THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

THIRTEENTH EDITION

Editor
Matthew T Murchison

THE LAWREVIEWS

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

THIRTEENTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2022
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Matthew T Murchison

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADER
Katie Hodgetts

SENIOR BUSINESS DEVELOPMENT MANAGER
Rebecca Mogridge

BUSINESS DEVELOPMENT MANAGER
Joey Kwok

BUSINESS DEVELOPMENT ASSOCIATE
Archie McEwan

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Isabelle Gray

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Louise Robb

SUBEDITOR
Morven Dean

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.TheLawReviews.co.uk

ISBN 978-1-80449-141-6

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

ACKNOWLEDGEMENTS

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

ANANTLAW

BAGUS ENRICO AND PARTNERS

BAKER MCKENZIE

ELVINGER HOSS PRUSSEN

KIM & CHANG

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

SHIHUI PARTNERS

THE LAW FIRM OF SALMAN M AL-SUDAIRI

TRAPLE KONARSKI PODRECKI & PARTNERS

URÍA MENÉNDEZ

WEBB HENDERSON

CONTENTS

PREFACE v
Matthew T Murchison

LIST OF ABBREVIATIONS vii

Chapter 1 AUSTRALIA 1
Angus Henderson and Irene Halforty

Chapter 2 CHINA 37
Raymond Wang

Chapter 3 COLOMBIA 49
Carolina Pardo, Luis Alberto Castell and Catalina Castellanos

Chapter 4 EGYPT 62
Tarek Badawy, Salma Abdelaziz and Hoda ElBeheiry

Chapter 5 FRANCE 76
Myria Saarinen and Jean-Luc Juhan

Chapter 6 GERMANY 97
Joachim Grittmann and Alexander Wilhelm

Chapter 7 INDIA 112
Rahul Goel and Anu Monga

Chapter 8 INDONESIA 136
Enrico Iskandar, Debu Batara Lubis and Alwin Widyanto Hartanto

Chapter 9 JAPAN 148
Stuart Beraha, Hiroki Kobayashi, Benjamin Han, Takatomo Terasaki and Marina Yamashita

Chapter 10 LUXEMBOURG 179
Linda Funck

Chapter 11 MEXICO 208
Ricardo Ríos Ferrer, María Fernanda Palacios Medina and Sonia Cancino Peralta

Chapter 12 POLAND 221
Xawery Konarski

Chapter 13 SAUDI ARABIA 233
Brian Meenagh, Alexander Hendry, Homam Khoshaim, Lucy Tucker and Lojain Al Mouallimi

Chapter 14 SOUTH KOREA 260
Hyo Sang Kim, Seong-Hyeon Bang, Brian C Oh and Jung-Chull Lee

Chapter 15 SPAIN 271
Pablo González-Espejo and Ignacio Klingenberg

Chapter 16 SWITZERLAND 290
Lukas Bühlmann and Michael Reinle

Chapter 17 TAIWAN 305
Ken-Ying Tseng, Vick Chien and Sam Huang

Chapter 18 UNITED KINGDOM 317
Gail Crawford, David Little and Lisbeth Savill

Chapter 19 UNITED STATES 349
Matthew T Murchison, Elizabeth R Park and Michael H Herman

Appendix 1 ABOUT THE AUTHORS 375
Appendix 2 CONTRIBUTORS' CONTACT DETAILS 393

PREFACE

This 13th edition of *The Technology, Media and Telecommunications Review* provides updated overviews of legal and policy constructs and developments in the TMT arena across 18 jurisdictions around the world. As in years past, our goal with this publication is to provide a practical, business-focused survey of these issues, along with insights into how regulatory activity in this arena continues to evolve.

Policymakers in 2022 have continued to grapple with the impact of the covid-19 pandemic, which has focussed greater attention on the need for ubiquitous broadband internet connectivity and has hastened efforts to make broadband services more widely available. The height of the pandemic saw a significant rise in remote working, distance learning, tele-health visits, and similar broadband-enabled activities. And while more businesses and schools are now returning to an in-person environment, it remains the case that work, education, and other aspects of our daily lives are more reliant on broadband connectivity today than before the pandemic.

These developments have spurred numerous initiatives around the world to improve and expand broadband connectivity for consumers going forward. Governments in various jurisdictions are in the midst of implementing subsidy programmes and other efforts to speed the deployment of advanced networks in unserved and underserved areas. Regulators have also taken steps to preserve internet access where it already exists, including by exploring mandates requiring certain rates for low-income consumers. Such initiatives have sparked notable legal challenges and policy debates over whether government intervention, market-based solutions, or some combination of the two can be most effective at ensuring widespread broadband availability.

Regulators also are wrestling with how best to fund these ever-growing programmes to promote broadband deployment and availability. Recent years have seen the use of various paradigms, including direct appropriations from the government and funds fed by mandatory contributions from telecommunications service providers and their customers. At the same time, some jurisdictions are looking to other funding mechanisms, such as potentially requiring large online platform providers and streaming video services, whose content makes up a significant portion of internet traffic, to bear some responsibility for contributing to the deployment of networks that carry that traffic.

The relationship between these online content providers and the broadband providers delivering their content also remains the subject of wider policy debates. There continue to be long-simmering questions about 'net neutrality,' including whether 'zero-rating' and other kinds of network management practices by broadband providers benefit or harm consumers and online content providers, and whether efforts to promote a healthy internet ecosystem are best served by light-touch, market-based regimes or by more intrusive government regulations.

In the past year, Europe has been at the forefront of developments on these issues, while policymakers in the United States have faced obstacles to their anticipated re-evaluation of the light-touch approach reinstated in 2018. Debates about 'neutrality' have also carried over to the content side, where social media companies are facing ongoing scrutiny over claims of discriminatory practices in moderating third-party content 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 addition, governments around the world continue to take steps to harness new communications technologies. The era of 5G wireless services is now in full swing, and regulators are exploring ways to facilitate further deployment of these services. These efforts include actions to free up more radiofrequency spectrum for these services, by reallocating spectrum from one use to another, auctioning off wireless licences in bands newly designated for 5G, and adopting new spectrum sharing rules. Deployments of new satellite broadband systems, including large systems in low Earth orbit, also are underway, raising fresh questions about how best to ensure space safety and mitigate new sources of radiofrequency interference.

This edition's chapters for each country describe these and other developments, including updates on media ownership, privacy and data security, and efforts to combat fraudulent robocalling and the 'spoofing' of caller identification information. Our contributing authors have done tremendous work in preparing these updated overviews of TMT issues in their respective jurisdictions, and I hope this latest edition of *The Technology, Media and Telecommunications Review* will be a helpful resource to readers interested in the legal and policy developments in this sector.

Matthew T Murchison
Latham & Watkins LLP
Washington, DC
November 2022

Chapter 18

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 2022–23 Plan of Work (published in March 2022).[2] They include supporting the development of the UK economy through continued investment in high-quality, reliable and resilient fixed and mobile broadband, sustaining a strong and representative broadcasting sector anchored by the UK's public service broadcasters, establishing a solid foundation for the regulation of online safety, growing Ofcom's skills and capabilities (particularly in the areas of cyber and online technologies) and improving 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 increasingly 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). For example, in September 2022 Ofcom announced that, in close coordination with the CMA, it would launch a market study into the UK cloud services sector to examine whether the market is working well and whether any market features may limit innovation or growth.

