The Technology, Media and Telecommunications Review

Eighth Edition

Editor
John P Janka

The Law Reviews

© 2017 Law Business Research Ltd

The Technology Media and Telecommunications Review

Eighth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2017
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
John P Janka

The LawReviews

© 2017 Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

ACCOUNT MANAGERS
Pere Aspinall, Sophie Emberson,
Laura Lynas, Jack Bagnall

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Arthur Hunter

EDITORIAL COORDINATOR
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Robbie Kelly

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK
© 2017 Law Business Research Ltd
www.TheLawReviews.co.uk

No photocopying: copyright licences do not apply.
The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of November 2017, be advised that this is a developing area.
Enquiries concerning reproduction should be sent to Law Business Research, at the address above.
Enquiries concerning editorial content should be directed
to the Publisher – gideon.roberton@lbresearch.com

ISBN 978-1-910813-90-4

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

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

© 2017 Law Business Research Ltd

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC–PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

THE ISLAMIC FINANCE AND MARKETS LAW REVIEW

THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW

THE CONSUMER FINANCE LAW REVIEW

THE INITIAL PUBLIC OFFERINGS REVIEW

THE CLASS ACTIONS LAW REVIEW

THE TRANSFER PRICING LAW REVIEW

THE BANKING LITIGATION LAW REVIEW

THE HEALTHCARE LAW REVIEW

THE PATENT LITIGATION LAW REVIEW

www.TheLawReviews.co.uk

© 2017 Law Business Research Ltd

ACKNOWLEDGEMENTS

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

ABOU JAOUDE & ASSOCIATES LAW FIRM

ADVAITA LEGAL

BAKER & McKENZIE.WONG & LEOW

CLEARY GOTTLIEB STEEN & HAMILTON LLP

CMS

COELHO RIBEIRO & ASSOCIADOS

DNFP IN ASSOCIATION WITH HOGAN LOVELLS

ELVINGER HOSS PRUSSEN

HOGAN LOVELLS BSTL, SC

KT LAW ASSOCIATES

LATHAM & WATKINS LLP

LEE AND LI, ATTORNEYS-AT-LAW

NIEDERER KRAFT & FREY LTD

PINHEIRO NETO ADVOGADOS

UDO UDOMA & BELO-OSAGIE

ÜNSAL GÜNDÜZ

URÍA MENÉNDEZ

WEBB HENDERSON

WOLF THEISS

ZHONG LUN LAW FIRM

© 2017 Law Business Research Ltd

CONTENTS

PREFACE vii
John P Janka

LIST OF ABBREVIATIONS ix

Chapter 1 AUSTRALIA 1
Angus Henderson, Richard Dampney and Stephen Coudounaris

Chapter 2 BRAZIL 16
Raphael de Cunto and Beatriz Landi Laterza Figueiredo

Chapter 3 BULGARIA 28
Anna Rizova and Oleg Temnikov

Chapter 4 CHINA 42
Jihong Chen

Chapter 5 EU OVERVIEW 54
Marco D'Ostuni, Gianluca Faella and Manuela Becchimanzi

Chapter 6 FRANCE 73
Myria Saarinen and Jean-Luc Juhan

Chapter 7 GERMANY 90
Christian Engelhardt

Chapter 8 HONG KONG 107
Simon Powell and Chi Ho Kwan

Chapter 9 INDIA 123
Atul Dua and Anuradha

© 2017 Law Business Research Ltd

Chapter 10 INDONESIA......136
Aston Goad, Indra Dwisatria and Randy Rifdaan

Chapter 11 ITALY......148
Marco D'Ostuni, Marco Zotta and Manuela Becchimanzi

Chapter 12 JAPAN......167
Hiroki Kobayashi and David Lai

Chapter 13 KENYA......185
Brian Tororei

Chapter 14 LEBANON......197
Simon El Kai, Souraya Machnouk, Hachem El Housseini and Ziad Maatouk

Chapter 15 LUXEMBOURG......210
Linda Funck

Chapter 16 MEXICO......232
Federico Hernández Arroyo

Chapter 17 NIGERIA......243
Olajumoke Lambo and Godson Ogheneochuko

Chapter 18 PORTUGAL......252
Jaime Medeiros, Mónica Oliveira Costa and Ana Ramos Logrado

Chapter 19 RUSSIA......271
Maxim Boulba and Elena Andrianova

Chapter 20 SINGAPORE......281
Ken Chia and Daryl Seetoh

Chapter 21 SPAIN......307
Pablo González-Espejo

Chapter 22 SWITZERLAND......321
András Gurovits and Clara-Ann Gordon

Chapter 23 TAIWAN......338
Patrick Marros Chu, Vick Chien and Sam Huang

© 2017 Law Business Research Ltd

Chapter 24 TURKEY....349
Burçak Ünsal and Okan Gündüz

Chapter 25 UNITED KINGDOM....367
John D Colahan, Gail Crawford and Lisbeth Savill

Chapter 26 UNITED STATES....413
John P Janka and Jarrett S Taubman

Appendix 1 ABOUT THE AUTHORS....435

Appendix 2 CONTRIBUTING LAW FIRMS' CONTACT DETAILS....455

© 2017 Law Business Research Ltd

PREFACE

This fully updated eighth edition of *The Technology, Media and Telecommunications Review* provides an overview of evolving legal constructs in 26 jurisdictions around the world. It is intended as a business-focused framework for both start-ups and established companies, as well as an overview for those interested in examining evolving law and policy in the rapidly changing TMT sector.

Broadband connectivity and wireless services continue to drive law and policy in this sector. The disruptive effect of new technologies and new ways of communicating creates challenges around the world as regulators seek to facilitate the deployment of state-of-the-art communications infrastructure to all citizens and also to use the limited radio spectrum more efficiently than before. At the same time, technological innovation makes it commercially practical to use large segments of 'higher' parts of the radio spectrum for the first time. Moreover, the global nature of TMT companies compels them to address these issues in different ways than before.

A host of new demands, such as the developing internet of things, the need for broadband service to aeroplanes, vessels, motor vehicles and trains, and the general desire for faster and better mobile broadband service no matter where we go, create pressures on the existing spectrum environment. Regulators are being forced to both 'refarm' existing spectrum bands, so that new services and technologies can access spectrum previously set aside for businesses that either never developed or no longer have the same spectrum needs; and facilitate spectrum sharing between different services in ways previously not contemplated. Many important issues are being studied as part of the preparation for the next World Radio-communication Conference to be held in 2019. No doubt, this Conference will lead to changes in long-standing radio spectrum allocations that have not kept up with advances in technology, and it should also address the flexible ways that new technologies allow many different services to co-exist in the same segment of spectrum.

Legacy terrestrial telecommunications networks designed primarily for voice are being upgraded to support the broadband applications of tomorrow that will extend economic benefits, educational opportunities and medical services throughout the world. As a result, many governments are investing in or subsidising broadband networks to ensure that their citizens can participate in the global economy, and have universal access to the vital information, entertainment and educational services now delivered over broadband. Many governments are re-evaluating how to regulate broadband providers, whose networks have become essential to almost every citizen. Convergence, vertical integration and consolidation also lead to increased focus on competition and, in some cases, to changes in the government bodies responsible for monitoring and managing competition in the TMT sector. Similarly,

© 2017 Law Business Research Ltd

many global companies now are able to focus their regulatory activities outside their traditional home, and in jurisdictions that provide the most accommodating terms and conditions.

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

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

I would like to take the opportunity to thank all of the contributors for their insightful contributions to this publication, and I hope you will find this global survey a useful starting point in your review and analysis of these fascinating developments in the TMT sector.

John P Janka
Latham & Watkins LLP
Washington, DC
October 2017

© 2017 Law Business Research Ltd

Chapter 25

UNITED KINGDOM

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

I OVERVIEW

The Office of Communications (Ofcom) and the Communications Act 2003 (Act) regulate the UK communications landscape. Ofcom's current priorities are set out in its 2017–18 Annual Plan.[2] They include the implementation of the conclusions from Ofcom's 'Digital Communications Review', completing the integration of Ofcom's new responsibilities for regulating the BBC and awarding further mobile spectrum licences. European Commission (Commission) Digital Single Market (DSM) proposals (set out in more detail in Sections II.v and V.iv) promise to make significant changes to the UK communications landscape, if adopted in their current form and subject to longer-term changes to national legislation as a result of Brexit.

European law and standards currently govern the UK data protection framework and impose compliance obligations on organisations that process personal data. These rules apply broadly to, *inter alia*, the collection, use, storage and disclosure of personal data. In general, personal data are defined as information relating to an identified or identifiable natural person who can be identified directly or indirectly from that data (e.g., names, contact information, or sensitive personal data such as health data).

