THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

TWELFTH EDITION

Editor
Matthew T Murchison

THE LAWREVIEWS

© 2021 Law Business Research Ltd

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

TWELFTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2021
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Matthew T Murchison

THE LAWREVIEWS

© 2021 Law Business Research Ltd

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADERS
Joel Woods, Jack Bagnall

BUSINESS DEVELOPMENT MANAGERS
Rebecca Mogridge, Katie Hodgetts, Joey Kwok

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Georgia Goldberg

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Claire Ancell

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
© 2021 Law Business Research Ltd
www.TheLawReviews.co.uk

No photocopying: copyright licences do not apply.
The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at November 2021, be advised that this is a developing area.
Enquiries concerning reproduction should be sent to Law Business Research, at the address above.
Enquiries concerning editorial content should be directed
to the Publisher – clare.bolton@lbresearch.com

ISBN 978-1-83862-834-5

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

© 2021 Law Business Research Ltd

ACKNOWLEDGEMENTS

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

ANANTLAW

BAGUS ENRICO AND PARTNERS

BAKER MCKENZIE

CEDAR WHITE BRADLEY

CLEARY GOTTLIEB STEEN & HAMILTON LLP

CMS RUSSIA

ELVINGER HOSS PRUSSEN

LATHAM & WATKINS LLP

LEE AND LI, ATTORNEYS-AT-LAW

MLL MEYERLUSTENBERGER LACHENAL FRORIEP AG

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

SHAHID LAW FIRM

SORAINEN

THE LAW OFFICE OF SALMAN M AL-SUDAIRI

TRAPLE KONARSKI PODRECKI & PARTNERS

URÍA MENÉNDEZ

WEBB HENDERSON

ZHONG LUN LAW FIRM

© 2021 Law Business Research Ltd

CONTENTS

© 2021 Law Business Research Ltd

© 2021 Law Business Research Ltd

© 2021 Law Business Research Ltd

PREFACE

This volume marks the 12th edition of *The Technology, Media and Telecommunications Review*, which has been fully updated to provide an overview of evolving legal and policy activity in this arena across 25 jurisdictions around the world. This publication continues to occupy a unique space in the literature on TMT issues. Rather than serving a traditional legal treatise, this Review aims to provide a practical, business-focused survey of these issues, along with insights into how this legal and policy landscape in the TMT arena continues to evolve from year to year.

In 2021, the ongoing covid-19 pandemic has continued to loom large over legal and policy developments in this sector. As the threat of infection has continued to affect how we live, work and interact, the importance of connectivity has never been greater or more obvious. For many businesses, remote working has been the rule rather than the exception since March 2020, and may well persist in some form well after the pandemic is over. Many schools switched to distance learning formats during the pandemic. 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.

The experience of covid-19 has, in turn, continued to reshape policymakers' understanding of the TMT arena. The 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. 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 exploring mandates prohibiting disconnection of customers or requiring certain rates for low-income consumers – measures that, where adopted, sometimes have sparked fresh legal challenges and policy debates over the relative merits of government intervention and market-based solutions.

New technologies likewise have required new approaches and perspectives of policymakers. A notable example is the ongoing deployment of 5G wireless networks, as regulators continue to look for ways to facilitate such deployment. 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. Multiple jurisdictions have continued to auction off wireless licences in bands newly designated for 5G deployment, capitalising on service providers' strong demand for

© 2021 Law Business Research Ltd

expanded access for spectrum. The planned deployment of new satellite broadband services, including multiple large satellite constellations in low-earth orbit, also continues to be a focus of regulatory interest across the world.

Meanwhile, long-running policy battles over the delivery of content over broadband networks continue to simmer in various jurisdictions, and new fronts have opened on related issues involving the content moderation policies of social media companies and other online platforms. Policymakers continue to grapple with questions about network neutrality, the principle being 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. While the basic principle has been around for well over a decade, unresolved issues remain, including whether newer kinds of network management practices implicate such concerns, and whether efforts to promote a healthy internet ecosystem are best served by light-touch, market-based regimes or by more intrusive government interventions. In the United States, the light-touch approach reinstated in 2018 seems fairly certain to be revisited at the federal level, and certain states are continuing to claim an ability to impose their own restrictions on internet service providers. Regulators around the world have begun taking more aggressive enforcement action against 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. In addition, these neutrality principles, usually debated in the context of broadband networks, are now spilling over to the content side, where social media companies are facing increased scrutiny over claims of discriminatory practices in moderating content appearing on their platforms. Indeed, some jurisdictions are considering measures that not only would rescind immunities these platforms have traditionally enjoyed for their content moderation practices, but also would require increased transparency and potentially even impose anti-discrimination mandates or other consumer protections. In short, while the balance of power between broadband network operators and online content providers historically has turned on the degree of regulation of the former, both sides' practices are now very much in the spotlight.

The following country-specific chapters describe 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.

Thanks to all of our contributors for their insightful contributions to this publication. I hope readers will find this 12th edition of *The Technology, Media and Telecommunications Review* as helpful as I have found this publication each year.

Matthew T Murchison
Latham & Watkins LLP
Washington, DC
November 2021

© 2021 Law Business Research Ltd

Chapter 24

UNITED KINGDOM

Gail Crawford, David Little 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 2021–22 Annual Plan (published in March 2021).[2] They include improving broadband and mobile coverage by investing in strong and secure networks such as fibre networks across the UK, supporting UK broadcasting by maintaining a media environment that supports society, safeguarding the interests of telecoms consumers, including those who are vulnerable, sustaining the universal postal service during the covid-19 pandemic, and increasing diversity and inclusion.

The UK's data protection, e-privacy and cybersecurity frameworks impose wide-ranging compliance obligations on organisations in relation to their use and safeguarding of personal data and communications data. Following the end of the Brexit transition period on 31 December 2020, the UK regimes have broadly retained their EU foundations, though areas of divergence are starting to emerge.

II REGULATION

i The regulators and key legislation

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.

Furthermore, Ofcom has concurrent powers to apply competition law along with the primary UK competition law authority, the Competition and Markets Authority (CMA).

---

1 Gail Crawford, David Little and Lisbeth Savill are partners at Latham & Watkins LLP. The authors would like to acknowledge the kind assistance of their colleagues Alexandra Luchian, Stewart Robinson, Amy Smyth, and Francesca Forzoni in the preparation of this chapter.