---

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 Aisha Babalakin, Alexandra Luchian, Sean Newhouse, Stewart Robinson, Victoria Wan, Nara Yoo and Amy Smyth in the preparation of this chapter.

2 Ofcom's Plan of Work 2022/23 available at https://www.ofcom.org.uk/__data/assets/pdf_file/0019/234334/Statement-Plan-of-Work-2022_23.pdf.

It simultaneously announced that it would be examining other digital services over the following year, including online personal communication apps and devices for accessing audio-visual content.[3]

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.[4] Ofcom's main duties are set out in its 2022–23 Plan of Work.[5]

The prevailing regulatory regime in the UK is contained primarily in the Act, which entered into force on 25 July 2003 (as amended). 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 Network and Information Systems Regulations 2018 (NIS Regulation) which implement the EU Network and Information Security Directive (NISD) in UK law;
g the Freedom of Information Act 2000;
h the Investigatory Powers Act 2016;
i the Telecommunications (Security) Act 2021;
j the Enterprise Act 2002;
k the Copyright, Designs and Patents Act 1988 (CDPA);
l the Digital Economy Act 2017 (DEA);
m the Competition Act 1998;
n the Consumer Rights Act 2015;
o the European Convention on Transfrontier Television (ECTT);
p 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,[6] establishing the European Electronic Communications Code; and
q the National Security and Investment Act 2021.

3 See https://www.ofcom.org.uk/news-centre/2022/ofcom-to-probe-cloud,-messenger-and-smart-device-markets.

4 Section 3(1) of the Act.

5 Ofcom's Plan of Work 2022/23 available at https://www.ofcom.org.uk/__data/assets/pdf_file/0019/234334/Statement-Plan-of-Work-2022_23.pdf.

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

The CMA launched a Digital Markets Taskforce in 2020 in conjunction with Ofcom and the Information Commissioner's Office (ICO) to advise the UK government on designing a new regulatory regime for the digital sector. The Digital Markets Taskforce's advice was published in December 2020,[7] and it called 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';[8]

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 has been working in this capacity 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).[9] In a press release dated 20 July 2021,[10] 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. In the 2022 Queen's Speech, the UK government pledged to introduce a draft Digital Markets, Competition and Consumer Bill within the 2022–2023 parliamentary session.[11] Once enacted (which may well extend beyond the 2022–2023 parliamentary session), this would put the DMU and the regime recommended by the Digital Markets taskforce on a statutory footing.[12]

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

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

8 ibid.

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

10 See https://www.gov.uk/government/news/government-unveils-proposals-to-increase-competition-in-uk-digital-economy.

11 See https://www.gov.uk/government/speeches/queens-speech-2022.

12 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1074113/Lobby_Pack_10_May_2022.pdf.

and radio broadcasting requires a licence from Ofcom under the Broadcasting Act 1990 or 1996. Providers of on-demand programme services must notify Ofcom of their services in advance, and Ofcom regulates the editorial content (programming) of these services.

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 European Economic Area (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 (1) the need to ensure sufficient plurality of persons with control of media enterprises serving UK audiences; (2) the need for the availability throughout the UK of high-quality broadcasting calculated to appeal to a broad variety of tastes and interests; and (3) 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 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

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.

National Security and Investment Act 2021 (the NSI Act).[16] The NSI Act came into force on 4 January 2022, introducing a hybrid mandatory and voluntary notification regime. This brings to the UK a regime similar to the one under the EU Foreign Direct Investment Regulation. The NSI Act imposes mandatory notification requirements and associated stand-still obligations to relevant acquisitions in 17 sectors defined in the National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021.[17] The 17 sectors include advanced robotics, artificial intelligence, communications, cryptographic authentication, data infrastructure, quantum technologies and satellite and space technology. No financial thresholds or *de minimis* exemptions apply. A separate unit within the Department for Business, Energy and Industrial Strategy, the Investment Security Unit, handles notifications.[18]

v Digital single market (DSM) and beyond: mobile ecosystems, online platforms and telecoms

A key initiative of Europe's DSM Strategy is the Digital Services Act package. This was announced by the European Commission (the 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 2020, following stakeholder consultations, the Commission proposed two legislative initiatives to carry forward this vision: the Digital Services Act (DSA) and the Digital Markets Act (DMA); together they constitute the DSA package.

The DSA creates enforceable obligations and increased accountability rules for intermediary services offering network infrastructure, hosting services and online platforms. Specific areas of focus include content moderation, targeted advertising, transparency, business traceability and data access, among others. The DSA applies to entities offering their services in the EU single market, regardless of domicile, and will be enforced primarily by designated national competent authorities.[19] The DSA entered into force on 16 November 2022 and the majority of its provisions will apply from 17 February 2024.[20] Certain reporting obligations applicable to online platforms started to apply immediately upon the DSA's entry into force, and provisions governing 'very large online platforms' (a technical designation in the DSA) will apply four months following notification by the Commission to each platform concerned. The DSA does not apply in the UK, following Brexit, though the proposed UK 'online harms' regime covers certain similar topics (e.g., content moderation, transparency, online advertising), albeit under a substantively different framework (see online platforms sub-section).

The DMA, which will be enforced by the Commission, seeks to address perceived market imbalances associated with large online platforms acting as gatekeepers, defined

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

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

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

19 See https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

20 See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN.

under certain criteria. To this end, the DMA includes obligations affecting daily operations, including enabling transparency for advertisers, ensuring interoperability with competing third-party software in certain cases, and prohibiting gatekeepers from blocking users from un-installing software or apps. The DMA entered into force on 1 November 2022 and will be applicable from 2 May 2023.[21]

Mobile ecosystems

In June 2021, the CMA launched a market study into the supply of mobile operating systems (iOS and Android) along with the corresponding app stores and mobile web browsers. The market study concluded in June 2022. In its final report,[22] the CMA proposed a market investigation[23] into mobile browsers and cloud gaming and announced further enforcement action, including a new investigation into Google's app store payment practices (alongside the ongoing similar investigation into Apple).[24] The CMA acknowledged that its concerns may be resolved by the new SMS regime (once in force), as well as changes implemented as a result of the DMA, but the CMA nonetheless considered it necessary to take action using its existing powers.

The Commission has also continued to pursue investigations related to mobile ecosystems. In May 2022, it sent Apple a statement of objections alleging that Apple has abused its dominant position in the market for mobile wallets on iOS devices, by limiting the access of developers to the NFC (near-field communication) hardware and software on Apple devices.[25] The Commission also has an ongoing investigation into Apple's App Store rules, which was commenced in 2020 and which has led to a statement of objections in 2021.[26] In September 2022, the EU General Court largely upheld the Commission's 2018 decision to fine Google over €4 billion for abusing its dominant position by imposing contractual restrictions on mobile device manufacturers and mobile network operators.[27]

Online platforms

The role of online platforms in the economy has continued to expand over 2021/22. 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 (which came into force on 20 June 2020).[28] The Regulation has been implemented in the UK in the UK Platform to Business Regulations,[29] which include measures seeking to reduce unfair trading practices, increase transparency and resolve disputes more effectively.

21 See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.265.01.0001.01.ENG.

22 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1096277/Mobile_ecosystems_final_report_-_full_draft_-_FINAL__.pdf.