These laws and regulations are subject to substantial change as a result of the adoption of the General Data Protection Regulation (GDPR). The GDPR is due to come into force on 25 May 2018 across Europe. The UK government tabled in Parliament its draft implementing legislation – the Data Protection Bill – in September 2017. This and other EU data and cyber-related legislation are either scheduled to come into force on the same date or will adopt similar mechanisms of enforcement as the GDPR (i.e., antitrust-like fines relating to a percentage of global turnover). This will be the case even after Brexit, as the UK government has committed to strive to achieve equivalent standards for data protection in the UK post-Brexit.

II REGULATION

i The regulators

Ofcom is the independent communications regulator in the UK. The Department for Culture, Media and Sports (DCMS) remains responsible for certain high-level policy formulation

1 John D Colahan, Gail Crawford and Lisbeth Savill are partners at Latham & Watkins LLP. The authors would like to acknowledge the kind assistance of their colleagues Mark Sun, Frances Stocks Allen, Danielle van der Merwe, Rachael Hammond, Alexandra Luchian, Ashleigh Humphries, Elizabeth Longster, Emma Pianta and Caroline Omotayo in the preparation of this chapter.

2 Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0027/99621/Annual-Plan-2017-18.pdf.

© 2017 Law Business Research Ltd

and the promulgation of legislation (a role performed by the Department for Business, Innovation and Skills before 2011), but most key policy initiatives are constructed and pursued by Ofcom. Ofcom has largely delegated its duties for radio and TV advertising to the Advertising Standards Authority (ASA), and a number of new regulatory bodies have been established within the ASA (such as the Broadcast Committee of Advertising Practice). On 1 November 2014, Ofcom renewed its 10-year contract with the ASA until 2024,[3] with only minor changes from the previous contract. The changes were mainly intended to recognise established practices agreed between Ofcom and the ASA since the initial implementation of the co-regulatory system.

Ofcom's principal duty 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 by making communication markets work for everyone. This is enshrined in Ofcom's three main objectives: '(1) to promote competition and ensure that markets work effectively for consumers;[4] (2) to secure standards and improve quality; and (3) to protect consumers from harm.'[5]

Ofcom's priorities and major work areas (which in some cases underpin the three key objectives) for the year are set out below:

a Promote competition and ensure that markets work effectively for consumers:
- enabling competing operators to invest in super and ultra-fast fixed-line networks;
- strengthening Openreach's[6] strategic and operational independence from BT;
- overseeing the transition to the new model of legal separation notified by BT in March 2017;
- ensuring that European regulatory frameworks work for the UK;
- promoting competition in fixed-line services;
- making available better, more granular information for people and businesses in respect of availability, speed, quality of service and pricing of communications services; and
- ensuring fair and effective competition to deliver a wide range of high quality and varied content for broadcasting audiences.

b Secure standards and improve quality:
- improving the coverage of fixed and mobile communications services to meet the needs of people and businesses across the UK;
- improving the quality of service in fixed and mobile telecommunications services for consumers and businesses;
- implementing any government decision on a broadband USO;

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

4 Ofcom has concurrent powers to apply competition law along with the primary UK Competition Law Authority, the Competition and Markets Authority (CMA). Enhanced concurrency arrangements came into effect on 1 April 2014 with the objective of increasing the enforcement of competition law in the regulated sectors by strengthening the cooperation between the CMA and sector regulators, including Ofcom, referred to as concurrency. The most recent Annual Report on concurrency was published by the CMA on 28 April 2017, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/611593/annual-concurrency-report-2017-cma63.pdf.

5 Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0027/99621/Annual-Plan-2017-18.pdf

6 Openreach is part of the BT Group and develops and maintains the UK's main telecoms network.

© 2017 Law Business Research Ltd

- increasing the capacity of mobile networks by ensuring sufficient spectrum is available;
- securing quality in public service broadcasting (PSB); and
- ensuring broadcasting represents and accurately portrays UK society.

c Protect consumers from harm:
- addressing nuisance calls;
- continuing to respond to emerging consumer issues in relation to harmful content in TV, radio and on-demand services; and
- ensuring landline-only customers get value for money from voice services.

Ofcom's specific statutory duties fall into five main areas:

a ensuring the optimal use of the radio spectrum;

b ensuring that a wide range of electronic communications services – including high-speed data services – are available throughout the UK;

c ensuring plurality in the provision of broadcasting and a wide range of TV and radio services of high quality and broad appeal;

d securing the USO on postal services within the jurisdiction; and

e applying adequate protection for audiences against offensive or harmful material, and unfairness or the infringement of privacy.

On 25 February 2016, Ofcom published the initial conclusions of its overarching review of the UK's digital communications first announced on 11 March 2015.[7] This was Ofcom's second major assessment of the telecommunications sector: the first began in December 2003 and concluded in September 2005, and was the first of its kind in 10 years. The review encompassed two discrete phases. Phase one focused on evidence gathering and understanding experiences of digital communications. Ofcom started the first phase in July 2015 by publishing a discussion paper.[8] The second phase of the review resulted in initial conclusions focusing on six fundamental measures intended to facilitate the development of the UK communications market:

a universal availability of fixed and mobile services: the government consulted on this issue between July 2017 and October 2017. Following the consultation, the government now intends to make a decision as to the best route to deliver universal broadband;

b strategic shift to large-scale fibre deployment: Ofcom believes the key incentive for investment and innovation is to stimulate network-based competition to encourage improvements to current networks and the formulation of new network infrastructure;

c a step change in the quality of service: Ofcom identifies that the most-commented-upon issue throughout the conduct of this review was in relation to the quality of service;

d significantly strengthening the independence of Openreach: notwithstanding the functional separation of BT in 2005, Ofcom notes that the BT Group continues to exercise control over the strategic decision making and budget apportioned to the part of its network reserved for competitors;

7 Available at: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/digital-comms-review.

8 Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/63444/digital-comms-review.pdf.

© 2017 Law Business Research Ltd

e empowering and protecting consumers: against a backdrop of increasing diversity and expansion within the communications market, Ofcom is mindful of the need to provide clear and accurate information to consumers to enable informed choices on the best packages for their needs; and

f simplifying and removing unnecessary regulation: Ofcom reiterates its fundamental principle of non-interference except where strictly necessary and the promotion of deregulation where feasible. In this regard, Ofcom has introduced proposals to deregulate the market for central London business connections due to the plethora of competition.

The next steps set out in phase two were, as follows, to implement the proposed measures through the usual mechanism of regular reviews of individual markets and likewise to implement specific dedicated projects. Specific dedicated projects that have been envisaged or undertaken include:

a Ofcom working with the government to introduce the new universal right to broadband;

b Ofcom continuing to provide accurate, comparable, accessible and increasingly granular coverage information, published in its Connected Nations 2016 report;

c Ofcom using its power to require operators to improve mobile coverage, for example by including licence conditions on population and geographic coverage for new spectrum releases;

d Ofcom working with BT and industry to make BT's underground duct system more easily accessible to competitors. Ofcom will implement these changes through the Civil Infrastructure Directive and UK transposition legislation, which came into effect on 31 July 2016. Ofcom has also made specific proposals for improving access in its Wholesale Local Access Market Review. Ofcom will also use this Review to implement regulated access and pricing policies to support investment in access networks;

e Ofcom setting tough minimum standards for Openreach in the business market with rigorous enforcement and fines for underperformance. Ofcom fined Openreach £42 million in March 2017 for breaching contracts with telecoms providers;

f Ofcom published the first annual Report of Service Quality in 2017;

g Ofcom extending minimum standards, and introducing rules to incentivise Openreach to go beyond minimum standards and deliver better service. These rules were introduced in 2016, and have been consulted on throughout Ofcom's Wholesale Local Access Market Review, which took place from March 2017 until June 2017. The results of this Review will be published early 2018 with new measures resulting from this, taking effect in April 2018;

h Ofcom setting up a working group with the communications industry to coordinate better service quality;

i Ofcom consulting on the introduction of automatic compensation for consumers and small businesses;

j Ofcom developed detailed proposals on Openreach independence and discussed these proposals with the Commission in 2016;

k Ofcom working with industry and third parties (e.g., price comparison sites) to improve the level of information available to consumers, and exploring a requirement for providers to publish a standard cost comparison measure alongside their tariffs;

© 2017 Law Business Research Ltd

l Ofcom consulted on mobile switching in the first half of 2016, and completed a qualitative research piece on switching triple-play services (phone line, TV, broadband), in July 2016; and
m Ofcom consulted on proposals to streamline and update the General Conditions in summer 2016, with proposals to be finalised. Ofcom will also consider the scope for deregulation in one of every four market reviews.