2 Ofcom's Plan of Work 2021/22 available at https://www.ofcom.org.uk/__data/assets/pdf_file/0019/216640/statement-plan-of-work-202122.pdf

© 2021 Law Business Research Ltd

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.[3] Ofcom's main duties are set out in its 2021–22 Annual Plan.[4]

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;
d the UK GDPR and the DPA, which provide the UK's data protection framework;
e the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011);
f the NIS Regulation;
g the Freedom of Information Act 2000;
h the Investigatory Powers Act 2016;
i the Enterprise Act 2002;
j the Copyright, Designs and Patents Act 1988 (CDPA);
k the Digital Economy Act 2017 (DEA);
l the Competition Act 1998;
m the Consumer Rights Act 2015;
n the Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations 2020, implementing certain aspects of the European Electronic Communications Code Directive,[5] establishing the European Electronic Communications Code; and
o the European Union (Withdrawal) Act 2018.

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), which included a recommendation that the CMA conduct a market study into the digital advertising market.[6] On 1 July 2020, the CMA published its final report,[7] concluding that it would not be launching a market investigation, as a market investigation would risk cutting across broader regulatory reform and that launching a market investigation at the time would be inappropriate given the disruption caused by

3 Section 3(1) of the Act.

4 Ofcom's Plan of Work 2021/22 available at https://www.ofcom.org.uk/__data/assets/pdf_file/0019/216640/statement-plan-of-work-202122.pdf.

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

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

7 Available at https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.

© 2021 Law Business Research Ltd

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 then launched a Digital Markets Taskforce in conjunction with Ofcom and the ICO to advise the UK government on designing this regulatory regime. The Digital Markets Taskforce's advice was published in December 2020,[8] and it calls for:

a the establishment of a Digital Markets Unit (DMU): a body authorised to implement the new regulatory regime, whose primary duty would be 'to further the interests of consumers and citizens in digital markets by promoting competition and innovation';[9]

b a regulatory framework for digital firms designated as having strategic market status ("SMS"), including an enforceable code of conduct , as well as pro-competitive interventions, for example, in relation to data mobility, interoperability and data access. The code of conduct would aim to ensure: (1) fair trading; (2) open choices; and (3) trust and transparency. The SMS regime would be overseen by the DMU and complemented by SMS merger rules overseen by the CMA; and

c stronger consumer protection and competition laws that are better adapted to the digital age.

The DMU was launched in non-statutory form within the CMA in April 2021, and it will work alongside the CMA and the Digital Regulation Cooperation Forum (a body comprising the CMA, Ofcom, the ICO and the FCA, established to ensure greater cooperation on online regulatory matters).[10] In a press release dated 20 July 2021,[11] the government unveiled plans for a new pro-competition regime for digital markets following the Digital Markets Taskforce's advice. The plans include the following proposed powers for the DMU: designating tech firms having SMS; suspending, blocking and reversing decisions by firms designated as having SMS; and imposing fines of up to 10 per cent of turnover for serious breaches. These powers will require legislation. The government has committed to consulting on proposals for the new pro-competition regime in 2021 and legislating when parliamentary schedules allow it.

On 29 September 2021, responding to two government consultations, the CMA welcomed the government proposals to establish an SMS regime comprising codes of conduct, pro-competitive interventions and merger rules, empowering the DMU and enhancing the CMA's ability to tackle breaches of competition and consumer law.[12] The CMA also expressed support for the proposed levy funding model for the DMU and close collaboration and coordination between the DMU and other regulators such as the ICO, Ofcom and the FCA.

8 Available at https://assets.publishing.service.gov.uk/media/5fce7567e90e07562f98286c/Digital_Taskforce_-_Advice.pdf.

9 ibid.

10 See https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.

11 Available at https://www.gov.uk/government/news/government-unveils-proposals-to-increase-competition-in-uk-digital-economy.

12 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022636/CMA_response_to_Digital_Markets_consultation.pdf.

© 2021 Law Business Research Ltd

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. 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

The UK operates a merger control regime in which the parties to a transaction can choose whether to notify a transaction prior to closing. The administrative body currently responsible for UK merger control is the CMA. The 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.[13] The CMA consults Ofcom when considering transactions in the broadcast, telecommunications and newspaper publishing markets.[14]

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.[15] 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

13 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.

14 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.

15 This was confirmed by the Competition Appeal Tribunal in *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.

© 2021 Law Business Research Ltd

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.

In 2020, the UK government announced that it would implement a new extensive stand-alone regime to review transactions on grounds of national security through the National Security and Investment Act 2021 (the NSI Act).[16] The NSI Act received royal assent on 29 April 2021 and will come into force on 4 January 2022, albeit some of its provisions will extraordinarily apply retrospectively (between 12 November 2020 and the commencement of the regime).[17] The NSI Act introduces a hybrid mandatory and voluntary notification regime. This brings to the UK a regime similar to the one under the EU FDI Regulation. The Act imposes mandatory notification requirements and associated stand-still obligations to relevant acquisition in 17 sectors defined in the National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021.[18] The 17 sectors include advanced robotics, artificial intelligence, communications, cryptographic authentication, data infrastructure, quantum technologies and satellite and space technology. It will be unlawful to complete a notifiable transaction without the Secretary of State's prior approval, and failure to notify may render a transaction void and lead to both civil and criminal sanctions. No financial thresholds or *de minimis* exemptions are envisaged. A separate unit within BEIS, the Investment Security Unit, will be handling notifications.[19]

v DSM: online platforms and telecoms

Introduction

A key initiative of Europe's DSM Strategy is the Digital Services Act package. This was announced by the European Commission to strengthen the Single Market for digital services and foster innovation and competitiveness of the European online environment. It is based on two main pillars: framing the responsibilities of digital services and *ex ante* rules covering large online platforms acting as gatekeepers. In summer 2020, the Commission ran a 14-week public consultation to identify specific issues that may require EU-level intervention.[20] In, total 2,863 responses were submitted by a diverse group of stakeholders including public authorities, NGOs and business organisations, and around 300 position papers were received.[21] The consultation results were consolidated in a proposal for a regulation on a Single Market for Digital Services, which was adopted on 15 December 2020.[22] The proposal includes:

a transparency reporting obligations for online platforms and providers of intermediary services concerning content moderation;

16 See: https://www.lw.com/thoughtLeadership/uk-government-publishes-draft-legislation-for-a-new-foreign-direct-investment-regime.

17 Full text of the NSI Act available at: https://www.legislation.gov.uk/ukpga/2021/25/contents/enacted.

18 Full text of the legislation available at https://www.legislation.gov.uk/ukdsi/2021/9780348226935.

19 See: https://www.gov.uk/government/publications/national-security-and-investment-bill-2020-factsheets/overview-of-the-investment-security-unit-factsheet.

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

21 Summary report of the open consultation is available at https://digital-strategy.ec.europa.eu/en/summary-report-open-public-consultation-digital-services-act-package.

22 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0825&from=EN.