23 A market investigation is a longer, more in-depth examination which the CMA may launch following a market study if it considers that there are reasonable grounds for suspecting that there are features which prevent, restrict or distort competition in the relevant market(s).

24 See https://www.gov.uk/cma-cases/investigation-into-apple-appstore.

25 See https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2764.

26 See https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2061.

27 See https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210197en.pdf.

28 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.

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

The 'online harms' regime is the name given to a proposed UK regulatory framework governing content posted via online services. On 17 March 2022, the UK government formally introduced its draft Online Safety Bill into Parliament (the Bill).[30] The proposed regulatory regime under the Bill will apply to online user-to-user services (e.g., social media platforms, online marketplaces and online forums) and to internet search services that have 'links with the United Kingdom',[31] 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, and in certain circumstances from harmful 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).[32] The proposed duty of care imposes requirements on providers both in terms of processes they must implement and their moderation of specific content. Regulated service providers will be required to have regard to freedom of speech and privacy rights in parallel to their duties to safeguard against illegal and harmful content. In addition to the statutory duties of care, the Bill imposes obligations on providers to minimise the risk of fraudulent advertisements on their services, and, in the case of 'Category 1' services, to offer adult users the option to verify their identity and to choose to only interact with verified users. 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 provider's annual global revenue; and (2) court orders to disrupt or prevent access to the services of non-compliant providers. In addition, Ofcom will be able to recommend 'proactive technologies' to address online harms (e.g., content moderation, user profiling and behaviour identification technologies) and set its expectations for the use of such technologies in its codes of practices. 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 complaints to Ofcom. The Bill is intended to supersede relevant existing requirements under the UK Audiovisual Media Services Regulations for providers of video sharing platforms to take measures to protect the public from harmful material. The Bill will be subject to further debate and potential amendment in parliament as it progresses through the legislative process over the course of 2022 and into 2023.

Telecoms

The current European Commission telecoms and connectivity initiatives include:

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

30 Available at https://bills.parliament.uk/bills/3137/publications.

31 Defined in Sections 3(5) and 3(6) of the Bill as services that either (1) have a significant number of users in, or are targeted towards users in, the UK; or (2) are capable of being used in the UK and give rise to a material risk of significant harm to individuals in the UK.

32 Ofcom will also determine the threshold conditions for Category 2A and Category 2B 'as soon as reasonably practicable' after the first sections of the Bill come into force (see Section 81 of the Bill).

b a plan for an EU space-based secure communication system and a Regulation governing space-based secure connectivity.[33]

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.[34] 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 updates to the General Conditions of Entitlement have been coming into force on a staggered basis, with the final update scheduled to occur in December 2022.[35] They 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.[36] 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.[37]

The General Conditions of Entitlement[38] require all providers of public electronic communications networks (ECNs) to negotiate interconnection with other providers of public ECNs. Specific access conditions may also be imposed on operators with SMP.

33 See https://ec.europa.eu/commission/presscorner/detail/en/IP_22_921.

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

35 See https://www.ofcom.org.uk/__data/assets/pdf_file/0020/209504/eecc-statement-dec-20.pdf.

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

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

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

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 internet service providers (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 Data protection and cyber security

Overview of the UK data protection regime

In the UK, individuals' personal data is primarily protected by the UK Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR);[39] the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the ePrivacy UK Regulations); [40] and the NIS Regulation. In this chapter, references to the UK GPDR should be read as capturing both the UK GDPR and the DPA, unless stated otherwise.

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 imposes strict controls on the processing of personal data, including (but not limited to):

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 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 or that the individual has consented (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[41] and criminal offences data;

39 Available at https://www.legislation.gov.uk/eur/2016/679/contents#. The UK GDPR effectively retains the 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 (the General Data Protection Regulation or GDPR), in UK law post-Brexit (but does not automatically incorporate any changes made to the GDPR after 1 January 2021).

40 As amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, which implement EU Directive 2002/58/EC on Privacy and Electronic Communication, as amended by the ePrivacy Directive 2009/136/EC.

41 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

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

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;

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 (as set out below); and

h personal data must be processed in accordance with the rights of the data subject under the UK GDPR, including 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.

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, if they have operations in, or provide services to, individuals in the EEA and are caught by the GDPR's extraterritorial application; this may include the appointment of a legal representative within the EEA.

The UK GDPR features significant sanctions for non-compliance, including empowering the ICO to impose maximum fines of up to the higher of £17.5 million or 4 per cent of an organisation's annual global turnover.

International transfers of personal data

International transfer of personal data outside the UK is subject to certain conditions under the UK GDPR. 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.[42] Following Brexit, relevant adequacy decisions have

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).

42 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 2020 (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay). The UK has also agreed an adequacy decision in principle with the Republic of Korea, which is in the process of being formalised.

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.

The framework for international data transfers from the UK, and the EEA, has undergone significant change in recent years. On 16 July 2020, the CJEU issued its *Schrems II* decision[43] (which is binding on UK courts) in which it invalidated the EU–US Privacy Shield Adequacy Decision (2016/1250) with 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 United States. The Privacy Shield was one of the primary mechanisms for lawfully transferring personal data from the UK and the EEA to Privacy Shield-certified organisations in the United States. Since *Schrems II*, relevant US and EU bodies have sought to put in place a new, updated data transfer framework, to replace the Privacy Shield. In October 2022, President Biden signed an Executive Order on 'Enhancing Safeguards for United States Signals Intelligence Activities'[44] (the EO), which will underpin a new EU–US data transfer framework. Before organisations can start to rely on this new framework to ensure GDPR compliance for EEA to US data transfers, the EEA must be designated as a 'qualifying state' by the US Attorney General under the EO, and the Commission must issue an adequacy decision under the GDPR. In relation to data transfers to the US from the UK, the UK government has stated an intention to issue an adequacy decision under the UK GDPR on the basis of the EO, in October or November 2022.[45]

In relation to the standard contractual clauses (another key mechanism for lawful data transfers), the Court of Justice of the European Union (CJEU) in *Schrems II* held that the standard contractual clauses remain valid as a mechanism for international personal data transfer, but that they cannot be used if the legislation in the third country does not enable the data 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 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 EO will facilitate use of the standard contractual clauses, in addition to underpinning a new EU–US data transfer framework, by establishing enhanced redress mechanisms (assuming the EEA and the UK are designated as qualifying states under the EO for the purposes of those redress mechanisms) and proportionality requirements on US surveillance, which may be documented in transfer impact assessments to assist in evidencing adequate protection for data transferred to the United States.

For data transfers subject to the GDPR, the European Commission issued revised standard contractual clauses on 4 June 2021 (revised SCCs),[46] which replaced the previous standard contractual clauses from 27 September 2021 (though contracts under the previous

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

44 Available at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.

45 UK Government press release available at https://www.gov.uk/government/news/uk-and-us-meet-to-make-positive-progress-on-data-and-tech; UK–US Joint Statement available at https://www.gov.uk/government/publications/uk-and-us-progress-tech-and-data-partnership/uk-us-joint-statement-new-comprehensive-dialogue-on-technology-and-data-and-progress-on-data-adequacy.

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

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).