The discussion paper also provided insight into future policy challenges across fixed, mobile and content sectors, including:
a investment and innovation, delivering widespread availability of services. Ofcom deduced that a strategy must be implemented that offers appropriate incentives to stimulate private investment and innovation to ensure a diverse range of services are readily available. The strategy should also consider what needs to be done to ensure services are available in less commercially viable regions;
b sustainable competition, delivering choice, quality and affordable prices. In general, Ofcom believes that the best mechanism for delivering choice, quality and affordable prices is a healthy competitive market. It will continue to encourage this through regulation that protects both competition and incentives for efficient investment;
c empowered consumers, able to take advantage of competitive markets. Competition is only effective when consumers are equipped to make an informed decision and can easily act on that information to make a switch if they want to; and
d targeted regulation where necessary with deregulation elsewhere. Regulation works best when it is targeted where it is needed, and removed where it is not required.[9]

In addition, the Body of European Regulations in Electronic Communications (BEREC), formed after the adoption of Regulation (EC) 1211/2009,[10] is now playing an increasingly significant role at a European level. The BEREC replaces the European Regulators Group, and acts as an exclusive forum and vehicle for cooperation between national regulatory authorities (NRAs) and between NRAs and the Commission.

The prevailing regulatory regime in the UK is contained primarily in the Act, which entered into force on 25 July 2003. Broadcasting is regulated under a separate part of the Act in conjunction with the Broadcasting Acts of 1990 and 1996. Other domestic legislation also affects this area, in particular:
a the Wireless Telegraphy Act 2006;
b the Digital Economy Act 2010;
c the Data Protection Act 1998;
d the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011);
e the Freedom of Information Act 2000;
f the Regulation of Investigatory Powers Act 2000;
g the Data Retention and Investigatory Powers Act 2014 (DRIPA);
h the Enterprise Act 2002;

9 Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/63444/digital-comms-review.pdf.
10 Regulation (EC) No. 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing BEREC and the Office.

© 2017 Law Business Research Ltd

i the Copyright, Designs and Patents Act 1988;
j the Digital Economy Act 2017 (DEA); and
k the Competition Act 1998.

Following the review of the European Framework for Electronic Communications Regulation (Revised Framework),[11] the government adopted the Electronic Communications and Wireless Telegraphy Regulations 2011 on 4 May 2011, which amended the Act, the Wireless Telegraphy Act 2006 and other primary and secondary legislation, and implemented most aspects of the EU Better Regulation Directive (2009/140/EC)[12] and the Citizens' Rights Directive (2009/136/EC).[13]

The wholesale reform of the European data protection regime continues following the release in 2012 of a Draft General Data Protection Regulation. On 15 December 2015, the European Parliament and the Council reached a conclusive consensus on the EU data protection reform package, and in April 2016 the European Parliament and Council adopted the final version of the Draft Data Protection Regulation (General Data Protection Regulation) and the final version of the Data Protection Directive for police and judicial cooperation on criminal matters. The formal adoption of the EU data protection reform package and its applicability in all Member States from 25 May 2018 marks the end of disparate data protection rules across the EU.[14]

In May 2011, the DCMS also launched a review of communications regulation intended to lead to a new communications regulatory framework to be in place by 2015. It focused on three key aspects: (1) growth innovation and deregulation; (2) a communications infrastructure that provides the foundations for growth; and (3) creating the right environment in which the content industry may thrive. In June 2012, the DCMS announced that, following responses to its May 2011 review, it had concluded that a complete overhaul of the legislation was not required, but it recognised the need to update the regulatory framework to ensure that it is fit for the digital age. To inform the development of the regulatory framework, the government held a range of seminars to obtain industry and public opinion on topics including driving investment in TV content, competition in the content market, the consumer perspective, maximising the value of spectrum and supporting growth in the radio sector. It was originally anticipated that the DCMS would publish a white paper in the early part of 2013 with a communications bill to follow shortly thereafter. In July 2013, the DCMS published a policy paper titled 'Connectivity, content and consumers – Britain's

11 Available at: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf.

12 Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

13 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

14 Available at: http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

© 2017 Law Business Research Ltd

digital platform for growth' (Strategy Paper).[15] In line with the government's view that a large-scale overhaul of the existing legislation is unnecessary, the Strategy Paper focused on specific and incremental legislative changes to a number of areas, including the following:

a a consumer rights bill introducing a new category of digital content in consumer law, together with a set of statutory rights for the quality standards that this content should meet, and the remedies available to consumers when digital content does not meet these standards;

b changes to improve spectrum management and amendments to the Wireless Telegraphy Act 2006;

c amending the Electronic Communications Code (ECC) to make it easier for communications companies to use land for broadband infrastructure; and

d scaling back Ofcom's duty to review PSB at least every five years and draft PSB reports.

Following on from the above, the Consumer Rights Act 2015 introduced rights in respect of the quality of digital content and digital services. The Act received royal assent on 26 March 2015 and came into force in stages; the Act is now fully in force. The main provisions of the Consumer Rights Act 2015, including those relating to goods, services and digital content, came into force on 1 October 2015.

The DCMS issued its spectrum management strategy in March 2014, recognising the need for, among other things:

a a uniform system for the valuation of spectrum to set licence fees;

b the government to work together with Ofcom to encourage efficient use of spectrum, in particular in the release of spectrum, the transfer of spectrum and the assignment of spectrum to new users;

c encouragement of innovation; and

d a strategy to address increased demands on spectrum that will evolve from the growth of the 'internet of things' (IoT), machine-to-machine (M2M) communication and 5G.

The DCMS's strategy was followed in April 2014 by Ofcom's spectrum management strategy, discussed in more detail below.

A proposal to reduce Ofcom's duty to review public service broadcasters (PSBs), such that the duty would arise only upon the demand of the Secretary of State, was withdrawn in February 2014. Ofcom published the findings of its third review of PSBs on 2 July 2015. It found that overall, despite declining spending levels, PSBs continue to provide programmes that are highly valued by audiences.

In August 2014, the DCMS issued a consultation paper[16] seeking input on the goals and policies set out in a July 2013 report entitled 'Connectivity, content and consumers – Britain's digital platform for growth', which was explored further within a framework published in February 2014. The results of this consultation were used to develop the government's digital communications infrastructure strategy, which was published on 18 March 2015.[17]

15 Available at: www.gov.uk/government/publications/connectivity-content-and-consumers-britains-digital-platform-for-growth.

16 Available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/346054/DCIS_consultation_final.pdf.

17 Available at: www.gov.uk/government/publications/the-digital-communications-infrastructure-strategy/the-digital-communications-infrastructure-strategy.

© 2017 Law Business Research Ltd

This publication noted that these papers would all culminate in a formal review in 2018 to oversee the rapid pace of change that has taken place over the past five years. For the last few years, the government has made commitments in relation to broadband infrastructure, in particular superfast broadband, connectivity in rural areas and the delivery of mobile broadband connectivity. One step towards this objective came in the form of the Digital Economy Act, which received royal assent in April 2017. This allowed the development of a new broadband USO, giving every household and business a right to request a connection at a minimum speed of 10Mbps, regardless of geographical location. The government is currently consulting on the specific structure and design of the USO, which will eventually be laid out in secondary legislation.[18] As part of its focus on ensuring that the UK becomes a 'leading digital nation', the government has set up a Ministerial Digital Taskforce to develop networks, including infrastructure.

The DCMS published a consultation on 26 March 2015[19] on three areas of broadcasting regulation: the defence against copyright infringement in Section 73 of the Copyright, Designs and Patents Act 1988; the must-offer and must-carry provisions applicable to PSBs and ECNs respectively in the Act; and the rules on electronic programme guide prominence. On 5 July 2016, the government responded to the DCMS consultation.[20] The government response sets out that deregulation of the must-offer and must-carry legislation in the Act is not desirable and would risk endangering the balance of relationships between stakeholders. The government goes on to conclude that commercial PSBs are fairly compensated for their licensed PSB channels and that there should continue to be no net payments between platform operators and PSBs for carriage of their licensed PSB channels.