© 2021 Law Business Research Ltd

b transparency obligations in respect of online advertisements, including a requirement to display, in real time and in a clear and unambiguous manner, various pieces of information for each advertisement to each user;

c additional obligations on 'very large platforms' (i.e., those with an average number of active monthly users in the EU that is at least 45 million), including regarding assessment and mitigation of any significant systemic risks, independent audit and compliance officers; and

d proposed penalties for non-compliance of up to 6 per cent of the annual income or turnover, including the possibility of periodic penalty payments of up to 5 per cent of the average daily turnover in the preceding financial year.

Online platforms

The role of online platforms in the economy has continued to expand over 2020/21, accelerated by the covid-19 pandemic. Online platforms are facing increasing regulation in a number of areas, including in relation to online harms and in a business-to-business context. For the business-to-business online environment, the Commission adopted the Platform to Business Regulation in 2019 (in force from 20 June 2020).[23] The Regulation has been implement in the UK in the UK Platform to Business Regulations,[24] which include measures seeking to reduce unfair trading practices, increase transparency and resolve disputes more effectively.

The 'online harms' regime is the name given to a proposed UK regulatory framework governing content posted via online services. The UK government published its draft Online Safety Bill (the Bill)[25] on 12 May 2021; it is expected to put a final version of the Bill before parliament in late 2021 or early 2022. The proposed regulatory regime will apply to online user-to-user services (e.g., social media platforms, online marketplaces and online forums) and to internet search services, subject to certain widely drawn exemptions (including email or text messaging-only services, internal business services, services with limited user-to-user functionalities and content on news publishers' websites). The Bill imposes a range of statutory duties of care on regulated services providers, broadly to protect users from illegal content generated and shared by other users. In relation to harmful content, there are additional safeguarding obligations for services 'likely to be accessed' by children, and additional transparency and risk assessment requirements for services designated as 'Category 1' services (to be determined by Ofcom, based on threshold conditions to be set out in secondary regulation, referencing the number of users, the functionality of the service and the risk of harm from content). The proposed duty of care imposes requirements on providers both in terms of processes they must implement and their moderation of specific content. In addition to duties to safeguard against illegal and harmful content, regulated services providers are also under parallel duties to have regard to freedom of speech and privacy rights. Ofcom will regulate the regime, and is granted a range of sanction powers by the Bill, such as (1) fines of up to the greater of £18 million or 10 per cent of a providers' annual global revenue; and (2) court orders to disrupt or prevent access to the services of non-compliant providers. The proposed regime also establishes a super-complaints procedure, which will allow certain eligible entities (expected to include consumer rights organisations and similar) to make

23 Regulation on promoting fairness and transparency for business users of online intermediary services, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1150.

24 UK Online Intermediation Services for Business Users (Enforcement) Regulations 2020.

25 Available at https://www.gov.uk/government/publications/draft-online-safety-bill.

© 2021 Law Business Research Ltd

complaints to Ofcom. The Bill is intended to supersede relevant existing requirements under the UK AVMS Regulations for providers of video sharing platforms to take measures to protect the public from harmful material.

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

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

In December 2018, the Commission adopted the European Electronic Communications Code (the Code).

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 consumer protections via proposed regulations requiring telecoms providers to provide contract summaries and improved comparison tools. In the UK, the Code has been implemented through the Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations 2020, which will come into force in their entirety in December 2022. After confirming a set of rules designed to protect broadband, mobile, pay TV and landline customers in October 2020, Ofcom published a statement setting out the detailed approach to implementation of the European Electronic Communications Code Directive (EECC) in December 2020.[26] The new rules will be reflected into the General Conditions of Entitlement so that providers of electronic communications networks and services are obliged to comply with them if they wish to provide services in the UK. The new rules are coming into force on a staggered basis throughout December 2022 and are aimed at facilitating broadband switching, stopping mobile providers from selling 'locked' devices, enhancing contract information provision and exit rights for customers and ensuring that disabled customers have equivalent access to information about their communications services.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Universal service

Universal service is provided under the Act by way of the Universal Service Order.[27] Ofcom designated BT and KCOM as universal service providers in the geographical areas they cover. Consumers and businesses are now able to request connections since 20 March 2020.[28]

26 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0020/209504/eecc-statement-dec-20.pdf.

27 See https://www.ofcom.org.uk/consultations-and-statements/category-1/uso.

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

© 2021 Law Business Research Ltd

The General Conditions of Entitlement[29] 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.

ii Restrictions on the provision of service

The Digital Economy Act 2010 (DEA 2010) includes provisions that were aimed at tackling online copyright infringement as a result of file sharing. It empowers the Secretary of State to impose obligations on ISPs to limit the internet access of subscribers who engage in online copyright infringement. Under the DEA 2010, Ofcom proposed a code of practice governing the initial obligations on ISPs, with a second draft published in June 2012, but this has never been finalised. Instead, the government has looked to industry to develop voluntary measures such as Creative Content UK and Get it Right from a Genuine Site campaign.

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.

iii Music licences

Ofcom does not regulate the music industry, and the industry is generally less regulated than the rest of the media and entertainment sector discussed. A licence is required to be obtained from a collecting society – Performing Right Society Limited (PRS) and Phonographic Performance Limited (PPL) – to play recorded music in public and as part of an audiovisual or radio broadcast. They exist due to the practical difficulties, and administrative burden, for copyright owners and performers if they have to deal with granting licences individually to all those seeking licences. Following a joint venture in 2018 between PRS and PPL the licensing process has been streamlined, and a single licence can now be obtained from one entity. However, the underlying tariffs to be applied are still determined by each collecting society separately.

iv Security

Privacy and consumer protection overview

In the UK, consumers' personal data is primarily protected by the UK General Data Protection Regulation (UK GDPR),[30] which effectively retains the European General Data Protection Regulation (GDPR)[31] in UK law and the UK Data Protection Act 2018 (DPA); the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (the ePrivacy UK Regulations), which implement the EU Directive on Privacy and Electronic Communication,[32] as amended by the ePrivacy Directive;[33] and the NIS Regulation, which implements the NISD. The post-Brexit UK data protection regime, under the UK GDPR

29 See https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-competition-regulation/general-conditions-of-entitlement.

30 Available at https://www.legislation.gov.uk/eur/2016/679/contents#.

31 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

32 Directive 2002/58/EC.

33 Directive 2009/136/EC.

© 2021 Law Business Research Ltd

and the DPA, effectively retains the GDPR in UK law, but does not automatically incorporate any changes made to the GDPR after 1 January 2021. Organisations in the UK may need to comply with both the GDPR and the UK GDPR/DPA, if they have operations in or provides services to individuals in the EEA and are caught by the GDPR's extraterritorial application.