For data transfers subject to the UK GDPR, the government and the ICO published revised data transfer terms in February 2022, which came into force on 21 March 2022. These data transfer terms consist of an International Data Transfer Agreement (a standard-form, standalone data transfer agreement) and an International Data Transfer Addendum to the revised SCCs (a standard-form addendum to the revised SCCs, which allows the revised SCCs to be used for transfers subject to the UK GDPR).[47] For data transfers subject to the UK GDPR, the International Data Transfer Agreement and the International Data Transfer Addendum replaced the previous EU standard contractual clauses from 21 September 2022 (though contracts under the previous standard contractual clauses already in place on this date may continue to be relied on until 21 March 2024, by which date all previous standard contractual clauses must be migrated to either the International Data Transfer Agreement or the International Data Transfer Addendum). The ICO has also published a draft framework for conducting transfer impact assessments under the UK GDPR, as required post-*Schrems II*;[48] this is expected to be released in final form before the end of 2022.

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.[49] The UK GDPR also requires a data processor to notify a data controller if it becomes aware of a personal data breach.

Under the ePrivacy UK Regulations, providers of public electronic communications services (ECS) (mainly telecom providers and ISPs) are required to inform the ICO within 24 hours of a personal data security breach and, if 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.

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 by a person with parental responsibility.[50] 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

47 Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

48 ibid.

49 UK GDPR: Articles 33 and 34.

50 UK GDPR: Article 8.

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.[51] The ICO published its Age Appropriate Design Code[52] 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.

Enforcement

The ICO is responsible for the enforcement of, amongst other legislation, the UK GDPR, 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).

The ICO has shown that it is willing to use its powers to investigate and issue significant fines for breaches of UK data protection law, as evidenced in the ICO's largest data protection fines to date of £20 million against British Airways[53] and £18.4 million against Marriott International Inc,[54] in both cases relating to significant personal data breaches. On 23 May 2022, following a joint investigation with the Office of the Australian Information Commissioner, the ICO fined Clearview AI Inc over £7.5 million for UK GDPR breaches relating to Clearview's use of more than 20 billion images of people's faces and data from publicly available information on the internet and social media platforms to create a global online database that could be used for facial recognition. The ICO also ordered Clearview to stop its collection and use of UK residents' personal data and to delete such data from its systems.[55] More recently, in October 2022, the ICO fined Interserve Group Limited £4.4 million for alleged data security failings, resulting in a cyberattack impacting the personal data of over 100,000 Interserve employees.[56] In September 2022, the ICO issued TikTok Inc and TikTok Information Technologies UK Limited with a notice of intent to impose a provisional fine of £27 million for allegedly failing to protect children's privacy when using

51 UK GDPR: Article 17.

52 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/.

53 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/.

54 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/.

55 Available at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/.

56 Available at https://ico.org.uk/action-weve-taken/enforcement/interserve-group-limited/.

the TikTok video-sharing service.[57] These material fines from the ICO are part of an ongoing trend across Europe 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.

Reform of the UK data protection regime

On 10 September 2021, the UK government launched a public consultation on reforms to the UK data protection regime.[58] Following the consultation and the government's response,[59] in July 2022 the UK government introduced to Parliament the Data Protection and Digital Information Bill (the UK Reform Bill).[60] The UK Reform Bill largely maintains the GDPR framework in UK law, albeit with a number of modifications reflecting the government's intention to move away from prescriptive requirements to a more risk-based approach. The proposed reforms include:

a the introduction of risk-based 'privacy management programmes' to replace certain aspects of the GDPR's accountability framework;

b the creation of a specific, exhaustive list of legitimate interests that organisations can pursue without the need to apply the UK GDPR's balancing test, when relying on those legitimate interests as a lawful basis for data processing;

c removal of the general prohibition on automated decision making in the UK GDPR, to be replaced with a prohibition only when automated decision making involves processing special category personal data (absent contractual necessity, legal obligation or explicit consent);

d removal of the requirement for non-UK organisations that are subject to the UK GDPR to appoint a UK representative;

e adopting a risk-based approach to adequacy decisions, and creating a new power for the DCMS to recognise alternative transfer mechanisms. The impetus behind these particular proposals is to expand the UK's international data transfer framework and facilitate data flows from the UK; and

f a less restrictive approach to cookies and tracking technologies (detailed further below).

On 3 October 2022, in a speech at the Conservative Party Conference, the Secretary of State for the DCMS expressed the government's intention to replace the UK GDPR with a new 'business and consumer-friendly, British data protection system', designed to protect individual's privacy and relieve businesses from disproportionate regulatory burden. The Secretary of State did not refer to the UK Reform Bill in her speech, and the nature, extent, and timings of any new proposals for the UK's data protection regime remain to be seen.

57 Available at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-could-impose-multi-million-pound-fine-on-tiktok-for-failing-to-protect-children-s-privacy/.

58 '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.

59 Available at https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#:~:text=The%20government%20launched%20its%20consultation,the%20UK%27s%20National%20Data%20Strategy.

60 Available at https://bills.parliament.uk/bills/3322.

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 is required for the placement of cookies, 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. In July 2019, the ICO updated its guidance on cookies,[61] to clarify the interplay between the UK GDPR, DPA and the ePrivacy UK Regulations, to confirm that the GDPR standard of consent applies, and to specific that cookie consent mechanisms must seek clear, unbundled, express acceptance for each relevant category of cookies, prior to placement of cookies.

As referred to above, the UK Reform Bill includes a number of proposals in relation to cookies, including allowing the placement of non-strictly necessary cookies, absent user consent, for a limited number of non-intrusive purposes (e.g., website functionality or audience management). In the longer term, the government's stated aim is to move to an opt-out consent model for cookies, eliminating the need for UK websites to display cookie banners. The UK Reform Bill will also increase fines for breaches of the ePrivacy UK Regulations from the current maximum of £500,000 to UK GDPR level fines (i.e., £17.5 million or 4 per cent of global annual turnover).

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. To the extent that marketing involves the use of personal data (e.g., an individual subscriber's email address featuring their first and last name), the UK GDPR right to object to marketing applies in parallel to the rules under the ePrivacy UK Regulations.

The ePrivacy UK Regulations also govern the use of 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

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

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. Unlike the Code, which applies the ePrivacy Directive to both number-based and number-independent communications services, the UK implementation[62] 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 (but not in the UK) by the draft ePrivacy Regulation, which aims to establish a modern, comprehensive and technologically neutral framework for electronic communications, aligned to the GDPR. However, the draft regulation has been subject to intense scrutiny and debate over a number of years and remains under review through the European legislative process.[63]

Cybersecurity

The cybersecurity regime applicable in the telecommunications, technology, digital and platform space is likely to change considerably over the course of 2023 and beyond, with a number of new laws coming into effect. 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.

Historically, the regulatory landscape has consisted primarily of the Computer Misuse Act 1990 (as amended by the Police and Justice Act 2006) and the NIS Regulation, in addition to the UK GDPR. The Computer Misuse Act sets out a number of provisions that make hacking and any other forms of unauthorised access, as well as DoS (Denial of Service) attacks and the distribution of viruses and other malicious codes, criminal offences. In September 2022, the government opened a 'call for information',[64] as part of its 'Cyber Duty to Protect' programme, seeking views on potential updates to the Computer Misuse Act intended to enhance obligations on providers to protect against unauthorised access to online accounts and user data.