The government eventually repealed Section 73 of the Copyright, Designs and Patents Act 1988, which provided that copyright in a broadcast of PSB services (and any work in the broadcast) retransmitted by cable was not infringed where the broadcast was receivable in the area in which it was retransmitted. This was designed to ensure the retransmission of public service broadcasts in areas with poor aerial receptions. However, on consultation, all of the PSBs were in favour of the repeal, believing the repeal of Section 73 was a prerequisite for allowing PSBs to receive payments from the cable networks as compensation for the benefits they bring to them. The government believes that the repeal of Section 73 will have the simultaneous effect of closing the loophole used by providers of internet-based live streaming services by ensuring that such services cannot exploit PSB content without any benefit flowing to the PSBs. It remains to be seen whether the new regulatory framework will ensure a zero net fee position, or whether it will result in commercial PSBs seeking retransmission fees and subsequently lead to disputes. The repeal of Section 73 is dealt with in Section 34 of the DEA. Section 34 came into force on 31 July 2017 pursuant to the Digital Economy Act 2017 (Commencement No. 1) Regulations 2017.

With regard to the ECC, in December 2014 the government proposed to introduce a new code. This proposal was subsequently withdrawn in January 2015 following representations

18 Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/634016/USO_consultation_document.pdf.

19 Available at: www.gov.uk/government/consultations/the-balance-of-payments-between-television-platforms-and-public-service-broadcasters-consultation-paper.

20 Available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/534872/The_balance_of_payments_between_television_platforms_and_public_service_broadcasters_consultation_report___1_.pdf.

© 2017 Law Business Research Ltd

from stakeholders on the practical application of the proposed revised code. The government agreed to consult further. The DCMS published proposals in May 2016 after a consultation in 2015[21] (which closed on 30 April 2015) on reforming the ECC, focusing on:

a the definition of land and ownership;
b how consideration is to be determined;
c upgrading and sharing apparatus;
d contracting out the revised code;
e the role of land registration; and
f transitional arrangements, savings and retrospectivity.

The assent of the Digital Economy Act and the discussions as part of this assent further advocated the policy of reforming the ECC. In consultation, it was suggested that the adoption of the Bill would result in wide-ranging amendments to the ECC, most significantly new obligations on Ofcom: namely, to publish a new Code of Practice to accompany the proposed changes, to create a number of templates to be used by Code operators and landowners or occupiers, and to create standard terms that may be used by Code operators and landowners or occupiers when negotiating agreements to confer Code rights.[22]

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 radios for maritime, aeronautical and business purposes.

The Act replaced the system of individual licences with a general authorisation regime for the provision of ECNs or electronic communications service providers (ECSs). Operators of ECNs and ECSs must comply with the General Conditions of Entitlement as specified in the Act. As well as the General Conditions, individual ECN or ECS operators may also be subject to further conditions specifically addressed to them. These may fall into four main categories: universal service conditions, access-related conditions, privileged supplier conditions, and conditions imposed as a result of a finding of significant market power (SMP) of an ECN operator or an ECS provider in a relevant economic market.

Mobile and satellite services require licences under the Wireless Telegraphy Act 2006 to authorise the use of the operators' radio transmission equipment and earth stations on specified frequencies. Under the Act, Ofcom should adopt decisions on the rights of use for radio frequencies allocated for specific purposes within the national frequency plan within six weeks and, in any other case, as soon as possible after receipt of the application. Since 30 April 2014,[23] radio transmission equipment and earth stations mounted on mobile platforms (ESOMPs) on aircraft have been exempt from licensing requirements when operating within the 1800MHz or 2100MHz bands, provided they comply with European Telecommunications Standards Institute requirements.[24] From 27 June 2014, pursuant

21 Available at: https://www.gov.uk/government/publications/government-publishes-proposals-for-a-new-electronic-communications-code.
22 Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0031/99148/ecc-consultation.pdf.
23 Pursuant to the Wireless Telegraphy (Mobile Communication Services on Aircraft) (Exemption) Regulations 2014, SI 2014/953.
24 Available at www.etsi.org/standards/looking-for-an-etsi-standard/list-of-harmonised-standards.

© 2017 Law Business Research Ltd

to the Wireless Telegraphy (Exemption and Amendment) Regulations 2014,[25] land-based transmission equipment and ESOMPs are exempt from licensing requirements across all frequencies, provided they comply with certain technical specifications.[26]

iii Ownership and market access restrictions

No foreign ownership restrictions apply to authorisation to provide telecommunications services, although the Act directs that the Secretary of State for Culture, Media and Sport (Secretary of State) 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 broadcasters, there are no longer any rules that prohibit those not established or resident in the EEA from holding broadcasting licences. At the end of 2011, Ofcom was asked by the Secretary of State to report on measuring media plurality in light of the proposed acquisition of British Sky Broadcasting Group Plc (BSkyB) by News Corporation. In 2012, Ofcom submitted two reports to the Secretary of State advising on approaches to measure media plurality. Ofcom gave evidence and provided advice to the Leveson Inquiry, including advice on models of media regulation. In February 2014, the House of Lords Select Committee on Communications produced a report into media plurality, including advice on the scope and flexibility of any assessment of media plurality.[27] The report included a recommendation that Ofcom should conduct a review of media plurality every four or five years, that there be a higher threshold for intervention and that there be a reform of the system for reviewing mergers in the media sector. The DCMS produced a Media Ownership and Plurality Consultation Report on 6 August 2014 setting out a framework to assess media plurality and commissioning Ofcom to develop a suitable set of indicators.[28] Following on from this, Ofcom published a consultation proposing a framework for media plurality on 11 March 2015.[29] The proposed framework built on the advice Ofcom gave to the Secretary of State in 2012. The consultation in particular makes the following points, which Ofcom has either developed or affirmed since 2012:

a online news and digital intermediaries should be measured by the framework;
b cross-media consumption metrics should form the foundation of plurality assessment;
c impact metrics should feature in the assessment of plurality;
d qualitative factors should be considered alongside quantitative metrics (such as the above) in the assessment of plurality;
e the measurement framework must be capable of capturing the differences in the level of media plurality and sources of news across the UK and within the UK nations; and
f media ownership can be taken into account by using a framework with metrics that can be considered at both the retail and wholesale level.

25 SI 2014/1484.
26 Available at: http://stakeholders.ofcom.org.uk/binaries/spectrum/spectrum-policy-area/spectrum-management/research-guidelines-tech-info/interface-requirements/uk2027.pdf.
27 Available at www.publications.parliament.uk/pa/ld201314/ldselect/ldcomm/120/120.pdf.
28 Available at www.gov.uk/government/publications/media-ownership-plurality-consultation-report.
29 Available at http://stakeholders.ofcom.org.uk/binaries/consultations/media-plurality-framework/summary/Media_plurality_measurement_framework.pdf.

© 2017 Law Business Research Ltd

iv Transfers of control and assignments

For transactions that do not fall within EU merger control jurisdiction, the UK operates a merger regime in which the parties to a transaction can choose whether to notify a transaction prior to closing. The UK CMA monitors transactions prior to closing and has the power to intervene in un-notified transactions prior to closing or up to four months from the closing of a transaction being publicised. Where the CMA intervenes in a closed transaction it is policy to impose a hold-separate order.[30]

The administrative body currently responsible for UK merger control is the CMA, which was established on 1 April 2014 by merging the function of the former Office of Fair Trading and the former Competition Commission in accordance with the Enterprise and Regulatory Reform Act 2013. The CMA consults Ofcom when considering transactions in the broadcast, telecommunications and newspaper publishing markets.[31]

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, for example, the need to ensure sufficient plurality of persons with control of media enterprises serving UK audiences; the need for the availability throughout the UK of high-quality broadcasting calculated to appeal to a broad variety of tastes and interests; and the need for accurate presentation of news, plurality of views and free expression in newspaper mergers. 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.[32]

v DSM and telecoms

On 6 May 2015, the Commission published a Communication on a DSM Strategy for Europe. This Strategy aims to make the EU's single market 'fit' for the digital age through three pillars: better online access for consumers and businesses across Europe; creating the right conditions and a level playing field for the advanced digital networks and innovative services; and maximising the growth potential of the digital economy. The Strategy includes legislative proposals in a range of areas with a view to make cross-border e-commerce easier, to end unjustified geo-blocking, to reform the copyright regime and reduce burdens due to different VAT regimes. In addition to reviewing both the e-Privacy and the Audiovisual Media Services Directives, the Commission is also conducting an analysis of the role of platforms, seeking to improve cross-border parcel delivery and undertaking an initiative in relation to data ownership and the cloud. On 10 May 2017, the Commission published a report on the E-commerce Sector Enquiry. One of the main points the Commission raised

30 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.

31 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.

32 There is also the power to take 'appropriate measures' nationally to protect the plurality of the media under Article 21(4) of the EU Merger Regulations (Regulation 139/2004/EC).

