels.

The covid-19 pandemic has also reinforced the importance of PSBs as trusted providers of news information, helping PSBs to achieve their highest combined monthly viewing share in more than six years in March 2020 when they captured 58 per cent of broadcast viewing. The BBC, ITV and Channel 4 were each rated as trusted sources of news and information by more than eight in ten people at the start of lockdown, with the BBC services in particular being the most-used source of news and information about covid-19. During the first week of lockdown in the UK, 82 per cent of people said that they used BBC services for covid-19 related information, well ahead of other broadcasters, social media channels and other sources.[120]

iv PSBs

As part of its responsibility as regulator, in February 2020 Ofcom published a review of how public service broadcasting has delivered for UK audiences over a five-year period to 2018. The review found that audiences continue to highly value the purposes of public service broadcasting, including trustworthy news and programmes that show different aspects of UK life and culture. The review establishes that the PSBs have generally fulfilled the public service broadcasting remit pursuant to the Act. Investment by the PSBs has also played an important role in supporting the UK's creative economy, including an increasingly vibrant production sector across the nations and regions. However, Ofcom wrote that maintaining the current level and range of programmes is a challenge for the PSBs, particularly when, at the same time, other providers such as Sky and Netflix are offering both a large volume and wide range of high-quality content to UK audiences.[121]

In July 2020, Ofcom published a report discussing people's relationship with public service broadcasting, with a particular focus on the views of young people. The report finds that, in exploring media habits and attitudes, it is apparent that consumption behaviours differ across the generations as does the use and relevance of the PSBs. Younger audiences tend to feel they are using streaming services more than public service channels, with some claiming to use public services rarely. However, analysis of media diaries suggested that the amount of public service broadcasting content being consumed can often be significantly underestimated, in part due to young people often watching 'hero' content (referring to

120 All data from: (a) Media Nations 2020: UK report available at https://www.ofcom.org.uk/__data/assets/pdf_file/0010/200503/media-nations-2020-uk-report.pdf; and (b) Media Nations 2020: Interactive report available at https://www.ofcom.org.uk/research-and-data/tv-radio-and-on-demand/media-nations-reports/media-nations-2020/interactive-report.

121 Available at https://www.smallscreenbigdebate.co.uk/what-is-ssbd/ssbd-five-year-review.

programming that is particularly noteworthy and talked about, for example, at the time of publication of the report, programmes such as Peaky Blinders and 13 Reasons Why). Importantly, while younger generations may only recall watching one or two public service shows at any given time, they do acknowledge that these shows are often highly valued. The report also found that the PSBs' master brands (i.e., BBC, ITV and C4) seem to have distinct identities across all age groups and all can describe their characteristics relative to one another.

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 the public service channels and content via the PSBs' VOD services. Ofcom published its first such report on 27 July 2018.[122] The DEA also required Ofcom to review the EPG Code prior to 1 December 2020. Pursuant to this, on 14 August 2020, Ofcom published a consultation on its review of competition rules in the EPG Code. The closing date for responses was 25 September 2020.

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 the PSBs' VOD services. While public service VOD and catch-up services are currently generally well-positioned, this is due to commercial negotiation rather than regulation. Ofcom is implementing changes to the existing linear EPG Code,[123] which 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[124] include:

a 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);

b BBC Four being guaranteed a slot within the first 24 slots of any licensed EPG;

c BBC News, BBC Parliament, CBBC and CBeebies being guaranteed slots within the first eight slots of the relevant EPG genre or section; and

d local TV services being located in the first 24 slots on digital terrestrial television of any EPG.[125]

Ofcom's recommendations to the government for a new framework to keep public service TV prominent in an online world analysed options for the future regulation of prominence in the context of VOD services (including the position of the PSBs' VOD players and the availability of their 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 public service content to secure the health of the public service broadcasting system and, accordingly (following consultation), has set out the following recommendations:

a new legislation is needed to keep PSBs prominent and support the sustainability of the PSBs;

122 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0026/116288/report-psb-local-tv-discoverability.pdf.