On 10 September 2021, the UK government launched a public consultation on wide-ranging reforms to the UK data protection regime.[34] The proposed reforms include: an expansive framework of international data partnerships, to allow the free flow of personal data from the UK; reforms to the role of the ICO; the introduction of organisation-tailored privacy management programmes to replace certain aspects of the GDPR's accountability framework; raised thresholds for data breach reporting to the ICO; the creation of a specific, exhaustive list of legitimate interests that organisations can pursue without the need to apply the GDPR's balancing test; and removal of the requirement to obtain user consent to certain, limited uses of cookies and tracking technologies. The consultation closes in November 2021, following which further UK policy and regulatory developments are expected as the proposed reforms take shape.

Data protection

The UK data protection regime governs how organisations use or 'process' 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; this is interpreted broadly and includes names, contact information and certain device information. Processing of personal data is also interpreted widely, and includes, among other data, the collection, use, storage, disclosure and transfer of personal data. The UK GDPR and DPA impose strict controls on the processing 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 the legitimate interests of the data controller or a third party (subject to certain conditions) or fulfilling a contract (the standard for valid consent is high and requires consent to be freely given, specific, informed and unambiguous);

b more restrictive controls on the processing of 'special category' personal data[35] and criminal offences data;

c prescribing minimum information that must be provided to data subjects prior to the commencement of data processing, in a clear and accessible manner (subject to certain exemptions);

d 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;

34 'Data: A new direction', available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016395/Data_Reform_Consultation_Document__Accessible_.pdf.

35 Special category data is defined in the UK GDPR and the DPA as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation' (Article 9 of the UK GDPR and section 10 of the DPA 2018).

© 2021 Law Business Research Ltd

e the requirement that data be kept secure (i.e., be protected against unlawful processing and accidental loss, destruction or damage);

f the requirement that a contract (or equivalent legal act), containing minimum mandatory data processing terms, is put in place if a data controller (i.e., the entity determining the purposes and means of the data processing) engages the services of data processor to process personal data on its behalf;

g the restriction that data cannot be transferred to countries outside the UK unless certain conditions are met, such as signing the standard contractual clauses for personal data export (sometimes referred to as 'model clauses'); and

h personal data must be processed in accordance with the rights of the data subject under the UK GDPR, including that individuals have a right to access the personal data held about them; a right to data portability that requires 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; and a right in certain circumstances to have inaccurate personal data rectified or destroyed, among various other rights.

The UK GDPR mirrors the extraterritorial effect of the GDPR; it applies not only to organisations established in the UK, but also to organisations established outside the UK but offering goods or services to, or monitoring the behaviour of, individuals in the UK. Such non-UK organisations are required to appoint a legal representative within the UK. Similarly, organisations in the UK may need to comply with the GDPR, as well as the UK GDPR/DPA, if they have operations in, or provide services to, individuals in the EU and are caught by the GDPR's extraterritorial application; this may include the appointment of a legal representative within the EEA.

The GDPR introduced significantly increased sanctions for non-compliance, which are reflected in the UK data protection regime. The ICO may impose maximum fines of up to the higher of £17.5 million (€20 million under the GDPR) or 4 per cent of an organisation's annual global turnover.

International transfers of personal data

As referred to above, the international transfer of personal data outside the UK is subject to certain conditions under the UK GDPR and DPA. A transfer of data in this context includes access to the data from outside the UK (even if the data itself remains within the UK). This restriction on data transfers does not apply to countries recognised as 'adequate' by the UK Secretary of State, to which personal data may be transferred freely.[36] Following Brexit, relevant adequacy decisions have been passed by the respective European and UK authorities, under the GDPR and the UK GDPR, to permit the unrestricted transfer of personal data between the EEA and the UK and vice versa. In general, the framework for international data transfers from the UK and the EEA has undergone significant change in recent years.

In relation to data transfers from the EEA to the US, on 16 July 2020,[37] in what is known as the *Schrems II* decision, the CJEU invalidated the EU–US Privacy Shield with

36 The UK Secretary of State has recognised the following countries as having adequate protection: (1) all EEA jurisdictions; (2) Gibraltar; and (3) jurisdictions recognised as adequate by the European Commission, as at 31 December 2021 (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, and Uruguay).

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

© 2021 Law Business Research Ltd

immediate effect, on the basis that the Privacy Shield did not provide an 'adequate' level of protection as required under the GDPR for the transfer of personal data from the EEA to the US. The Privacy Shield was one of the primary mechanisms for lawfully transferring personal data from the UK and the EEA to the US; if the US recipient organisation was self-certified under the Privacy Shield regime, personal data could be freely transferred to that recipient. Following *Schrems II*, the Privacy Shield can no longer be relied on to ensure compliance with the UK GDPR or the GDPR for relevant existing or future data exports to the US.

In relation to the standard contractual clauses, the CJEU in *Schrems II* held that the standard contractual clauses remain valid as a mechanism for personal data transfer outside the EEA, and the 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 (a 'transfer impact assessment'). If, in the relevant context, the standard contractual clauses are assessed to insufficiently protect individuals' data, additional supplementary measures should be put in place. The *Schrems II* decision is binding on UK courts; in August 2021, the ICO launched a public consultation on a revised data transfer package under the UK GDPR, which includes guidance and a framework for conducting transfer impact assessments and implementing supplementary measures (as discussed further below).

On 4 June 2021, the European Commission issued revised standard contractual clauses for data transfers subject to the GDPR (revised SCCS),[38] which replace the previous standard contractual clauses from 27 September 2021 (though contracts under the previous standard contractual clauses already in place on this date may continue to be relied on until 27 December 2022, by which date all previous standard contractual clauses must be migrated to the revised SCCs). The revised SCCs are not recognised for data transfers subject to the UK GDPR, for which organisations should continue to rely on the previous standard contractual clauses, until the ICO's revised data transfer mechanisms under the UK GDPR are in effect. On 11 August 2021, the ICO opened a consultation on its proposed, revised data transfer package under the UK GDPR,[39] which includes an International Data Transfer Agreement to replace the previous standard contractual clauses; a UK Addendum to the revised SCCs intended to allow the revised SCCs to be used for data transfers under the UK GDPR; and a framework for conducting transfer impact assessments, as required post-*Schrems II*. The consultation also sought views on certain broader points including the extraterritorial application of the UK GDPR and the scope of the UK GDPR's restrictions on international data transfers. The consultation period closed on 11 October 2021; it is not yet clear when the ICO will publish final documentation.

Protection for children

Children are afforded additional safeguards under the UK data protection regime. The DPA has set the defined age of a 'child' as anyone younger than 13 years old (which is the minimum permitted age threshold under the GDPR). Consent to the processing of personal data in connection with the provision of online services to children is required to be given

38 Available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.

39 Available at https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-data-transferred-outside-of-the-uk/.

© 2021 Law Business Research Ltd

by a person with parental responsibility.[40] 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 UK 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.[41] The ICO published its Age Appropriate Design Code[42] 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 focusing on providing default settings that 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. The safety of children online is monitored and supported by a number of governmental, regulatory and industry bodies and programmes, including: the UK Council for Internet Safety; Ofcom's online safety remit; and the Kitemark for Child Safety Online programme. Further, as referred to above, the draft Online Safety Bill includes proposals for specific duties and obligations in relation to the protection of children from illegal and harmful content online.

ePrivacy UK Regulations

The ePrivacy UK Regulations implemented the ePrivacy Directive into UK law, and continue to apply largely unchanged following Brexit. The ePrivacy UK Regulations broadly govern unsolicited direct marketing, restrictions on the use of cookies, and rules on the use of communications content, traffic and location data.