© 2017 Law Business Research Ltd

was that with the growth of e-commerce, business practices have emerged that may raise competition concerns, such as pricing restrictions and online marketplace (platform) bans. The Commission noted that it is important to avoid diverging interpretations of the EU competition rules in e-commerce markets, which may in turn create obstacles for companies to the detriment of a Digital Single Market. The Commission hopes that establishing a supportive investment climate for digital networks will help to mobilise private investment and generate investor confidence. The proposals aim to stimulate increased cross-border commerce within the EU and change some of the legislative frameworks that govern content diffusion and communications.

The UK government published a response to the Commission's initial 2015 DSM proposals in January 2016,[33] and the Commission's legislative proposals will be discussed by the European Parliament and the Council (to the extent they have not already been agreed). In certain areas, it is not expected that the Commission's proposals will become binding on Member States for several years. However, in other areas, the proposals are well progressed. For instance, the new regulation on cross-border portability of online content services will apply from 1 April 2018.

On 14 September 2016, Commission President Jean-Claude Juncker announced the Commission's DSM Strategy proposals for telecoms regulation reform and plans to modernise and improve connectivity across the EU (a proposal to modernise the EU's copyright rules was also announced). The telecoms and connectivity proposals included:

a recasting four existing Directives (Framework, Authorisation, Access and Universal Services Directives) as one Directive, the European Electronic Communications Code (Code);

b upgrading BEREC to a fully fledged EU agency;

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

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

The Commission released a mid-term review in May 2017 to take stock of the progress made, increase the pace on proposals already presented from the 2015 Strategy, and outline further actions relating to online platforms, the data economy and cybersecurity. There are developments that have arisen from the Strategy and that have begun to address the issues highlighted in the original Communication. One significant development has been the abolition of retail roaming charges throughout the EU, effective from 15 June 2017, as part of the ongoing focus on promoting cross-border e-commerce. From early 2018, consumers will be able to access online subscriptions for films, sport events, video games or music when travelling across the EU as if they were in their home Member State. The mid-term review also clearly emphasised the necessity to rapidly adopt the proposals for the Electronic Communications Code.

Generally, the proposed Code aims to address and harmonise spectrum policy and regulation, including spectrum auction timing, across the single market in part to stimulate competition and investment in 5G networks. It also tries to address new technologies and services that are not clearly contemplated by current legislation. In the UK, the rules and timelines for the spectrum auctions were announced by Ofcom in July 2017 and the auctions were expected to begin in October 2017. However, BT and Three commmenced

33 Available at: www.gov.uk/government/publications/audiovisual-media-services-directive-review-eu-consultation-response.

© 2017 Law Business Research Ltd

judicial review proceedings challenging, among other things, the legality of the spectrum cap proposed by Ofcom as part of the spectrum auction. The implementation of the new auction regime will be delayed until this challenge is resolved.

OTT services would be classified as a sub-class of ECS and subject to regulations concerning security (including security audits) and interconnectivity (among end-users and to emergency services). Other amendments regarding number allocation have been made to address potential competition issues with the expected advent of the IoT and M2M communication: national regulators would be allowed (but not required) to assign numbers to undertakings other than providers of electronic communications networks and services. The Code also proposes to sweep away universal service access requirements to legacy technologies (e.g., public payphones) and replace 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 proposed Code contains additional consumer protections via proposed regulations requiring telecoms providers to provide contract summaries and improved comparison tools.

It is also proposed that the regulatory role of BEREC be enhanced with a view to improving regulatory consistency across the single market. For example, it is proposed that decisions on spectrum assignment be subject to a 'peer review' process whereby BEREC would issue an opinion on whether the decision should be amended or withdrawn to ensure consistent spectrum assignment. BEREC would also issue opinions on any remedy proposed by NRAs in relation to maintaining the Code's objectives. These opinions are proposed to be persuasive rather than binding, but the Code requires that the NRA and the Commission (as relevant) take BEREC opinions into account. BEREC would also be granted legally binding powers, including a 'double-lock' system in relation to any draft remedy proposed by an NRA (i.e., where BEREC and the Commission agree on a position regarding such draft remedy, the NRA could be required by the Commission to amend or withdraw the draft measure).

In terms of policy proposals, the 5G Action Plan proposes to bring 'uninterrupted 5G coverage' to all major European urban areas and transportation corridors by 2025, with several interim deadlines relating to, among others, development of a deployment road map (by the end of 2017), spectrum assignment (2019) and development of global 5G standards (2019). Specifics of the 5G Action Plan, such as the development of 5G standards, are still under development. There is limited guidance on funding for the 5G Action Plan, although the Code in itself has stimulated to an extent such investment, and the Commission has launched the European Broadband Fund (combining private and public investments) to support network deployment throughout the EU. The Commission has also committed to exploring a proposal by a telecoms industry group to provide a venture financing facility (jointly funded by public and private sources) for start-ups developing 5G technologies and applications. The WiFi4EU initiative proposes to assist local authorities to offer free Wi-Fi connections in parks, libraries and other public spaces by providing local authorities with small grants of up to €60,000 (from a total initial budget of €120 million) for equipment and installation costs. In May 2017, the European Parliament, Council and Commission reached a political agreement on the initiative and its funding. It is intended that this would develop into a more harmonised telecoms regulatory regime, with an advanced 5G network that could be in place by 2025, providing a robust platform for delivery of the single market aims.

© 2017 Law Business Research Ltd

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

As previously noted, the Act is technology-neutral, and as such there is no specific regulatory regime for internet services. ISPs are also ECNs or ECSs depending on whether they operate their own transmission system, and are entitled to provide services under the Act in compliance with the general conditions and, where applicable, specific conditions.

VoIP and VoB are specifically subject to a number of general authorisation conditions under the Act, such as those related to emergency call numbers.

Following various market reviews, Ofcom has imposed conditions on access to the internet on BT and KCOM (formerly Kingston Communications) where it found that these had SMP. As part of these conditions, both companies must make regulatory financial statements. Since April 2014, BT has been required to increase the amount and improve the clarity of information in these statements, and in 2015 Regulatory Accounting Guidelines were put in place by Ofcom.[34] Conversely, KCOM's reporting requirements have been reduced.[35]

In the context of the 'net neutrality' debate, the Revised EU Framework adopted a range of internet traffic management provisions allowing NRAs such as Ofcom to adopt measures to ensure minimum quality levels for network transmission services, and to require ECN and ECS operators to provide information about the presence of any traffic-shaping processes operated by ISPs. These provisions were implemented into UK telecoms legislation following the legislative changes approved by the government on 4 May 2011.

Prior to the EU Regulation on Open Internet Access coming into force in 2016, the Broadband Stakeholders' Group published a voluntary industry code of practice on traffic management transparency for broadband services introducing transparency requirements on ISPs' traffic management practices in March 2011. Subsequently, in July 2012, major ISPs published the Open Internet Code of Practice, which commits ISPs to providing full and open internet access. The latest Open Internet Code was published on 8 June 2016. The new Code continues to preserve the concept of an open internet while clarifying the context in which some innovative services, which could become more prevalent as the IoT becomes a reality, could be provided alongside the open internet. The new Code adds three new commitments, namely ISPs promise open and full access to the net across their range of products; firms cannot market a subscription package as including 'internet access' if certain kinds of legal content or services are barred; and members must not target and degrade content or applications offered by a specific rival.[36] Notably, Everything Everywhere (EE) has opted out of signing the new Code.

From April 2016, the EU Regulation on Open Internet Access[37] put in place EU-wide rules for net neutrality and granted end-users the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location (Article 3(1)). The aim is that users will have access to online content that is not subject to discrimination or interference.

34 Available at: http://stakeholders.ofcom.org.uk/consultations/BT-cost-attribution-review-second-consultation.

35 'Changes to BT and KCOM's regulatory and financial report 2013/14 update', available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0029/68762/bt_kcom_1314_statement.pdf.

36 Available at: www.broadbanduk.org/wp-content/uploads/2016/06/BSG-Open-Internet-Code-2016.pdf.

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

© 2017 Law Business Research Ltd

Likewise, companies may not pay for prioritisation, so access to a small or medium-sized enterprise's (SME's) website will not be unjustly slowed down to allow access for larger companies. The requirement that all internet traffic be treated equally is subject to exceptions to:

a comply with EU or national legislation related to lawfulness of content or with criminal law;

b preserve the security and integrity of the network such as to combat viruses;

c minimise network congestion that is temporary or exceptional; and

d filter spam (i.e., to filter unsolicited communications and allow parents to set up parental filters).