123 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0031/19399/epgcode.pdf.

124 Amended EPG Code available at https://www.ofcom.org.uk/__data/assets/pdf_file/0025/154384/annex-5-epg-code-appropriate-prominence-provisions.pdf.

125 Ofcom Statement of Changes to EPG Code available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/154459/statement-on-changes-to-the-epg-code.pdf.

b these new rules should specify which PSB content is given prominence, and on which platforms;
c the initial focus should be on connected TVs;
d viewers should be able to find PSB content easily on the homepage of connected TVs;
e on-demand services should only be given prominence if the service is clearly delivering PSB content;
f PSB content should also be given protected prominence within TV platforms' recommendations and search results;
g the new framework should protect the prominence of PSB content that is made available without charge; and
h there may need to be new obligations to ensure the continued availability of PSB on-demand content to viewers.[126]

v Impact of covid-19

The media sector has been significantly impacted by the covid-19 pandemic. Production arrangements have been severely disrupted. Sports and other live entertainment ground to halt for a period and, while at the time of writing UK sports have generally resumed, they are largely being played behind closed doors. Cinemas were also closed, with many releases delayed. On the flip side, covid-19 is seemingly resulting in some positives for the VOD industry. Lockdown prompted a surge in TV viewing in the UK that amplified the shift from broadcast to on-demand. During April 2020's full lockdown, viewing time per person per day averaged an estimated six hours 25 minutes, an increase of approximately an hour and a half on the average figure for 2019. Of this, approximately 40 minutes was attributed to SVoD services and viewing of YouTube increased by an average of nine minutes per person per day. SVoD subscriptions also grew.[127]

At the time of writing, we have seen some production resume. Industry guidelines have been published concerning covid-19-safe procedures.[128] The government has announced a new UK-wide £500 million Film and TV Production Restart Scheme. The Scheme has been instigated with the aim of helping productions that are halted or delayed by an inability to obtain insurance to cover covid-19 related risks.[129]

Additionally, the government has provided a Culture Recovery Fund to help Britain's culture, arts and heritage organisations including cinemas, impacted by the pandemic. General cross-sector aid measures that may assist businesses in the media sector are also available.

126 Ofcom Recommendations available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/154461/recommendations-for-new-legislative-framework-for-psb-prominence.pdf.

127 Media Nations 2020: UK report available at https://www.ofcom.org.uk/__data/assets/pdf_file/0010/200503/media-nations-2020-uk-report.pdf.

128 Available at: http://britishfilmcommission.org.uk/guidance/regarding-covid-19-coronavirus/; and https://www.pact.co.uk/covid-19/production-guidance.html.

129 Draft Scheme Rules: https://www.gov.uk/government/publications/film-tv-production-restart-scheme/film-tv-production-restart-scheme-draft-rules; Explanatory Notes: https://www.gov.uk/government/publications/film-tv-production-restart-scheme/film-tv-production-restart-scheme-draft-explanatory-notes.

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. The UK left the EU on 31 January 2020 (exit day), and entered a transition period that ends on 31 December 2020.

The UK's legal framework giving effect to Brexit during, and following, the transition period is governed by the European Union (Withdrawal) Act 2018 (Withdrawal Act), as amended by the European Union (Withdrawal Agreement) Act 2020. This framework provides that:

a the European Communities Act (ECA) 1972 was repealed on exit day;

b all existing EU legislation (including EU-derived legislation, such as national implementing legislation) was enshrined into British law on exit day;

c the jurisdiction of the CJEU over the UK continues during the transition period, and shall end on 31 December 2020 (subject to certain exceptions in which jurisdiction continues); and

d 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.

Following the end of the transition period on 31 December 2020, the following key events will occur:

a The Withdrawal Act savings for the ECA 1972 and any EU-derived domestic legislation are repealed;

b Material Withdrawal Act provisions take effect (mostly automatically);

c 'Retained EU law' is created by the Withdrawal Act, which effectively captures the EU law that applied to the UK at the end of the transition period (and which will be amended by UK legislation as appropriate in order to operate effectively within the UK legal regime); and

d The majority of Brexit-related regulations and statutory instruments will come into force, in order to give effect to the complex framework of post-EU UK legislation (for example, to implement required UK standards and policies in previously EU-governed areas, and to amend retained EU law to operate in a UK context).