In relation to cookies and similar tracking technologies, the 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 ePrivacy UK Regulations apply the UK GDPR standard of consent for the purposes of those Regulations, including in relation to cookies, which requires that consent 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 and placement of cookies. Silence or inactivity does not constitute consent. Further, the data subject must have the right to withdraw consent at any time.[43] In July 2019, the ICO updated its guidance on cookies,[44] to clarify the interplay between the GDPR, DPA and ePrivacy UK Regulations and to confirm that the GDPR standard of consent applies (i.e., consent mechanisms must seek clear, unbundled, express acceptance for each relevant category of cookies). Other than

40 UK GDPR: Article 8.

41 UK GDPR: Article 17.

42 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/.

43 UK GDPR: Article 7(3).

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

© 2021 Law Business Research Ltd

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). As referred to above, the UK government's proposed reforms to the UK data protection regime include allowing cookies to be placed without user consent in limited circumstances, such as use of analytics cookies and use for certain purposes for example detecting faults and enhancing functionality.

Individual data subjects have the right under the UK 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. Use of traffic data is also restricted, to certain limited purposes (for example, to manage traffic and billing, limited fraud detection, certain marketing and value added services, in some cases only with user consent). In the EU, 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). The UK has implemented various aspects of the Code, but has not expanded the scope of the ePrivacy UK Regulations to the full extent envisaged by the Code. Where the Code applies the ePrivacy Directive to both number-based and number-independent communications services, the UK implementation[45] does not include number-independent services, which are therefore not brought within the scope of the ePrivacy UK Regulations by virtue of the Code.

The ePrivacy Directive is set to be replaced in the EU by the draft ePrivacy Regulation, which aims to establish a modern, comprehensive and technologically neutral framework for electronic communications, aligned to the GDPR. 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. In February 2021, the European Council announced that the EU Member States had agreed a version of the ePrivacy Regulation,[46] which is currently under review by the European Parliament; the proposals may be further amended before the Regulation is finalised. The Regulation will not be directly applicable in the UK; the ePrivacy UK Regulations will continue to apply as UK national law. The

45 The Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations 2020.

46 Available at https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

© 2021 Law Business Research Ltd

current draft of the Regulation applies extraterritorially, to organisations outside the EU that provide services to end users in the EU; UK organisations may therefore be subject to both the UK ePrivacy regime and the new ePrivacy Regulation, depending on the scope of the finalised text.

Data breach notification

The UK GDPR requires data controllers to notify personal data breaches to the ICO without undue delay and not later than 72 hours after becoming aware of a breach, unless the data security breach is unlikely to result in a risk to the rights and freedoms of a data subject. If a personal data breach results in a high risk to the rights and freedoms of a natural person, a data controller must inform the natural person of the data breach without undue delay.[47] The UK GDPR also requires a data processor to notify a data controller if it becomes aware of a personal data breach. As referred to above, the UK government's proposed reforms to the UK data protection regime include raising the threshold for a data breach reportable to the ICO, from a breach likely to result in 'a risk' to a breach likely to result in 'a material risk' to a data subject. One of the motivations for this proposed change is to reduce the volume of breaches reported to the ICO, which received 9,532 notifications in 2020/21 (71 per cent of which required no further action),[48] and therefore to allow a greater focus on those material breaches which are more likely to require ICO intervention.

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.

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 recent 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). 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).[49] 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

47 UK GDPR: Articles 33 and 34.

48 Available at https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf.

49 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 (the Investigatory Powers Act 2016 (Commencement No. 12) Regulations 2020 (SI 2020/766)).

© 2021 Law Business Research Ltd

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 widens the categories of telecommunications operators (TOs) that can be subject to most powers by including private as well as public operators;

c includes the power to require TOs to retain UK internet users' data, including internet connection records, for up to one year;

d 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); and

e creates new criminal offences for unlawfully accessing internet data, and 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, in the UK courts and at the CJEU. In its decision in *Privacy International v. UK*,[50] delivered on 6 October 2020, the CJEU confirmed that national law derogations from European fundamental rights of privacy must be strictly necessary and proportionate. It determined that UK legislation[51] 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 25 May 2021, the Grand Chamber of the European Court of Human Rights ruled in the case of *Big Brother Watch and Others v. the United Kingdom*[52] that, while a bulk interception regime may in principle be compatible with the European Convention on Human Rights (ECHR), certain aspects of the bulk interception and related regimes under RIPA violate Article 8 ECHR (the right to respect for private and family life and communications) and Article 10 ECHR (the right to freedom of expression).

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

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

51 The Telecommunications Act 1984 and RIPA.

52 ECHR Grand Chamber, *Big Brother Watch and Others v. the United Kingdom* (applications Nos. 58170/13, 62322/14 and 24960/15).

© 2021 Law Business Research Ltd

£1.9 billion over five years until 2021.[53] 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.

The UK Network and Information Systems Regulations 2018 (NIS Regulation) implement the EU Network and Information Security Directive (NISD) in UK law. The NIS Regulation imposes cybersecurity and cyber breach notification requirements on certain regulated operators and service providers, specifically, the NIS Regulation:

a applies to (1) essential service operators (ESOs), subject to certain exemptions (e.g., the finance and civil nuclear sectors), with thresholds designed to capture the most important operators in their sector due to, for example, their size; ESOs must register with their competent authority; and (2) digital service providers (DSPs), which includes online marketplaces, online search engines and cloud computing service providers, subject to certain exemptions (e.g., small and micro businesses);

b is regulated by the ICO in respect of DSPs and, in respect of ESOs, by the competent industry-specific regulator, such as the Department for Business Energy and Industrial Strategy, Ofcom and NHS Digital;

c requires operators to develop minimum levels of security, as well as evidence that these 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 UK 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 empowers competent authorities to impose significant penalties for breach, with fines up to the higher of £17 million or 4 per cent of annual worldwide turnover.

In the EU, the Commission released proposals for an updated NISD in December 2020.[54] The proposals include: an expansion of the sectors and services within NISD scope (to include, inter alia, ECS, social media platforms and data centre services); higher minimum cybersecurity standards; additional obligations in relation to supply chain cybersecurity; and more prescriptive incident notification requirements. Any updated NISD will not apply in the UK, and the UK government has not currently indicated plans for material changes to the NIS Regulation.