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) operators of essential services (OESs), 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; OESs may be designated as such by a relevant competent authority and must register with their

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

63 The version of the ePrivacy Regulation agreed by the EU Member States in the European Council is available at https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

64 Available at https://www.gov.uk/government/consultations/unauthorised-access-to-online-accounts-and-personal-data/call-for-information-unauthorised-access-to-online-accounts-and-personal-data.

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 OESs, by the competent industry-specific regulator, such as the Department for Business Energy and Industrial Strategy, Ofcom or 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. 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 OESs), 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.

Following the consultation on wide-ranging proposals to reform the NIS Regulations in January 2022, on 4 July 2022, the DCMS published its second post-implementation review of the NIS Regulation,[65] and highlighted areas of improvements such as registration of relevant digital service providers and related guidance, ensuring that the right organisations are in scope of the NIS Regulations, supply chains, capability and capacity of operators and competent authorities, incident reporting, enforcement and increased cross-sector coordination. The next statutory post-implementation review of the NIS Regulations will be carried out in 2027.[66] The proposed development of the NIS Regulations complements the government's consultation on broader legislative reform to improve the UK's cyber resilience, which closed in April 2022.[67]

A significant new piece of telecoms legislation – the Telecommunications (Security) Act 2021[68] (TSA 2021) – came fully into force on 1 October 2022 and introduces a new telecoms security framework in the UK for 5G technology and full fibre networks.[69] The TSA 2021 (1) imposes minimum security standards and compromise notification requirements on providers of public ECNs and public ECSs; (2) places duties on such providers to identify

65 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1094301/Second_Post_Implementation_Review_of_the_Network_and_Information_Systems_Regulations_2018.pdf.

66 In May 2022, the European institutions agreed the text of an updated NISD (NIS 2 Directive), which expands the scope of the NISD (to include, inter alia, ECS, social media platforms and data centre services); raises minimum cybersecurity standards; introduces obligations in relation to supply chain cybersecurity; and includes more prescriptive incident notification requirements.

67 Available at https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience.

68 Available at https://www.legislation.gov.uk/ukpga/2021/31.

69 The TSA 2021 replaces Sections 105A to 105D of the Communications Act 2003 with new Sections 1-5A to 105Z29; under the original sections of the Communications Act 2003, providers were broadly responsible for setting their own security standards for their networks and communications services.

and reduce the risk of security compromises and prepare for the possibility of their occurrence; and (3) imposes contractual obligations on those ECN and ECS providers, that are expected to indirectly impact a range of providers in the telecommunications supply chain. The TSA 2021 also allows the government to prohibit or restrict relevant telecommunications providers from procuring or using goods or services supplied by government-specified 'designated vendors' on national security grounds.

The specific measures ECN and ECS providers must take to meet the security standards of the TSA 2021 are set out in the Electronic Communications (Security Measures) Regulations 2022[70] (Security Measures Regulations), which also came into force on 1 October 2022. The Security Measures Regulations detail security measures relating to, inter alia, (1) network architecture; (2) data and network functions; (3) supply chain measures; (4) prevention of unauthorised access or interference; (5) remediation and recovery; (6) patches and updates; (7) testing; and (8) governance. The Security Measures Regulations are accompanied by a draft code of practice,[71] which contains technical guidance on how providers can meet their legal obligations. Ofcom oversees the TSA 2021 and the Security Measures Regulations and has powers to impose financial penalties of up to 10 per cent of turnover or £100,000 per day for ongoing violations.

In relation to digital and connected consumer product security, the government introduced to parliament the Product Security and Telecommunications Infrastructure Bill[72] (PSTI Bill) on 11 May 2022. The PSTI Bill proposes to:

a ban universal default passwords;

b impose a requirement on manufacturers of 'connectable products' (all devices that can access the internet or that can connect to multiple other devices) to inform customers about the minimum amount of time for which a product will receive security updates and patches, or disclose that a product does not come with security updates;

c compel manufacturers to provide a public point of contact to simplify reporting of flaws of bugs in products; and

d impose security requirements on relevant retailers.

The PSTI Bill includes fines for non-compliance of up to £10 million or 4 per cent of global annual turnover, and daily fines of £20,000 per day for ongoing violations.

Data retention, interception and disclosure of communications data

The powers of government authorities (and, in a more limited capacity, private organisations) to intercept communications, acquire communications data and interfere with communications equipment is governed primarily by the Investigatory Powers Act 2016 (IPA) and the Regulation of Investigatory Powers Act 2000 (RIPA). The IPA overhauls, and in some cases extends, the scope of RIPA, and also repeals Part One of RIPA (which covered the

70 Available at https://www.legislation.gov.uk/uksi/2022/933/contents/made.

71 The draft code of practice was laid before Parliament on 5 September 2022 and will remain in draft for Parliamentary scrutiny for 40 sitting days, after which time the government intends to issue the code of practice. The draft code is available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1102307/Code_of_practice_-_Web_PDF.pdf.

72 Available at https://bills.parliament.uk/bills/3069.

interception and acquisition of communications data).[73] 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 imposes a general prohibition on the interception of communications unless the interceptor has lawful authority to carry out the interception, such as where a warrant has been issued by the Secretary of State (interception warrant). The IPA also governs the use and oversight of investigatory powers of the executive branch, including:

a 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 the power to require telecommunications operators (TOs) to retain UK internet users' data, including internet connection records, for up to one year;

c 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

d 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*,[74] 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[75] 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. The UK courts have subsequently endorsed the CJEU's decision,[76] but have yet to rule on the consequences of the UK's regime for the acquisition of bulk communications data being deemed incompatible with EU law.

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 by users (e.g., mobile network operators 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.

73 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)).

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

75 The Telecommunications Act 1984 and RIPA.

76 *Privacy International v. SSFCA & Ors* [2021] UKIPTrib IPT/15/110/CH.

The 2016 framework established three key elements when identifying potential sharing opportunities in certain bands: (1) characteristics of use for all users that inform the initial view of the potential for sharing, and what tools may be relevant; (2) 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 (3) regulatory tools and market and technology enablers that match the characteristics of use and barriers to facilitate new and more intense sharing.[77] 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.

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,[78] 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.

To achieve these goals, Ofcom has identified several areas of increased focus, including: (1) promoting spectrum sharing, where possible; (2) supporting wireless innovation by making spectrum more accessible by a wide range of users; and (3) furthering licensing to fit local and national services.

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

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

Following a consultation, on 30 June 2022 Ofcom announced that it will not be proceeding with proposals to add the upper 6GHz band to Ofcom's Shared Access licensing framework for low-power, indoor use, in light of lack of evidence of demand and the wider discussions around the long-term future of the band.[79]

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 radio frequencies 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 700MHz and 3.6–3.8GHz spectrum and confirmed results on 27 April 2021[80] 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).[81] Under this Directive, obligations to provide free and uninterrupted access to national and European emergency numbers 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'. 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)

79 See https://www.ofcom.org.uk/consultations-and-statements/category-2/spectrum-sharing-upper-6-ghz-band.

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

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

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.