The full picture of the future UK–EU relationship is still developing as negotiations continue, which will go beyond the end of the transition period.

ii Towards regulated digital services?

On 1 July 2020, the CMA published its final report concluding the market study into online platforms and digital advertising. The CMA's key recommendations focused on search advertising and display advertising and aligned with the recommendations set out in the Furman Report published in 2019. The CMA recommended to the UK government that it introduce a new regulatory regime to monitor large platforms. The CMA's report recommended that this new regulatory regime should include:

a Provision for a Digital Markets Unit (DMU): a body authorised to implement the new regulation, which could be a new or an existing institution, or several bodies sharing relevant functions.
b An enforceable code of conduct to govern the behaviour of platforms that are designated as having SMS. The code would aim to ensure: (1) fair trading, (2) open choices, and (3) trust and transparency.
c A requirement for a DMU to designate businesses that have SMS, maintain the code of conduct, and produce detailed guidance.
d Authorising the DMU to enforce the principles of the code on a timely basis, and amend the code's principles in line with evolving market conditions.
e Authorising the DMU to intervene so that platforms give appropriate data access, offer sufficient consumer choice, and implement ownership separation and operational separation.

With the publication of the final report, the CMA has now launched the Digital Markets Taskforce to advise the government on how to design a new *ex ante* regulatory regime. To inform this work, the CMA published a new call for information and is writing to relevant businesses to seek their views and information. The scope of the Taskforce encompasses all online platforms, including those that are not funded by digital advertising. The Taskforce intends to deliver advice to the UK government by the end of 2020. The CMA will lead the Digital Markets Taskforce and also work with Ofcom and the ICO to examine the impact of privacy regulation, with the three bodies establishing a new Digital Regulation Cooperation Forum to support broader UK regulatory coordination in online services.

Competition authorities and several governments in other jurisdictions are also considering further regulation in digital markets. For example:

a the European Commission is currently consulting on a proposal to develop a new competition tool to address structural competition problems, as well as a Digital Services Act, including an *ex ante* regulatory instrument for online platforms;
b the US Department of Justice announced in July 2019 that it is reviewing the practices of a number of platforms that may create or maintain structural impediments to greater competition;[130]
c the ACCC is currently conducting an inquiry in Australia into adtech and ad agencies, which builds on the ACCC's previous work examining digital advertising markets more generally in a digital platforms inquiry; and
d the BKartA is currently conducting a sector inquiry in Germany into market conditions in the online advertising sector.

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 was a milestone in the area of data protection law, and the developments introduced in the drafts of the ePrivacy Regulation could have significant implications (though the text if not yet finalised and timings for implementation remain unclear).

130 https://www.justice.gov/opa/pr/justice-department-reviewing-practices-market-leading-online-platforms.

The invalidation of the EU–US Privacy Shield in July 2020 in the *Schrems II* litigation, and the caveats imposed on the use of the standard contractual clauses as an alternative mechanism for the transfer of personal data to the US (and other countries outside the EU and UK), was a further controversial development. It remains to be seen what the long-term implications of this decision will be.

With regard to the media and entertainment industry in the UK, the rise in popularity of SVoD services has seen further OTT services launched in the UK in the past year, including Apple TV+ and Disney+ which has quickly established itself as the third-most-subscribed-to SVoD service. The proliferation of OTT services and their need for high-quality content to drive subscriber numbers continue to reshape the industry. From a regulatory perspective, we have seen further platform regulation which impacts on internet-delivered content services whether standalone OTT platforms or social media. We have outlined above the key legislative changes effective 1 January 2021 in the media and entertainment sector – we now have greater clarity over the changes and industry is preparing for this date. However, we have seen huge disruption caused by the covid-19 pandemic. Production arrangements have been severely disrupted. Sports and other live entertainment ground to halt for a period and cinemas were closed, with many releases delayed. On the flip side, lockdown prompted a surge in TV viewing in the UK that amplified the shift from broadcast to on-demand. The government has made available certain industry-specific support, as well as general cross-sector aid measures that may assist businesses in the media sector. It remains to be seen how the media and entertainment sector will be impacted by the pandemic on a longer-term basis.