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

54 Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN.

© 2021 Law Business Research Ltd

Enforcement

The ICO is responsible for the enforcement of, amongst other legislation, the UK GDPR and DPA, the UK ePrivacy Regulations, the IPA, and the 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 has shown that it is willing to use its powers under the UK GDPR to investigate and issue significant fines for breaches. In its 2020/21 reporting period, the ICO issued three fines under the GDPR/UK GDPR, totalling £39.65 million.[55] In October 2020, the ICO fined British Airways £20 million for failing to protect the personal and financial details of more than 400,000 of its customers impacted by a data breach.[56] Later the same month, the ICO fined Marriott International Inc £18.4 million for infringements of the GDPR stemming from a data breach at Starwood, which Marriott acquired in 2016, effecting millions of individuals.[57] Although these represent a reduction of nearly 90 per cent and 81 per cent, respectively, of the originally proposed fines, the British Airways fine represents the largest fine imposed by the ICO to date for breach of the GDPR. In November 2020, the ICO fined another multinational corporation £1.25 million for failing to keep its customers' personal data secure, arising from a data breach that impacted 9.4 million of its customers across the EU and the UK (1.5 million in the UK). According to the ICO's Annual Report for 2020/21,[58] the ICO has particularly focused its investigation and enforcement efforts on the following topics: improving data handling and transparency practices in the credit referencing and data broking industries; addressing compliance concerns around marketing firms and unsolicited marketing calls in particular; and its ongoing investigation into personal data practices in the adtech industry and real-time bidding environment. These material fines from the ICO are part of an ongoing trend across the EU of data protection supervisory authorities utilising 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.

IV SPECTRUM POLICY

i Development

The current regulatory framework for spectrum has been in force since 2003 following the introduction of the Telecoms Reform Package at EU level. This regulatory framework, requires the neutral allocation of spectrum in relation to the technology and services proposed

55 As stated in the ICO's Annual Report for 2020/21, available at https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf.

56 Available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/.

57 Available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/.

58 Available at https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf.

© 2021 Law Business Research Ltd

by users (e.g., MNOs and radio broadcasters). 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.

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.[59] The Spectrum Policy Forum acts as a proactive industry-led 'sounding board' to the UK government and Ofcom on future policy and approaches on spectrum, and as a cross-industry 'agent' for promoting the role of spectrum in society and the maximisation of its economic and social value to the UK.

ii Flexible spectrum use

Currently, auctions are the primary market tool used to implement the allocation of spectrum.

The Wireless Telegraphy (Mobile Spectrum Trading) Regulations 2011 are 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. They made significant changes to the lengthy process previously required to trade spectrum, 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 and to consider accommodating new types of transfers where there is sufficient evidence of their benefits.[60]

iii Broadband and next-generation mobile spectrum use

The technology has provided more capacity at faster speeds for mobile services on smartphones such as video streaming, email and social networking sites. Following a consultation, on 19 July 2021 Ofcom published its spectrum management strategy for the next decade,[61] whose principal objectives are to:

a drive continued improvements and growth for 'mass market' wireless services (such as Wi-Fi and cellular mobile services);

b ensure businesses, public sector and other organisations with specialist requirements are able to access the wireless communication or spectrum options they require;

c provide increased flexibility in spectrum use to support innovation, with appropriate assurances for continued use; and

d ensure efficient use of spectrum.

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

60 See: https://www.ofcom.org.uk/__data/assets/pdf_file/0029/88337/Trading-guidance-notes.pdf.

61 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0017/222173/spectrum-strategy-statement.pdf.

© 2021 Law Business Research Ltd

To achieve these goals, Ofcom has identified several areas of increased focus, including: promoting spectrum sharing, where possible; supporting wireless innovation by making spectrum more accessible by a wide range of users; and furthering licensing to fit local and national services.

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.

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.

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.

Ofcom ran its latest 5G spectrum auction in early 2021 in respect of 700 MHz and 3.6–3.8 GHz spectrum and confirmed results on 27 April 2021[62] with EE, Hutchinson, Telefonica and Vodafone all securing spectrum.

vi Emergency services bandwidth prioritisation

The Universal Services Directive, a part of the Telecoms Reform Package, introduced several extended obligations in relation to access to national emergency numbers and the single European emergency call number (112).[63] Prior to this, obligations to provide free and uninterrupted access to national and European emergency numbers applied only to providers of publicly available telephone services. 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 organisation. 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.

62 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0028/217954/notice-reg-121.pdf.

63 See https://www.gov.uk/guidance/999-and-112-the-uks-national-emergency-numbers.

© 2021 Law Business Research Ltd

On 25 October 2021, the CMA decided to launch a market investigation into Motorola's Airwave network.[64] The CMA will investigate whether the market for the supply of the mobile radio network used by all emergency services in Great Britain is working well, including in view of Motorola's dual role as both owner of Airwave Solutions, the company currently providing the mobile radio network, and key supplier in the new planned ESN.

V MEDIA

The transition from traditional forms of media distribution and consumption towards digital converged media platforms continues to rapidly evolve, with members of the media and entertainment industries 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 (albeit 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

The increasing demand of internet-delivered content services calls for the UK's broadband infrastructure to be upgraded. People and businesses have demanded more bandwidth this year, especially during lockdown. However Ofcom has reported that the UK's fixed and mobile networks have generally coped well with increased demands during the pandemic.[65]

The government is focused on exploring ways to take superfast broadband to the most remote and hardest-to-reach places in the UK. As at May 2021, superfast broadband coverage sat at 96 per cent, but ultrafast broadband rose to 62 per cent superfast broadband, up from 61 per cent at the start of the year. Mobile operators are rolling out the shared rural network, as agreed with the government in 2020, which will take 4G coverage to 95 per cent of the UK's landmass by 2025. Meanwhile, while Ofcom has noted that full fibre and gigabit-capable networks are still at a relatively early stage of rollout, it reports that over five million (18 per cent) UK homes now have access to full fibre connections – an increase of 8 per cent or just over 2 million premises in the past year (the largest year-on-year increase in full fibre coverage to date).

ii European DSM Strategy, Brexit 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[66] and the UK implemented the revisions to the AVMSD into national law through the Audiovisual Media Services

64 See https://www.gov.uk/government/news/cma-opens-investigation-into-motorola-s-airwave-network?utm_medium=email&utm_campaign=govuk-notifications&utm_source=032eb173-e851-4cc0-9194-2be9631fbc14&utm_content=immediately.

65 Connected Nations 2020: UK report available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/209373/connected-nations-2020.pdf.

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

© 2021 Law Business Research Ltd

Regulations 2020 (UK AVMS Regulations) on 30 September 2020. This amended the existing UK Broadcasting Acts and the Act.[67] Most of the regulations came into force on 1 November 2020, with the remainder coming 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; and

e an obligation on on-demand audiovisual media services to ensure 30 per cent of the works in their catalogues are European works.