On 25 October 2021, the CMA decided to launch a market investigation into Motorola's Airwave Network.[82] The investigation is examining 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 a key supplier in the new planned ESN. In October 2022, the CMA issued a provisional decision in which it provisionally identified an adverse effect on competition stemming from Airwave Solutions' and Motorola's market power in the supply of Land Mobile Radio network services for public safety in Great Britain. The CMA proposed to (1) limit the prices that Airwave Solutions may charge for the Airwave Network and services; and (2) impose new obligations on Airwave Solutions and Motorola regarding the development and delivery of alternative technology facilitating the transition to the new ESN.[83] The CMA also proposed to make a recommendation to the Home Office supplementing these proposed remedies. The CMA plans to issue its final report in December 2022.[84]

V MEDIA

The transition from traditional forms of media distribution and consumption towards converged digital media platforms continues to rapidly evolve, with members of the media and entertainment industries grappling with new business models to monetise content and building frameworks to provide sufficient protection for the rights of content creators and consumers alike. The UK government is committed to investing in strong and fast broadband to ensure the audience's ability to consume media at ease. At the same time, the UK's exit from the EU in 2020 means that the UK is no longer party to various EU regulatory regimes and therefore must commit to enhancing its own regulatory framework. In particular, DCMS has been vocal about its commitment to protecting audiences while ensuring the sector remains competitive.[85] Continuous innovation in the music and social media sectors also prompted an increased interest in ensuring the implementation of adequate safety measures online.

82 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.

83 See https://assets.publishing.service.gov.uk/media/634914bd8fa8f5346899531c/Summary_of_provisional_decision_MRN.pdf.

84 See https://assets.publishing.service.gov.uk/media/617fc8e4e90e071981081689/Revised_Administrative_Timetable_290922_MRN.pdf.

85 DCMS White Paper, 'The Government's Vision for the Broadcasting Sector', available at https://www.gov.uk/government/publications/up-next-the-governments-vision-for-the-broadcasting-sector/up-next-the-governments-vision-for-the-broadcasting-sector.

i Investment in strong and superfast broadband and media across the UK

The UK's broadband infrastructure has to be regularly upgraded to accommodate the increasing demand of online content services. One of Ofcom's key priorities in 2022 is investment and innovation in high-quality and reliable communications networks.[86] Thanks to steady investment in the sector, the proportion of homes in the UK that can access gigabit-capable services has increased to 19.3 million homes (66 per cent of all homes), up from 13.7 million homes (47 per cent) in May 2021.[87] This increase has been driven by several factors, including the roll-out of full-fibre broadband, and the actions taken by service provider Virgin Media O2, which made its entire network gigabit capable in December 2021. In February 2022, the UK government set a target for gigabit-broadband to be available in at least 99 per cent of premises by 2030, and to support this target, it has pledged £5 billion in funding to deliver gigabit-broadband to properties not reached by the commercial market.[88]

The government continues to explore ways to ensure superfast broadband is available in the most remote and hardest-to-reach places in the UK. As at May 2022, superfast broadband (download speeds of at least 30Mbit/s) coverage sat at 96 per cent; however, the vast majority (99 per cent) of UK properties can still access broadband of at least 10Mbit/s download and 1Mbit/s upload speed.[89] In addition, mobile operators are rolling out the shared rural network, as agreed with the government in 2020, which will take 4G coverage from 92 per cent to 95 per cent of the UK's landmass by the end of 2025. In addition, 5G coverage is developing, with the government committing to the majority of the population having access to a 5G signal by 2030. Current coverage for both Scotland and Wales is significantly lower than in the rest of the UK; the goal is to achieve between 82 per cent and 85 per cent coverage in Scotland and 85 per cent and 88 per cent coverage in Wales by 2027.[90] While Ofcom had previously noted that full fibre and gigabit-capable networks were at a relatively early stage of rollout, it reported in May 2022 that just under 9.6 million (33 per cent) of UK homes now have access to full fibre connections – an increase of 5 per cent since September 2021.

ii Brexit, the European Convention on Transfrontier Television and media

In May 2016, as part of the Digital Single Market Strategy, the European Commission adopted a legislative proposal to revise the Audiovisual Media Services Directive (AVMSD), the legislation that coordinates national legislation on all audio-visual media including TV broadcasts and on-demand services within the EU. The revised Directive entered into force on 19 December 2018[91] and the UK implemented the revisions to the AVMSD into national law through the Audiovisual Media Services Regulations 2020 (UK AVMS Regulations) on

86 Ofcom's Plan of Work 2022/2023, available at https://www.ofcom.org.uk/consultations-and-statements/category-2/plan-of-work-2022-23.

87 Ofcom's Connected Nations Spring Update, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0031/237865/spring-2022-connected-nations-update.pdf.

88 House of Commons, 'Gigabit-broadband in the UK: Government Targets and Policy', available at https://researchbriefings.files.parliament.uk/documents/CBP-8392/CBP-8392.pdf.

89 Ofcom's Connected Nations Spring Update, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0031/237865/spring-2022-connected-nations-update.pdf.

90 Ofcom's Connected Nations Spring Update, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0031/237865/spring-2022-connected-nations-update.pdf.

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

30 September 2020 (prior to leaving the European Union), which amended the existing UK Broadcasting Acts and the Act.[92] 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 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 audio-visual media services to ensure 30 per cent of the works in their catalogues are European works.

Although the UK has exited the European Union, the definition of European works under the AVMSD includes works of countries that are part of the 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, even after Brexit.

On 31 December 2020, the government published practical guidance on the AVMSD amendments and on the implications of Brexit on broadcasting and video on demand (VOD) services.[93] On 1 January 2021, the AVMSD (including its country of origin principle),[94] ceased to benefit services under UK jurisdiction, and the UK was designated as a third country. 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). The consequence of the UK's new designation was that, by June 2021, the owners of over 250 broadcast licences had decided to move some of their international operations from the UK, moving these operations to alternative countries (such as the Netherlands, Luxembourg and Spain) to maintain their country of origin status within the EU.[95] According to data published by the European Audiovisual Observatory's MAVISE database in Europe, the list of such service providers includes household names such as Discovery, Disney and NBC. However, these companies retained their Ofcom licences in relation to their operations within the UK.

The ECTT remains relevant to the UK, as it is a signatory to the European Convention. The ECTT relies upon the principles of mutual assistance and cooperation between the parties of the Convention. Similar to the AVMSD, the ECTT includes a country of origin

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

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

94 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)).

95 Advanced Television, 'Survey: Brexit drives out 250 broadcast licences', available at https://advanced-television.com/2021/06/17/report-brexit-sees-mass-migration-of-uk-originating-channels/.

principle.[96] The principle means that broadcast providers established in states that are parties to the ECTT do not need a licence from Ofcom to broadcast into countries that are signatories to the Convention (and vice versa). Furthermore, the ECTT framework provides for freedom of reception and retransmission.[97] This means that, broadly speaking, 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 within the EU (Belgium, Denmark, Greece, Ireland, Luxembourg, the Netherlands and Sweden), additional licences and consents are required, subject to local law requirements. Furthermore, VOD services are outside of the scope of the ECTT.

Portability Regulation

On 9 December 2015, the Commission proposed a regulation to enable the cross-border portability of online content services.[98] The resulting Portability Regulation came into force on 1 April 2018, allowing Europeans who purchase or subscribe to audio-visual 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.[99]

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.[100]

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. In January 2020, the government announced that the UK had no plans to implement the Directive.[101] This decision could lead to 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.

96 Explanatory Memorandum to the Broadcasting (Amendment) (EU Exit) Regulations 2019, available at https://www.legislation.gov.uk/uksi/2019/224/pdfs/uksiem_20190224_en.pdf.