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 in the run-up to, and following, the end of the transition period on 31 December 2020.

Appendix 1

ABOUT THE AUTHORS

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.

LISBETH SAVILL

Latham & Watkins LLP

Lisbeth (Libby) Savill is a partner in the London office of Latham & Watkins and co-chair of the firm's entertainment, sports and media industry group.

Ms Savill has been recognised as a leading lawyer in the film and television industries for many years, and brings a wealth of experience and knowledge to her practice to help clients

navigate the ever-changing landscape in this area. She represents a wide range of entities across the media and entertainment sectors including film and television producers and distributors (including major studios), broadcasters, platforms and digital-first companies, and financiers (debt and equity) and investment funds. Her work includes the creation and financing of audiovisual content, distribution, licensing and other exploitation arrangements of audiovisual and live content, funds and co-financing arrangements and commercial advice on strategic joint ventures and the purchase, sale and financing of entertainment and media companies.

LATHAM & WATKINS LLP

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
www.lw.com

Chapter 20

UNITED STATES

Matthew T Murchison, Elizabeth R Park and Michael H Herman[1]

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 Matthew T Murchison is a partner, Elizabeth R Park is counsel 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 or other applications or petitions for authority that would result in legally cognisable non-US ownership of FCC-regulated businesses. Notably, on 4 April 2020, the President signed an executive order establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Sector (the Committee), a group of agencies composed of the DOJ and the US Departments of Defence and Homeland Security, and advised by various other government agencies and departments, formalising the informal group previously referred to as Team Telecom. Applications and petitions filed with the FCC involving foreign ownership that are referred to the Committee typically are subject to additional information requests in connection with the Committee's review, and because the FCC typically will not grant such applications until the Committee has 'signed off', the Committee effectively has the power to delay, if not block, a transaction or

the grant of authority 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 requires 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 certain types of 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.

iv 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 indirect 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 and applications that are consistent with the foreign ownership limits described above may be scrutinised, and effectively blocked, as a result of a review by the Committee (i.e., the successor to Team Telecom) or CFIUS (as described above). Beginning in 2019, the FCC, in consultation with the executive branch agencies that now constitute the Committee, has denied an application for authority to provide international telecommunications services (which are not subject to foreign ownership restrictions in Section 310 of the Communications Act) and has commenced reviews of previous grants of such authority based on national security and law enforcement concerns. Specifically, the FCC denied a long-pending application by China Mobile USA for authority to provide international telecommunications services in the US, finding that its ownership and control by the Chinese government raised substantial national security and law enforcement risks that could not be resolved through mitigation measures. Following on that action, the FCC commenced reviews of previously granted authority issued to China Telecom Americas, China Unicom Americas, Pacific Networks, and ComNet – each of which is ultimately

subject to the ownership and control of the Chinese government – at the recommendation of the executive branch agencies to revoke these authorisations based on similar national security concerns.

Further, over the course of 2019 and 2020, the federal government imposed various restrictions on Chinese communications technology companies – most notably Huawei and ZTE – that it has determined pose national security threats to the United States. For instance, since May 2019, the DOC has effectively prohibited American companies from transacting with Huawei, ZTE, and other Chinese firms that could provide the Chinese government the means to intercept or disrupt the communications of American citizens and the US government. Moreover, in June 2020, the FCC formally designated Huawei and ZTE as national security threats, forbidding federal universal service support from being used to purchase equipment or services from either company.