In terms of the latter, such measures need to be transparent, non-discriminatory and proportionate, and may not be able to be maintained for longer than is necessary. Likewise, providers of internet access services must publish information on traffic management measures in end-user contracts, along with details on the privacy of end-users and the protection of their personal data. Notably, the NRAs in charge are required to monitor and enforce the open internet rules, although it is for Member States to lay down rules on the penalties applicable for infringements of the net neutrality provisions. On 30 August 2016, BEREC published guidelines[38] for NRAs on the implementation of net neutrality under the EU Regulation on Open Internet Access, in particular covering obligations to monitor closely and ensure compliance with the EU net neutrality rules to ensure equal treatment of traffic in the provision of internet access services and related end-user rights.

ii Universal service

Universal service is provided under the Act by way of the universal service order. The USO in the UK covers ECNs and ECSs and activities in connection with these services. Ofcom designated BT and KCOM as universal service providers in the geographical areas they cover.

The Commission's Europe 2020 Strategy of March 2010 included aiming for broadband access for all by 2013, and access for all to internet speeds of 30Mb/s or above by 2020. To support the Digital Agenda for Europe, the European Parliament and the Council passed a Directive[39] in May 2014 aiming to cut the costs of the high-speed rollout. By 1 July 2016, Member States had to apply measures to, *inter alia*, better coordinate civil works, provide greater access to, and information regarding, infrastructure, and reduce the time taken to grant permits required to lay down networks. In July 2016, the UK implemented this Directive in the form of the Communications (Access to Infrastructure) Regulations 2016.

In September 2012, as part of a scheme to create 'super-connected cities', the government announced £144 million in investment across 10 of the UK's largest cities to help provide them with superfast broadband: London, Belfast, Cardiff, Edinburgh, Birmingham, Bristol, Leeds, Bradford, Manchester and Newcastle received £94 million between them, while smaller cities will share a £50 million fund. The scheme was extended to Aberdeen, Brighton and Hove, Cambridge, Coventry, Derby, Londonderry, Newport, Oxford and Perth in December 2012.

38 Available at: http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules.

39 Directive 2014/61/EU of the European Parliament and of the Council of 15 May 2014 on measures to reduce the cost of deploying high-speed electronic communications networks.

© 2017 Law Business Research Ltd

However, following legal challenges by two of the UK's biggest networks, the government withdrew the state-aid application relating to the super-connected cities. Consequently, public funds for the super-connected cities scheme had to be withdrawn in July 2013, before the DCMS diverted the allocated sums to a scheme that allowed SMEs to apply for vouchers to install faster internet connections in August 2013.[40] As part of the government's 2014 autumn statement, this scheme was extended by 12 months to March 2016 with a further £40 million of funding. The plan to install wireless access points across the super-connected cities, however, was re-emphasised in July 2013. In January 2014, the DCMS announced a £10 million fund for a pilot programme to extend superfast broadband to hard-to-reach areas. In February 2014, a further £12 million was allocated to provide superfast broadband to Wales. Both funds opened for bids in March 2014. An August 2014 report from the DCMS confirmed that the rollout of superfast broadband to 95 per cent of UK homes and businesses was on track for completion by 2017. In a Parliament briefing paper published in March 2017, it was stated that this would be completed by December 2017. As part of the Commission's state aid clearance decision, the UK committed to undertake an *ex post facto* evaluation of the National Broadband Scheme. This was published by Oxera in March 2015.[41] The Commission has approved an extension on materially the same terms, and the scheme will now be valid until December 2020. The government is committing further funds to 'put the UK at the forefront of the global technology revolution',[42] investing £200 million to fund local projects with the aim of testing ways to accelerate the market for the delivery of new full-fibre broadband.

The development of superfast broadband will require the rollout of fibre-optic cable throughout the UK telecommunications network infrastructure. In June 2014, Ofcom published its follow-up conclusions to a December 2010 review of the wholesale broadband access market setting out remedies to promote competition and investment in current and superfast broadband services. In June 2015, Ofcom published a report setting out its assessment and recommendations on the provision and availability of communications services for SMEs in the UK.[43] Ofcom found that the availability of superfast broadband to SMEs is significantly lower than to residential premises. In Ofcom's annual review for 2017 to 2018, Ofcom noted that it was key to continue to help SMEs engage in the communications market.

Access and interconnection are regulated in the UK by EU competition law and by specific provisions in the Act aimed at increasing competition. The General Conditions require all providers of public ECNs to negotiate interconnection with other providers of public ECNs. Specific access conditions may also be imposed on operators with SMP. Although prices charged to end-users are not regulated, Ofcom may regulate wholesale rates charged by certain operators to alternative operators for network access. This is the case, *inter alia*, for wholesale fixed termination rates, wholesale mobile call termination rates, wholesale broadband access rates (as detailed above), local loop unbundling and wholesale line rental services.

40 See the DCMS's consultation on the Connection Vouchers Scheme, 25 June 2013. Available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/239182/BDUK_vouchers.pdf.

41 Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/428381/The_UK_s_National_Broadband_Scheme_-_an_independent_evaluation.pdf..

42 Available at: http://www.broadbanduk.org/2017/03/08/budget-2017-more-details-on-the-governments-full-fibre-and-5g-ambitions.

43 Available at: http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/sme/bb-for-smes.pdf.

© 2017 Law Business Research Ltd

Ofcom imposed specific conditions on BT and KCOM in certain areas where they enjoy SMP so as to allow alternative operators to compete in the retail broadband market.[44] These include an obligation to provide general and non-discriminatory network access to BT and KCOM's wholesale broadband products to alternative operators on a reasonable request; an obligation to maintain separate accounts between the services to alternative operators and its own retail division as well as other related transparency obligations; and a charge control on BT to ensure that charges for its broadband wholesale products are based on the costs of provision. Network access obligations included virtual access to new fibre lines laid by BT (through its access service division, Openreach), allowing alternative operators to combine their own electronics with physical infrastructure rented from BT. Furthermore, in June 2015, Ofcom proposed a charge control on the wholesale prices BT charges for products using leased telecoms lines, which provide vital high-speed links for businesses and providers of superfast broadband and mobile services.[45] In 2016, Ofcom also stated that Openreach must become more independent from BT and proposed that Openreach become a distinct company with its own board and accountable executives. Openreach should also have independent branding, own assets that it already controls and have a separate strategy in relation to budget allocation. Likewise, in February 2016, Ofcom committed to making it easier for telecoms providers to invest in advanced, competing infrastructure by improving access to Openreach's network of telegraph poles and ducts allowing competitors to connect their own fibre-optic cables directly to homes and businesses.[46] The aim of Ofcom to promote the restructuring of BT and Openreach came to fruition in March 2017, when BT agreed that Openreach should become a distinct company with its own staff, management, strategy and legal purpose. This separation will likely take some time to be fully reflected in the market; however, significant progress has occurred already.

iii Restrictions on the provision of service

The Digital Economy Act 2010 empowers the Secretary of State to impose obligations on ISPs to limit the internet access of subscribers who engage in online copyright infringement. Under the Digital Economy Act 2010, Ofcom has proposed a code of practice (in the absence of a code put forward by the industry) governing the 'initial obligations', which require ISPs to send notifications to their subscribers following receipt of reports of copyright infringement from copyright owners. ISPs must also record the number of reports made against their subscribers and provide copyright owners, on request, with an anonymised list that enables the copyright owner to see which of the reports it has made are linked to the same subscriber (also known as the copyright infringement list). Despite the Court of Appeal's dismissal of an appeal against the Digital Economy Act 2010 by BT and TalkTalk in March 2012, there are still arguments as to whether the information to be collected by ISPs on copyright offenders might infringe data protection legislation and which costs are to be borne by ISPs.

A second draft of the Code of Practice that would implement the Act was published in June 2012. This version, and legislation on cost sharing, have to be approved by both Houses of Parliament and then subjected to EU scrutiny before coming into effect; however,

44 Review of the wholesale broadband access markets, Ofcom, 3 December 2010. Available at: http://stakeholders.ofcom.org.uk/binaries/consultations/wba/statement/wbastatement.pdf.

45 Business Connectivity Market Review: Leased lines charge controls and dark fibre pricing. Available at http://stakeholders.ofcom.org.uk/binaries/consultations/llcc-dark-fibre/summary/llcc-dark-fibre.pdf.