97 Article 4 of Council of ECTT.

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

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

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

101 https://questions-statements.parliament.uk/written-questions/detail/2020-01-16/4371.

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[102] 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. 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 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.

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 and Disney+). BBC iPlayer and ITV Hub are examples of broadcaster video on demand (BVoD) platforms, while Netflix, Amazon Prime Video and NowTV are examples of subscription video on demand (SVoD) platforms.

The industry is transforming as the growth of superfast broadband and connected televisions continues to change the ways in which people watch audio-visual content. Ofcom reports that in the year 2021, total television and audio-visual viewing fell from its peak during the 2020 and 2021 covid-19 lockdowns. The average amount of time spent watching television and video content across all devices in 2021 was 5 hours and 16 minutes a day, 25 minutes less than in 2020.[103] 59 per cent of this viewing time was dedicated to broadcast content, whether live television, recorded playback or BVoD. Although there was an inflation of viewing numbers in 2020 (caused by people staying at home during the pandemic restrictions), by the end of 2021, the average amount of time spent watching content from television broadcasters was 3 hours 7 minutes per person per day – a decrease of 9 per cent from 2020.

Similarly, viewership figures of SVoD services also grew in 2020 as a result of the covid-19 lockdowns and restrictions, but by the end of 2021, the viewing time for these services decreased by 6 per cent to 58 minutes a day on average. The number of households using SVoD services began to decline in the second quarter of 2022, because of the rising cost of living in the UK and its subsequent effect on consumer spending.[104] The adoption of multiple SVoD subscriptions within one household has become increasingly common – the proportion of households with access to two or more SVoD services was 46 per cent in the

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

103 Ofcom Media Nations 2022, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0016/242701/media-nations-report-2022.pdf.

104 Ofcom Media Nations 2022, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0016/242701/media-nations-report-2022.pdf.

first quarter of 2022, up from 43 per cent in the last quarter of 2021.[105] The SVoD sector has also significantly changed how audiences first search for something to watch – 40 per cent of online adults and teens aged 13 and above report that, when they do not yet have a specific programme in mind, they usually visit SVoD services first, comparatively to the 37 per cent who try linear tv channels first.[106] It will be useful to monitor these particular viewership figures over time to gauge audience attention and interest.

One category of OTT service that resisted the trend was BVoD viewership, which continues to grow. In 2021, Ofcom reported an increase in viewership of BVoD services of an average of 3 minutes per person per day, to 15 minutes of viewing, compared to 2020.[107]

A total of 32 per cent of online adults in Great Britain (statistics are available for England, Scotland and Wales only) watch short-form video content daily – content located on services such as Facebook, Instagram, TikTok and Snapchat. TikTok in particular, is continuing to grow – by March 2022, nearly 5 million visitors aged 15 to 24 years old spent an average of 57 minutes on TikTok per day. This is partly because TikTok increased the maximum video length of its videos from one minute to three minutes, which resulted in an increase in the average video length of TikTok videos.

In summary, overall viewership of television and video has fallen from its peak during the pandemic, despite the increased viewership of BVoD services. Service providers will need to remain competitive to satisfy today's audience, which is spending more and more time on social media platforms such as TikTok.[108]

iv Content regulation of video-on-demand services

Under Ofcom's regime, VOD services in the UK are not regulated to the same extent as UK linear television channels. For instance, while Ofcom regulates editorial content on UK VoD services, Ofcom's Broadcasting Code (which provides for audience protection from 'harmful and inoffensive material') does not apply to VoD services (other than BBC iPlayer). In addition, Ofcom is only able to regulate a service if both its head office and editorial decision-making function are in the UK. Following Brexit and the UK's withdrawal from the AVMSD regime in 2021, EU-based VoD services such as Netflix (whose European operations are based in the Netherlands) are no longer subject to any regulatory framework in relation to UK audiences. The UK government considers it necessary to protect audiences from harmful material and regulate the way audiences consume content from VoD providers. Thus, in August 2021, the UK government launched an 8-week consultation on audience protection standards on VoD services. The consultation considered whether UK audiences viewing VoD content (for example on Netflix or Amazon Prime Video) should receive the same or similar level of protections as if they were watching linear television channels.[109] After

105 BARB Establishment Survey, available at https://www.barb.co.uk/news/barb-releases-establishment-survey-data-for-q1-2022/.

106 Ofcom Media Nations 2022, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0016/242701/media-nations-report-2022.pdf.

107 Ofcom Media Nations 2022, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0016/242701/media-nations-report-2022.pdf.

108 Ofcom Media Nations 2022, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0016/242701/media-nations-report-2022.pdf.

109 Available at https://www.gov.uk/government/consultations/audience-protection-standards-on-video-on-demand-services/outcome/government-response-to-the-consultation-on-audience-protection-standards-on-video-on-demand-services.

receiving the responses to the consultation, the UK government declared its intention to introduce 'light-touch' legislation to give Ofcom the powers to draft and enforce a new VoD Code, which would be similar to the Broadcasting Code. The purpose of a new VoD Code is to ensure that all television-like content, no matter how it is consumed, will be subject to similar standards.[110]

The UK government's stated intention is to protect consumers from harmful material and so the proposed VoD Code will be targeted at the larger VoD providers, who will be subject to enhanced regulation by Ofcom. Under the VoD Code, these services are expected to have the same or similar obligations as the traditional linear television broadcasters, such as protecting against harmful materials, and providing their audiences with the ability to air complaints directly to Ofcom. Ofcom is expected to be equipped with an enhanced, ongoing duty to assess on-demand providers' audience protection measures – this is to ensure that the systems put in place by the VoD providers are effective and fit for purpose. The UK government has not yet set the exact parameters of which 'large' VoD providers will be brought under regulation, although Apple TV+ and Netflix are named in the government report.[111] While the parameters of the anticipated VoD Code are set out initially as part of the government's response to the consultation on audience protection standards on VoD services, the government has indicated that further detail will be provided before 2023 as part of a wide-ranging white paper into the future of broadcasting.

v Music

The music industry is generally less regulated than the rest of the media and entertainment sector discussed. Whilst music licensing can be complex,[112] music is not otherwise regulated by Ofcom.

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,

110 DCMS Consultation Outcome: Audience Protection Standards on Video-on-Demand Services, available at https://www.gov.uk/government/consultations/audience-protection-standards-on-video-on-demand-services/audience-protection-standards-on-video-on-demand-services.

111 DCMS Consultation Outcome: Audience Protection Standards on Video-on-Demand Services, available at https://www.gov.uk/government/consultations/audience-protection-standards-on-video-on-demand-services/audience-protection-standards-on-video-on-demand-services.

112 A licence is required to be obtained to play recorded music in public and as part of an audio-visual or radio broadcast. Collecting societies – Performing Right Society Limited (PRS), Phonographic Performance Limited (PPL) and Mechanical-Copyright Protection Society (MCPS) – deal with granting licences on behalf of copyright owners and performers individually to all those who seek them. Following a joint venture in 2018 between PRS and PPL (PRS for Music), the licensing process has been streamlined, and a single licence (TheMusicLicence) can now be obtained from one entity. PRS for Music also provides certain of its management and administrative services to MCPS. However, the underlying tariffs to be applied are still determined by each collecting society separately.