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, after the United States Court of Appeals for the Third Circuit found that the FCC had failed to consider the consequences of such deregulation on diversity in media ownership, the FCC reinstated the cross-ownership restrictions in December 2019. In doing so, the FCC made clear that it was simply complying with the Third Circuit's ruling and expressly reserved its right to seek review of the appeals court's decision by the US Supreme Court, which it did in April 2020.

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 non-substantive 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.

The past year has seen relatively few major telecommunications and media transactions. Notably, however, T-Mobile US, Inc (the nation's third-largest wireless carrier) and Sprint Corp (the nation's fourth-largest wireless carrier) closed their merger in April 2020. Although the transaction already had been approved by the DOJ (in July 2019) and by the FCC in (October 2019), attorneys general of a number of states and the District of Columbia nevertheless challenged the transaction in the United States District Court for the Southern District of New York. Following a trial that spanned several weeks in December 2019 and January 2020, the court ruled against the states, paving the way for the companies to consummate the transaction, which had been pending since April 2018. Pursuant to a condition of the DOJ's approval of the merger, in July 2020, DISH Network Corp acquired Boost Mobile (Sprint's prepaid service business unit) in order to facilitate the direct-broadcast satellite (DBS) provider's entry into the wireless market. In August 2020, the Sprint brand was discontinued, and 'new' T-Mobile currently is in the process of integrating the operations of the two carriers.

Although approved by the FCC in 2016, Charter Communications, Inc's acquisition of Time Warner Cable, Inc and Bright House Networks, LLC recently became the subject of renewed activity. In June 2020, Charter urged the FCC to terminate conditions imposed in connection with the transaction that prohibit the company from imposing data caps and usage-based pricing and require it to provide non-discriminatory, fee-free interconnection to certain entities. Then, two months later, the United States Court of Appeals for the District of Columbia Circuit vacated the interconnection condition noted above as part of a separate legal challenge to the FCC's approval of the transaction. While the court's decision effectively mooted Charter's petition insofar as it sought relief from the interconnection requirement,

the company's request that the FCC sunset the restriction on data caps and usage-based pricing is still pending, and Charter remains subject to certain other conditions, including broadband buildout commitments.

vi 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:

a that consumers are protected;
b the integrity of the universal service support mechanism is preserved;
c robust competition;
d responsible use of the public airwaves; and
e 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, failure to contribute to universal service funds, misuse of universal service support or other violations of universal service funding rules, 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).

The covid-19 pandemic – and Americans' attendant reliance on broadband connectivity for distance learning, remote work and telehealth – has reinvigorated ongoing efforts to ensure the availability of reliable and affordable internet access across the United States. In March 2020, the FCC introduced the Keep Americans Connected Pledge, pursuant to which more than 800 service providers agreed not to disconnect consumers and small business customers for non-payment and to waive such customers' late fees incurred, in each case due to the crisis. A number of states (including Delaware, Indiana and Maryland) went further, issuing executive orders or enacting emergency legislation mandating that service providers take such steps. Congress enacted the Coronavirus Aid, Relief and Economic Security (CARES) Act, which among other things provided funds to states to support connectivity for schools, teachers and students to facilitate distance learning, and allocated US$200 million for the

FCC to distribute to healthcare providers offering connected care services to their patients in response to the pandemic. Policymakers' focus on establishing and maintaining robust connectivity precipitated by the covid-19 pandemic likely will inform future policy debates concerning universal service and the appropriate regulatory treatment of broadband internet access service.

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 27 per cent of covered revenues for most of 2020. 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 adopted in 2010 recommended that the FCC modify universal service subsidy programmes, which historically focused on voice telecommunications, 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 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 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. In 2019, the FCC began disbursing funds to the reverse-auction's winning bidders, a process that has continued into 2020. 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 January 2020, the FCC established the new Rural Digital Opportunity Fund (RDOF) that it had proposed the previous year. Modelled after the CAF programme, the RDOF will provide US$20.4 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. At the time of writing, the first of two RDOF auctions, through which the FCC will provisionally award approximately US$16 billion in support to winning bidders, is scheduled for August 2020; the second RDOF

auction, through which the remainder of the fund will be distributed, will be held at a later date. 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. After the DC Circuit denied various petitions for rehearing in early 2020, the parties ultimately declined to seek review by the US Supreme Court, thereby solidifying broadband internet access service's 'information service' classification for the time being.