A video sharing platform (VSP) is distinct from a VOD service provider and will be regulated in its own right under the UK AVMS Regulations. 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 and new regulations applying to UK-established VSP services came into force on 1 November 2020. From 6 April 2021, VSP providers in the UK jurisdiction are legally obliged to submit a formal notification of their service to Ofcom.. Providers must make their own assessment of whether their service meets the statutory criteria and should therefore be notified. In March 2021, Ofcom published guidance intended to help providers understand whether they fall within scope of the definition of a VSP for the purposes of the Act. Where it appears to Ofcom that a service meets the statutory criteria but has not notified it, Ofcom has the statutory powers to request information in order to make an assessment, and to take enforcement action if a provider has failed to notify. This can include a financial sanction and directing the provider to notify Ofcom. Under the regulations, VSP must have appropriate measures in place to protect children from potentially harmful content and all users from criminal content and incitement to hatred and violence.[68]

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.

On 31 December 2020, the UK government published practical guidance on the AVMSD amendments and on the implications of Brexit on broadcasting and VOD services.[69]

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

68 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0024/215457/statement-video-sharing-platforms-who-needs-to-notify.pdf.

69 Available at https://www.gov.uk/guidance/broadcasting-and-video-on-demand-services-between-the-uk-and-eu.

© 2021 Law Business Research Ltd

On 1 January 2021, the AVMSD, including the country of origin principle,[70] ceased to benefit services under UK jurisdiction made available in the EU, and the UK is now 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). It is 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 still applies, which provides for freedom of reception and retransmission.[71] 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 are 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.

Portability Regulation

On 9 December 2015, the Commission proposed a regulation to enable the cross-border portability of online content services.[72] The resulting Portability Regulation was published in the Official Journal on 30 June 2017[73] and came into force on 1 April 2018.[74] 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.

However, the Portability Regulation ceased to apply to UK–EEA travel from 1 January 2021 and content service providers are no longer 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 see restrictions on the content ordinarily available to them in their home country.[75]

70 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)).

71 Article 4 of Council of ECTT.

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

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

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

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

© 2021 Law Business Research Ltd

Changes to copyright law from 1 January 2021

The EU Copyright Directive came into force on 7 June 2019, and Member States had until 7 June 2021 to transpose the Directive into national law. The Copyright Directive aims to widen copyright exceptions and limitations to the digital and cross-border environment, provide for licensing practices that ensure wider access to creative content and clarify copyright rules to promote a well-functioning copyright marketplace. The UK government has confirmed that the UK will not be required to implement the Copyright Directive and that it has no plans to do so. As a result, there could 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.

In addition to country of origin issues, the revocation of the Portability Regulation, and the continued implementation of the Marrakesh Treaty (which provides an exception to copyright rights for blind or otherwise print disabled persons), a government guidance note published on 30 January 2020[76] identifies changes to copyright law that came 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 changes, 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, which came 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. 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 government has published guidance on *sui generis* database rights,[77] collective rights management,[78] and orphan works.[79]

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), cable and satellite platforms (e.g., Virgin Media and Sky offer VOD products) and standalone VOD platforms (e.g., Netflix, Amazon Prime Video, Disney+ and NowTV).

The industry is transforming as the take-up of superfast broadband and connected televisions changes the way in which people watch audiovisual content. According to Ofcom, people's total television and audiovisual viewing increased dramatically as a result of covid-19 lockdowns, with an increase in total viewing of audiovisual content by 47 minutes to five

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

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

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

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

© 2021 Law Business Research Ltd

hours 40 minutes per person per day in 2020 relative to 2019, with nearly all forms of video viewing increasing year on year. Covid-19 also contributed to the UK's PSBs seeing some of their highest TV viewing shares for five years. However, the highest growth was with SVoD services, which continued to accelerate their share of total viewing.

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. There has also been a notable increase in games console use to an average of over half an hour per day.

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 (and have contracted further during the pandemic), with both digital multichannel and commercial PSBs seeing a decline in total revenue in 2019. According to Ofcom, TV advertising revenue is set to rebound in 2021, but TV broadcasters must continue to adapt to stay competitive (such as improved cross-media measurement, programmatic advertising technologies and addressable advertising).[80]

iv Music

After years of double-digit growth, the UK music industry was expected to have a hugely positive 2020. However, covid-19 stopped all that in its tracks. Overnight, the sector was upended, with live performances banned, international travel restricted and hundreds of thousands unable to work. According to UK Music, in 2020, the music industry contributed £3.1 billion to the UK economy – a 46 per cent decrease from £5.8 billion in 2019. Collecting societies PPL and PRS saw a sharp decline in public performance income, and broadcast income also fell as advertising spend declined, impacting labels, publishers, artists and songwriters. However, the consumption of recorded music remained strong, with streaming income increasing and vinyl sales up on 2019.[81]

Regulators are taking a more keen interest in the sector now. In July 2021, the government published the findings of its inquiry into the economics of streaming and concluded that comprehensive reform of legislation and further regulation is needed, not only to redress the balance for songwriters, performers and composers, but to tackle fundamental problems within the recorded music industry. Its key recommendations are that the government:

a legislate so that performers enjoy the right to equitable remuneration for streaming income;

b refer the industry to the CMA to undertake full market study into the economic impact of the major music groups' dominance; and

c should introduce robust and legally enforceable obligations to normalise licensing arrangements for user-generated content hosting services, to address the market distortions and the music streaming 'value gap'.[82]

80 All data from: (a) Media Nations 2021: UK report available at https://www.ofcom.org.uk/__data/assets/pdf_file/0023/222890/media-nations-report-2021.pdf; and (b) Media Nations 2021: Interactive report available at https://www.ofcom.org.uk/research-and-data/tv-radio-and-on-demand/media-nations-reports/media-nations-2021/interactive-report.

81 Available at https://www.ukmusic.org/wp-content/uploads/2021/10/This-is-Music-2021-v2.pdf.

82 Available at https://publications.parliament.uk/pa/cm5802/cmselect/cmcumeds/50/5002.htm.

© 2021 Law Business Research Ltd

Following the government report, the CMA announced, on 19 October 2021, that it plans to launch a market study into music streaming. The scope of the market study is to be determined before it is formally launched, but it is expected that the CMA would examine whether the sector works in the interests of consumers.[83]

v PSBs

As part of its responsibility as regulator, in December 2020, Ofcom published its findings from its extensive Small Screen: Big Debate research and analysis. The review looked at how to maintain and strengthen public service broadcasting across the next decade and beyond and sets out recommendations for modernising the current framework in order to deliver public service media for audiences watching broadcast TV and online.[84] Ofcom published its recommendations to the government in July 2021.[85]

Broadly, it found that PSBs sit at the heart of the UK's creative industry and has shaped the system as it is today so there is still a strong case for PSBs with benefits including the fact that some types of programming rely heavily on the contribution made by public service broadcasters (e.g., trusted news, art, children's, education and religion programmes), PSBs bring people together by creating shared national experiences, and PSBs reflect the UK's diversity across its nations and regions.