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.[113]

Regulators are taking a keener interest in the sector now. In July 2021, the House of Commons DCMS Committee (Select Committee) 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 introduce legislation so that performers enjoy the right to equitable remuneration for streaming income;

b refer the industry to the CMA to undertake a 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' that the Select Committee identified.[114]

Following the government report, in January 2022, the CMA launched a market study into music and streaming.[115] The purpose of the study is to determine whether the sector is operating in the interest of consumers and whether competition is functioning well, by examining the music value chain (from the deals between artists and record labels through to music streaming services). In July 2022, the CMA published an update paper setting out its interim findings that the market is, on balance, delivering good outcomes for consumers.[116] Given that the focus of the CMA's market study is on competition, the update paper does not cover in detail the other recommendations in the Select Committee's report. For example, the update paper notes that the government is separately carrying out research on remuneration models (including equitable remuneration) in response to recommendations from the Select Committee. With respect to user-uploaded content (UUC) platforms and the music streaming 'value gap', the update paper sets out the CMA's preliminary view that any market distortions are unlikely to lead to substantial competition concerns. The update paper further indicates that the CMA plans to collect additional evidence on this topic and then feed its findings into the government's research, to inform decisions about any legislative changes to safe harbour protections for UUC platforms. The CMA is proposing not to make a market investigation reference and has solicited comments on this proposal. The CMA is scheduled to publish its final report for the market study by the end of January 2023.[117]

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

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

115 See https://www.gov.uk/government/news/cma-launches-probe-into-music-streaming-market.

116 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1093698/220726_Music_and_streaming_-_update_paper.pdf.

117 Amended EPG Code available at https://www.ofcom.org.uk/__data/assets/pdf_file/0025/154384/annex-5-epg-code-appropriate-prominence-provisions.pdf. See https://www.gov.uk/cma-cases/music-and-streaming-market-study#administration-timetable.

vi PSBs

In April 2022, the UK government published its White Paper 'Vision for the Broadcasting Sector', which described the UK's PSBs as the heart of a diverse broadcasting ecosystem and the key to the sector's success.[118]

The White Paper set out how the government plans to ensure that public service broadcasting is strengthened over the next decade and beyond. The White Paper sets out recommendations for modernising the current framework to deliver public service media for audiences watching broadcast TV and online.[119] Following recommendations made by Ofcom to the government in July 2021,[120] the government announced its intention to introduce a new framework, which would establish clear goals for public service media providers, with greater choice over how they achieve them and this new system should ensure public service media remains prominent so audiences can readily find it. There are six PSBs in the UK – three are publicly owned (the BBC, Channel 4 and the Welsh channel S4C) and three are privately owned (ITV, STV and Channel 5). The public service remit of these PSBs was introduced within the Communications Act in 2003, and it includes a set of 14 overlapping 'purposes and objectives', which the relevant authorities now consider outdated. The government intends to replace these with a new, shorter remit, that will give the PSBs greater flexibility in how they deliver their content to audiences, while guaranteeing that effective options are available should an intervention become necessary. An example of such change relates to the 'prominence' framework, whereby Ofcom sets broadcasting rules in relation to linear broadcasting that controls the prominence of these channels on the television (i.e., the channel number order). This framework is essential to the success of PSBs, as it boosts viewership and engagement. However, the prominence framework does not yet apply to the PSB's on-demand services. Based on recommendations from the DCMS Select Committee and Ofcom in 2019 and 2021,[121] the government proposed a new principle-based legislative framework, whereby the providers of designated TV platforms will be required to designate prominence to the PSBs' on-demand services. According to the government, this new prominence regime will incorporate rules that require (1) PSB providers to offer their on-demand services to platforms, and (2) the platforms to carry these on-demand services. This new regime will be enforced by Ofcom, which will regulate the process and develop and maintain guidance on the framework.

The White Paper also expanded on the government's plans to transfer the ownership of one of the PSBs, Channel 4, to a private owner. The prevailing argument is that the channel's public ownership model is 'constraining its ability to respond to the challenges and opportunities' of the changing broadcasting market in the long term. Having greater access to capital and the ability to produce and sell its own content, the government argues, will give Channel 4 the best range of tools to succeed in the long term.[122] The government

118 DCMS White Paper, 'The Government's Vision for the Broadcasting Sector', available at https://www.gov.uk/government/publications/up-next-the-governments-vision-for-the-broadcasting-sector/up-next-the-governments-vision-for-the-broadcasting-sector.

119 ibid.

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

121 DCMS, the Future of Public Service Broadcasting Inquiry.

122 DCMS White Paper, 'The Government's Vision for the Broadcasting Sector', available at https://www.gov.uk/government/publications/up-next-the-governments-vision-for-the-broadcasting-sector/up-next-the-governments-vision-for-the-broadcasting-sector.

intends to sell Channel 4 to a private owner, and re-invest the proceeds from this sale into the sector. The proposal was met with opposition across party lines in Parliament, as well as the executives at Channel 4. However, this plan was proposed under Boris Johnson's premiership in April 2022, but both Liz Truss and Rishi Sunak, the subsequent UK Prime Ministers, have been reluctant to endorse this plan once in power. In November 2022, the *Financial Times* reported that the Sunak government will want to 'quietly drop privatization' of Channel 4.[123] Although Sunak supported the decision to privatise Channel 4 during his leadership campaign, he has since communicated that he wishes to review some of his campaign pledges, including the proposed sale of Channel 4. It remains to be seen whether the government will move ahead with the plans to sell Channel 4.

VI THE YEAR IN REVIEW

Towards regulated digital services?

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

a the US Congress has been considering multiple pieces of legislation focused on digital markets, including the American Innovation and Choice Online Act sponsored by Senator Amy Klobuchar;[124]

b the ACCC is currently conducting a digital platform services inquiry, which will conclude in 2025,[125] and it recently published a final report concluding its digital advertising services inquiry,[126] which includes a number of recommendations relating to data portability and interoperability, as well as the ad tech supply chain; and

c 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'.[127] The BKartA has since designated three companies as having this status.[128]

VII CONCLUSIONS AND OUTLOOK

In addition to initiatives to regulate digital markets such as those outlined above, the areas of data privacy and cyber security remain subject to extensive regulatory scrutiny, and significant ongoing debate both inside and outside the courtroom. The government's proposed reform of the UK data protection regime, and focus on developing the UK's cyber security frameworks,

123 https://www.ft.com/content/2898cce0-42b0-4e5e-b59a-46996229061a.

124 See https://www.congress.gov/bill/117th-congress/senate-bill/2992/text.

125 See https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025.

126 Available at https://www.accc.gov.au/system/files/Digital%20advertising%20services%20inquiry%20-%20final%20report.pdf.

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

128 See https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/06_07_2022_Amazon.html.

has the potential to significantly change the data protection and security landscape for the future, and introduce divergence between the UK and EEA regimes. Much debate and controversary have also surrounded the proposed online harms regime and the issue of liability for content online; these areas are likely to remain unsettled for online platforms and providers over the course of 2023 and beyond.

With regard to the media and entertainment industries in the UK, the rise in popularity of SVoD services continues, but it does not appear likely that viewership will return to its pandemic levels. At the same time, the music streaming industry continues to grow, resulting in increased returns for labels, songwriters and owners of music catalogues.

ISBN 978-1-80449-141-6