46 Available at: http://media.ofcom.org.uk/news/2016/making-digital-communications-work-openreach-bt.

© 2017 Law Business Research Ltd

at the time of writing there have been no further updates on this. In June 2012, Ofcom had expected that the first notification letters would be sent out in early 2014. Due to delays in implementing legislation, Ofcom announced in May 2013 that the first letters would not be sent out until the latter half of 2015. In September 2013, to accelerate the process, music and film companies tried to convince ISPs to sign up to a voluntary code of practice that would also require them to create a database of repeat offenders. In July 2014, the DCMS announced a scheme named 'Creative Content UK', spearheaded by ISPs and media industry leaders and supported by a government contribution of £3.5 million, to raise awareness of copyright infringement and warn internet users whose accounts are used to illegally access and share copyright material. As part of the initiative, the 'Get It Right from a Genuine Site' awareness campaign launched in January 2017 with the aim of educating consumers on the legal sources of content available to UK consumers. This service incorporates the distribution of emails by ISPs to educate internet subscribers whose internet connections have been used to share files that contain copyright-protected content with others.[47] In addition to this educational function, the Voluntary Copyright Alert Programme (VCAP) has also been introduced, under which educational warning letters will be sent to those suspected of online piracy.

In the area of linking to content, there have been a few recent decisions of note. A decision of the Court of Justice of the European Union (CJEU) in February 2014[48] held that providing a hyperlink to material protected by copyright that is freely available to the public on another website (with the copyright holder's consent) does not constitute copyright infringement on the basis that the communication is not to a new public. This decision was followed by a UK High Court decision that required six UK ISPs to block access to websites providing hyperlinks to copyrighted content.[49] A decision of the CJEU in April 2016[50] dealt with linking to content made available online without the copyright owner's consent. The CJEU held that linking to infringing content does not constitute copyright infringement in itself unless the person who posted the link knew or ought to have known that the content was infringing. There is a rebuttable presumption that such knowledge test is satisfied where the linking was for financial gain.

The DEA received royal assent in April 2017 with the aim of improving internet connectivity and providing improved protections for internet users. Among the provisions of the DEA is an increased maximum penalty for online copyright infringement of 10 years. Although some sections of the DEA are in force, the remainder are subject to staggered commencement dates.

iv Security

Privacy and consumer protection overview

In the UK, consumers' personal data are primarily protected by the Data Protection Act 1998 (DPA), which implements the EU Data Protection Directive (Data Protection Directive),[51]

47 Commentary available at: https://www.gov.uk/government/news/get-it-right-from-a-genuine-site-copyright-campaign-update.

48 *Svensson and others v. Retriever Sverige AB, Case C- 466/12*, 13 February 2014.

49 *Paramount Home Entertainment International Ltd and others v. British Sky Broadcasting Ltd and others* [2014] EWHC 937 (Ch).

50 *GS Media v. Sanoma Media Netherlands BV and others*, Case C- 160/15, 7 April 2016.

51 Directive 95/46/EC.

© 2017 Law Business Research Ltd

and by the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (the ePrivacy UK Regulations), which implement the EU Directive on Privacy and Electronic Communication,[52] as amended by EU Directive 2009/136/EC (ePrivacy Directive). The Data Protection Directive will be replaced on 25 May 2018 by the GDPR,[53] which will become directly applicable in all EU Member States. Until this date, the Data Protection Directive will remain in force and there will be a transition period for organisations to upgrade their privacy compliance programmes to ensure compliance with the new law. The UK government has confirmed it will implement the GDPR on 25 May 2018, and introduced the Data Protection Bill in Parliament on 13 September 2017 (Bill). The GDPR will significantly change the current UK law (via the Data Protection Bill) – and broader European – data protection framework. In line with the Commission's DSM Strategy and the reforms being brought in by the GDPR, proposals for reform of the ePrivacy Directive are also currently under consideration. This year, the Commission proposed a draft ePrivacy Regulation (Draft ePrivacy Regulation), which is currently part way through the European legislative review process. The intention is for the Draft ePrivacy Regulation to come into force at the same time as the GDPR (although this seems optimistic).

Data protection

The DPA is based on the principles in the Data Protection Directive that impose strict controls on the processing (including disclosure) of personal data, including but not limited to the following:

a providing one or more listed conditions that must be met to ensure personal data are processed fairly and lawfully, such as that the individual has consented or that the processing is necessary for the purposes of fulfilling a contract;

b the requirement that data can generally only be processed for the purpose for which they were obtained, must be kept accurate and up to date and for no longer than is necessary, and must not be excessive;

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

d the restriction that data cannot be transferred to countries outside the EEA unless certain conditions are met, such as with the EU–US Privacy Shield (see 'Litigation and EU–US transfers of personal data' for more details), whereby personal data can be transferred to US entities that have undertaken a process of self-certification to determine that it meets an 'adequate' standard of privacy protection and commits to seven privacy principles; and

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

The restrictions in the DPA may affect the ability of a business to disclose information that includes personal data to third parties, including public bodies, unless certain conditions are met.

52 Directive 2002/58/EC.

53 Regulation (EU) 2016/679.

© 2017 Law Business Research Ltd

There has been significant criticism of the Data Protection Directive by numerous industry groups, and by various directorates-general within the Commission, on the basis that certain protections are disproportionately restrictive, create additional administrative and operational burdens for businesses to an inappropriate and unjustified extent, and dilute the potential benefits of the harmonising effect of the regulation by reserving various powers for Member States to put in place additional national rules.

The Commission aims to address these issues via the GDPR to bring various cost savings to organisations operating in Europe (by harmonising the rules across EU Member States and simplifying certain administrative requirements), lead to more efficient cooperation between national regulators and businesses, and set the 'gold standard' for data protection law.

The key changes under the GDPR include:

a the implementation of the new rules as a regulation, rather than a directive, which will be directly applicable in every Member State;

b the removal of the requirement to notify or register data-processing activities with the national regulator; however, controllers and processors will need to keep their own record of processing;

c the introduction of an extraterritorial effect, resulting in the regulation applying not only to organisations established within the EEA, but also to organisations established outside the EEA but offering goods or services to, or monitoring the behaviour of, individuals in the EEA (although it remains unclear how this will operate in practice);

d a tightening of the requirements for valid consent, with the effect that consent will only be deemed to be valid if it is freely given, specific, informed and unambiguous;

e a stricter approach to the export of data outside the EEA, resulting from the general standards of data protection being raised throughout the Regulation as a whole;

f the introduction of mandatory data breach notification requirements (including notification to both the national regulators and, in certain circumstances, to data subjects affected by the breach). On the occurrence of a breach, organisations must now inform the UK Information Commissioner's Office (ICO) without undue delay and, where feasible, not later than 72 hours after becoming aware of a data breach;

g a right to data portability that will require the data controller to provide information to the data subject in a machine-readable format and so that it may be transferred to another controller;

h maximum fines of the higher of up to €20 million or 4 per cent of an organisation's annual global turnover for breaches;

i certain categories of online 'identifiers' such as internet cookies and IP addresses may be classified as personal data;[54] and

j new definitions termed 'genetic data' and 'biometric data', which include data relating to characteristics obtained during foetal development and data that allow the unique identification of a person to be confirmed through facial images or dactyloscopic data – now categorised as 'special categories of personal data' (i.e., sensitive personal data).

54 In *Patrick Breyer v. Bundesrepublik Deutschland* (C-582/14) the CJEU ruled in October 2016 that where a website operator holds IP addresses and has 'the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person' then these will be classified as personal data.

© 2017 Law Business Research Ltd

The Queen's Speech on 21 June 2017 introduced the Bill that will replace the DPA and implement the GDPR in the UK. It is the government's intention for the UK to obtain an 'adequacy' status post-Brexit to ensure the maintenance of a free flow of information between the UK and EU Member States.

The GDPR permits certain derogations by Member States, and the Bill seeks to provide for these accordingly to accommodate various existing UK statutes. For instance:

a it includes exemptions for journalists, research organisations, financial services firms (for anti-money laundering purposes) and employers (to process special categories of personal data and criminal conviction data without consent to comply with employment law obligations);

b certain actions (with some exceptions for actions necessary for preventing crime, etc.) relating to data will be criminal offences (subject to a fine), for example obtaining, procuring, retaining or selling data against a controller's wishes (even where lawfully obtained); intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data (or knowingly handling or processing such data); and altering records with the intent to prevent disclosure following a subject access request; and

c parental or a guardian's consent will be required to process the personal data of a child who is under 13 years old (the GDPR permits Member States to set this age between 13 and 16 years old).

Litigation and EU–US transfers of personal data

There are several valid legal bases for transfer of personal data from the EU to countries outside the EU, of which two are subject to ongoing litigation: the Privacy Shield (successor to the Safe Harbor) and standard contractual clauses (also known as 'model clauses').