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. A challenge to this decision brought by a number of municipalities is currently before the United States Court of Appeals for the Sixth Circuit, which refused to stay the FCC's August 2019 order pending the outcome of the appeal.

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. Consistent with the DC Circuit's directive, the FCC solicited comments on these issues in February 2020.

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. Although the DC Circuit vacated the 2018 order's express pre-emption provision, it left room for such challenges to proceed based on conflict pre-emption principles. Because the court denied petitions for rehearing and the parties declined to seek review by the US

Supreme Court, the stays in these challenges to California's and Vermont's net neutrality regulations have been lifted; in California, the federal government and BIAPs have filed amended complaints and renewed motions for preliminary injunctions.

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 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, while updated and comprehensive privacy legislation has stalled at the federal level, certain states have pressed forward with privacy requirements of their own. For example, following on the enactment of the California Consumer Privacy Act in 2018 – which imposes far-reaching privacy obligations on a wide range of businesses doing business in California, including broadband service providers and internet platforms – the California attorney general's office issued regulations implementing the statute in June 2020.

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. Despite having opened a new proceeding to consider reforms to its implementation of the TCPA in light of the court's ruling in May 2018, the FCC has yet to provide clarity on these issues. Over the course of late 2019 and early 2020, two challenges to the TCPA reached the US Supreme Court. Although it rejected a First Amendment challenge to the statute in July 2020, the Court is expected to resolve a longstanding dispute concerning the proper interpretation of the term 'autodialler' by mid-2021.

In tandem with the FCC's efforts to clarify the scope of the TCPA, other regulatory and legislative steps have been taken 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, in December 2019, the US Congress passed the TRACED Act, which provides additional flexibility to service providers to block illegal and unwanted robocalls and imposes a June 2021 deadline for the implementation of SHAKEN/STIR, an end-to-end call authentication protocol aimed at curtailing unwanted 'spoofed' robocall traffic travelling on and among their networks. Pursuant to the TRACED

Act, in July 2020 the FCC established safe harbours (from liability for unintentional blocking of wanted calls) for service providers that employ certain 'reasonable analytics' to block robocalls and that decline to complete calls originated from upstream service providers deemed to be 'bad actors'. In addition, although many of the nation's largest carriers already have implemented SHAKEN/STIR, the FCC is actively working to ensure that all service providers deploy this technology as soon as possible.

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 5 and 6 GHz bands 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 through its 'spectrum frontiers' proceeding, made spectrum above 24GHz available for '5G' wireless mobile and other broadband services. Since the inception of this proceeding, the FCC made available over 6GHz of millimetre-wave spectrum for flexible wireless use, in the 24.25–24.45 and 24.75–25.25GHz bands (24GHz band), the 27.5–28.35GHz band (28GHz band), the 37–38.6GHz band (37GHz band), the 38.6–40GHz band (39GHz band), the 47.2–48.2GHz band (47GHz band), and the 50.4–51.4GHz band. The FCC also made available the 64–71GHz band for use by unlicensed devices. 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 28GHz band, which raised over US$700 million and resulted in the grant of new licences to dozens of winning bidders in October 2019. And in March 2020, the FCC completed an auction for spectrum in the upper 37, 39 and 47GHz bands, raising more than US$7.5 billion (including nearly US$4.5 billion for the government).

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 24GHz, 28GHz, 39GHz, and 47GHz bands, and authorised satellite use in the 50GHz band, to permit greater flexibility in the deployment of earth stations. The FCC also provided for expanded unlicensed use of the 57–71GHz band on-board aircraft.