However, technology and global competition are driving the need for change with audiences increasingly turning away from broadcast TV, in particular younger viewers. Ofcom finds that a new regulatory framework is urgently needed as the current PSB system and regulatory regime has seen little change since 2003 (e.g., it remains focused on traditional broadcast television services such that the benefits and obligations placed on ITV/STV, Channel 4, S4C and Channel 5 only apply to their main television channels, and the obligations in the BBC's operating licence mostly apply to its TV and radio output). Therefore, a new framework would establish clear goals for public service media providers, with greater choice over how they achieve them and new system should ensure public service media remains prominent so audiences can readily find it. As with any critical change, Ofcom notes that, for the sector to be effective, it needs to be financially resilient (with licence fee and broadcast TV advertising declining) and deeper strategic relationships between PSBs and other key companies – particularly on platforms and distribution – could help PSM keep pace and compete effectively with global players (e.g., current PSBs are already collaborating on Freeview and BritBox).

The DEA required Ofcom to review the EPG Code prior to 1 December 2020. Pursuant to this, on 30 November 2020, Ofcom published its conclusions on its review of competition rules in the EPG Code. Broadly, Ofcom found that EPGs are an important way to access content on linear TV, competition rules are still required to ensure that licensees do

83 Available at https://www.gov.uk/government/news/cma-plans-probe-into-music-streaming-market.

84 Available at https://www.smallscreenbigdebate.co.uk/__data/assets/pdf_file/0032/208769/consultation-future-of-public-service-media.pdf.

85 Available at https://www.smallscreenbigdebate.co.uk/__data/assets/pdf_file/0023/221954/statement-future-of-public-service-media.pdf.

© 2021 Law Business Research Ltd

not enter into or maintain arrangements or engage in a practice that would be considered to be prejudicial to fair and effective competition, and that the existing rules are indeed working well.[86]

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 implemented changes to the existing linear EPG Code,[87] which came into force on 4 January 2021 with 18 months for EPG providers to implement the new rules.[88]

vi Impact of covid-19

Certain aspects of the media and entertainment sectors have been significantly impacted by the covid-19 pandemic. For example, production arrangements were severely disrupted, sports and other live entertainment, such as music events, ground to a halt and cinemas were also closed, with many releases delayed. Furthermore, TV content investment has been hit hard by the pandemic, with PSB spend on original productions falling by 18 per cent in 2020. This follows a period of strong revenue growth experienced by the UK independent production sector in recent years. However, production activity has now resumed, with help from the government's UK-wide £500 million Film and TV Production Restart Scheme.

On the flip side, covid-19 is seemingly resulting in some positives for the VOD industry. As set out earlier, lockdown prompted a surge in TV viewing in the UK that amplified the shift from broadcast to on-demand. Overall, Ofcom believes that strong demand from international TV broadcasters and SVoD providers, together with continuing commissions from PSBs, indicates that the sector is well placed to recover. However, it remains to be seen how the media and entertainment sector will be impacted by the pandemic on a longer-term basis.

VI THE YEAR IN REVIEW

Towards regulated digital services?

The CMA and the UK government are not alone in planning an *ex ante* regulatory regime in digital markets (as discussed in Section II.i). Competition authorities and governments in other jurisdictions are also considering further regulation and enforcement in this space. For example:

a the European Commission has put forward proposals for the Digital Services Act (DSA) and Digital Markets Act (DMA), and has also been developing a new competition tool to address structural competition problems. The EU Parliament and the EU Council are currently in the process of assessing the European Commission's proposals and are due to publish a draft report. Timing remains unclear, but it is expected that the DMA and DSA will not be entering into force before late 2022 or 2023;

86 Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0022/208480/epg-code-statement-non-confidential.pdf.

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

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

© 2021 Law Business Research Ltd

b in the US, the House Judiciary Antitrust Subcommittee made a number of recommendations relating to digital platforms[89] and 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;[90]

c the ACCC recently published an interim report as part of its digital advertising services inquiry,[91] which includes a number of recommendations relating to data portability and interoperability; and

d in Germany, the 10th amendment to the German Competition Act, which entered into force in January 2021, included a new power for BKartA to prohibit certain types of conduct by companies which are considered 'of paramount significance for competition across markets'.[92]

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 area of international data transfers has seen particularly significant developments over the course of 2020/21, the full implications of which remain to be seen: 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; the introduction of new standard contractual clauses for transfers subject to the GDPR; and the publication of the ICO's proposed new data transfer package under the UK GDPR. The government's proposed reform of the UK data protection regime has the potential to significantly change the data protection landscape for the future, and introduce divergence between the UK and EEA regimes.

With regard to the media and entertainment industries in the UK, the rise in popularity of SVoD services continues and has been accelerated by covid-19. The proliferation of OTT services and their need for high-quality content (both audio-visual and music) to drive subscriber numbers continue to reshape the industry.

89 See the 'Investigation of Competition in Digital Markets Majority Staff Report and Recommendations' available at https://judiciary.house.gov/issues/issue/?IssueID=14921.

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

91 Available at https://www.oaic.gov.au/engage-with-us/submissions/digital-advertising-services-inquiry-interim-report/.

92 See https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html.

© 2021 Law Business Research Ltd

Appendix 1

ABOUT THE AUTHORS

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.

DAVID LITTLE

Latham & Watkins LLP

David Little is a partner in Latham & Watkins' London office. He advises clients on many of their most significant and complex UK, EU and international competition law matters, including merger control, anticompetitive agreements, abuse of dominance and litigation. Drawing on more than a decade of experience spanning large-value transactions and sensitive disputes and investigations, Mr Little counsels leading global clients on a variety of competition issues. Mr Little has advised on some of the largest and highest-profile TMT matters in recent years. Mr Little represents clients before key UK and EU regulatory authorities, including the UK Competition and Markets Authority (CMA), the UK Financial Conduct Authority and the European Commission (EC), and in litigation before the courts of England and Wales and the European courts in Luxembourg. Mr Little offers sophisticated insight into navigating regulatory processes, having been seconded to the CMA in 2015 and having worked with many of the major global antitrust agencies.

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.

© 2021 Law Business Research Ltd

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
gail.crawford@lw.com
david.little@lw.com
lisbeth.savill@lw.com
www.lw.com

© 2021 Law Business Research Ltd

an LBR business

ISBN 978-1-83862-834-5

© 2021 Law Business Research Ltd