Efforts also are underway to make more mid-band spectrum available for flexible wireless use, including 5G deployments. For instance, in July 2020, the FCC commenced an auction of licences in the 3.5GHz band. And following the DC Circuit's June 2020 rejection of a challenge brought by small satellite operators to the FCC's plan to repurpose the 3.7–4.2GHz band (which to date has been used primarily for satellite-based video distribution) for 5G, the FCC scheduled an auction of spectrum in the 3.7–3.98GHz portion of that band for December 2020. The FCC has a continuing inquiry into potential ways to facilitate more intensive use of the frequencies between 3.7GHz and 24GHz. The FCC also is exploring other underutilised spectrum to support 5G and other recent technologies, and this year commenced a proceeding to examine proposals to expand commercial use of the 71–76GHz, 81–86GHz, 92–94GHz and 94.1–95GHz bands.

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.

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 federal government and industry collaborate to improve space safety and mitigate orbital debris and 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. At the same time, the FCC continues to evaluate operators' proposals for non-geostationary orbit satellite deployments and, in March 2020, initiated a new processing round for such applications, and is considering proposals to establish rules for coexistence among these systems.

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.

Internet-based media platforms, including social media platforms, have long been shielded from liability by Section 230 of the Communications Act both for third-party (i.e., user-generated) content and for such platforms' good-faith exercise of editorial discretion to block or limit access to users' posts. In May 2020, however, the President issued an executive order articulating a narrow view of Section 230 immunity, and setting in motion a re-examination of the statute at the federal level, including at the FCC. Various groups have mounted legal challenges to the executive order.

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.

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.

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.

Although states and localities in their role as franchisors frequently impose requirements on CATV operators (including to extract 'in kind' benefits, as described above), their authority to regulate CATV is limited in many respects by the pre-emptive effect of the Communications Act and the FCC's rules. The proper scope of states' and localities' authority over CATV operations is the subject of an ongoing lawsuit brought by Comcast and various programmers against the governor and attorney general of Maine, whose state legislature passed a law requiring all CATV operators in the state to provide all channels, and all programmes on all channels, on an 'à la carte' basis. The industry plaintiffs, which have challenged the state law on First Amendment and pre-emption grounds, successfully

obtained a preliminary injunction in the United States District Court for the District of Maine. The state defendants appealed, and the United States Court of Appeals for the First Circuit heard arguments in the case in September 2020.

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 established a roadmap to free additional spectrum resources for such services, and the FCC brought these plans to fruition through the spectrum proceedings discussed above. The advent of these services, many of which would not use 'broadcast' spectrum, reflects increasing convergence in the communications industry, and has led to increased efforts 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 at the federal level, though a number of states have begun testing the water on broadband regulation. 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. Whether any new requirements enacted by Congress or adopted by the FCC turn out to be less stringent or more stringent than earlier regulatory efforts likely will depend in large part on the outcome of the upcoming presidential election.

Appendix 1

ABOUT THE AUTHORS

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*.

ELIZABETH R PARK

Latham & Watkins LLP

Elizabeth R Park is counsel in the Washington, DC office of Latham & Watkins LLP, where her practice focuses on representing communications, information technology and media companies in both transactional and regulatory matters. Ms Park's transactional experience includes securing federal and state regulatory consents in connection with mergers and acquisitions, structuring private equity investments and other financing transactions to meet regulatory requirements, and negotiating a variety of communications, technology and content agreements. She has also guided clients in transaction reviews by 'Team Telecom' and other executive branch agencies. In the regulatory arena, Ms Park assists clients in navigating regulatory policy issues and the procedures of the Federal Communications Commission (FCC) and other government agencies, and has represented clients in a wide range of adjudicatory and rulemaking proceedings before the FCC. Ms Park obtained her JD from George Washington University Law School and her BS from Tufts University.

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.

LATHAM & WATKINS LLP

555 Eleventh Street, NW
Suite 1000
Washington, DC 20004-1304
United States
Tel: +1 202 637 2200
Fax: +1 202 637 2201
matthew.murchison@lw.com
elizabeth.park@lw.com
michael.herman@lw.com
www.lw.com

an LBR business

ISBN 978-1-83862-508-5