Under the Safe Harbor agreement, if a US recipient of personal data is self-certified under the US Safe Harbor regime, data transfers can be made to that recipient in the US, notwithstanding the general prohibition on transfer under the Data Protection Directive, because such a recipient was deemed to have adequate protection in place. The Safe Harbor regime was challenged in a case brought by Max Schrems who argued that the EU–US Safe Harbor agreement did not provide adequate security for EU citizens in light of the revelations exposed by Edward Snowden about PRISM and United States National Security Agency programmes. Schrems challenged the self-certification process involved in Safe Harbor and claimed that the personal data of EU citizens were no longer adequately protected due to US government surveillance. The CJEU invalidated the legal basis for Safe Harbor on 6 October 2015 with the immediate effect that the agreement was no longer considered to provide adequate protection under the eighth data protection principle.

Following the decision in *Schrems v. Data Protection Commissioner*, which invalidated the Safe Harbor Framework, the Commission and the US government entered into lengthy negotiations as to a new means of EU–US data transfers. The new EU–US Privacy Shield came into effect on 1 August 2016 following approvals by the Commission and the Member States (see Section VI for more details).

Under the new Privacy Shield, US organisations commit to seven privacy principles to ensure that adequate protections are in place. These include the notice principle, the data integrity and purpose limitation principle, the choice principle, the security principle, the access principle, the recourse, enforcement and liability principle as well as the accountability for onward transfer principle (Principles). To join the Privacy Shield, an organisation must

© 2017 Law Business Research Ltd

publicly commit to and implement the Principles through a self-certification process; be subject to the authority of US law by the relevant enforcement authority; and publicly disclose its privacy policy.[55]

The most significant changes from the Safe Harbor framework to the Privacy Shield include the following:

a individuals affected by non-compliance with the Principles can seek redress (from the organisation itself, from an independent dispute resolution body and from the national DPA) and non-compliance can be enforced by various bodies (the Federal Trade Commission (FTC), a newly created privacy shield panel and judicial redress);

b there are tighter controls on transfers of personal data;

c annual joint reviews by the Commission, the FTC and the Department of Commerce on whether the Privacy Shield meets the adequacy finding that entitles companies to transfer personal data overseas legally; and

d written assurances by the US government that any access to personal data by public authorities will be subject to clear limitations, safeguards and oversight mechanisms.

In April 2017, the European Parliament passed a non-legislative resolution stating that the Commission should review the Privacy Shield to ensure it does not undermine the EU Charter on Fundamental Rights and the GDPR. In September 2017, the first joint review of the US Privacy Shield is due to take place between the EU and US. The Privacy Shield is itself under scrutiny from privacy campaigners who have brought claims before the General Court (the lower court of the CJEU) contesting the Commission's adequacy finding for privacy shielding on the grounds that the Privacy Shield also does not provide a level of data protection equivalent to the level of data protection required by European data protection law.

In May 2016, Max Schrems filed a complaint with the Irish Data Protection Commissioner concerning the legal status of data transfers under Facebook's standard contractual clauses. The Irish Data Protection Commissioner has referred the case to the CJEU to determine the legal status of the use of standard contractual clauses to transfer personal data outside the EU.[56] The CJEU will need to consider if personal data transfer using model clauses is legal.

ePrivacy Regulation

The Draft ePrivacy Regulation would introduce further rules for the electronic communications sector, including controls on unsolicited direct marketing, restrictions on the use of cookies, and rules on the use of traffic and location data. As with the existing ePrivacy Directive, the intent with the ePrivacy Regulation is to complement the DPA and the GDPR, and establish a modern, comprehensive and technologically neutral framework for electronic communications.

The Draft ePrivacy Regulation (which is subject to further changes) aims to improve on the existing ePrivacy Directive in several ways, including:

a expanding the scope of ePrivacy laws to include OTT providers who provide services functionally equivalent to traditional telecoms providers (e.g., Facebook Messenger,

55 Available at: www.privacyshield.gov/welcome.

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

© 2017 Law Business Research Ltd

Whatsapp, Skype); and apply to organisations worldwide as long as they are providing services to end-users in the EU;

b tightening and calibrating rules on cookies whereby GDPR-equivalent consent would be required except for certain situations, such as for website analytics; and browsers must offer privacy-by-design features (e.g., activating privacy friendly features by default);

c tightening rules in relation to direct marketing (including business-to-business marketing);

d restricting use of content and metadata to only where necessary to provide a service, or for quality control, billing, or fraud or abuse monitoring purposes, or with the consent of the end-user for specific purposes;

e alignment of sanctions to the GDPR: for example, breach could bring liability of up to €20 million or 4 per cent of annual worldwide turnover; and

f unifying the ePrivacy Regulation's enforcement under GDPR enforcement bodies.

The European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE), Article 29 Working Party and the European Data Protection Supervisor have all produced reports on the proposed Draft ePrivacy Regulations. Though parts of the proposed Draft ePrivacy Regulation were well received by these reports (such as the expansion of scope to include OTT providers and regulation of metadata), they also contain ample criticism for the proposed regulation. In particular, criticism centres on four main areas:

a location tracking via collection of Wi-Fi or Bluetooth signals is too permissive and should be subject to specific, informed consent and, in certain circumstances, immediate anonymisation of data;

b browser settings in the current draft only need to offer do-not-track options, but full privacy-by-design features should be enabled by default;

c tracking walls (whereby service providers offer take-it-or-leave-it options for their services: for example, services are only accessible if end-users agree to be tracked) should be prohibited in certain circumstances (such as for sites dealing with health or other sensitive information, state-funded websites, etc.); and

d analysis of content and metadata should only be permitted with the meaningful consent of all end-users (sender and recipient).

These criticisms will be countered by industry groups who will argue that the viability of the services they provide depend on compelling the tracking of end-users to begin with, or the analysis of the metadata they generate.

The intention is for the Draft ePrivacy Regulation to apply from 25 May 2018, the same day as the GDPR comes into effect. This deadline is ambitious considering the legislative processes involved. However, in principle, the Draft ePrivacy Regulation will arrive before the UK's planned departure from the EU in 2019, and companies should assume it will take effect (in its eventual form) in the UK and act accordingly. Given the criticism gained by the proposal, companies should also be prepared to see substantial changes to the Draft before its passage.

© 2017 Law Business Research Ltd

Legislative process

The Data Protection Bill will undergo further scrutiny in the House of Lords and House of Commons before it is given royal assent and officially enacted in the UK. It is likely that the Data Protection Bill will be the subject of lobbying and debate, and its development must therefore be followed.

The Draft ePrivacy Regulation must be approved by the European Parliament and European Council prior to taking effect. Development of this law should be tracked to ensure ongoing compliance.

Enforcement

Under the current DPA framework, the ICO is responsible for the implementation and enforcement of the DPA and the ePrivacy Regulations 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 continues to increase its focus on enforcement generally, and on the use of monetary penalties (of up to £500,000 at any one time) in particular. According to the ICO's Annual Report for 2016 and 2017, the ICO issued the most civil monetary penalties for Privacy and Electronic Communications Regulations breaches, with 23 penalties totalling £1,923,000 for a range of prohibited marketing activities. A total of 16 civil monetary penalties cumulating in £1,624,500 were issued across public and private spheres for breaches of data protection principles. The largest of these was a £400,000 fine on TalkTalk Telecom Group Plc (TalkTalk) for security failures that permitted a cyberattacker to obtain customer data.

The most common ground for large fines and enforcement action is loss of data, automated marketing calls and other major data security breaches. The ICO takes a serious view of the loss of data. In January 2017, Royal & Sun Alliance Insurance PLC was fined £150,000 by the ICO as a result of losing the personal data of nearly 60,000 customers.[57] Greater Manchester Police were fined £150,000 in May 2017 after three DVDs containing footage of interviews with victims of sexual crime got lost in the mail.[58] A large amount of fines were issued against private companies for unsolicited marketing calls and messages. In May 2017, the ICO issued the highest-ever nuisance calls fine of £400,000 to Keurboom Communication Ltd, which was responsible for 99.5 million nuisance calls.[59] In September 2017, True Telecom Limited was fined £85,000 for making illegal nuisance calls.[60] HomeLogic UK Ltd, a domestic energy saving firm, received a £50,000 fine in August 2017 for making marketing calls that people had expressly stated they did not want to receive.[61] Moneysupermarket.com received a fine of £80,000 for sending millions of emails to people who had made it clear they did not want to be contacted in that way.[62]

57 Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/150-000-fine-for-insurance-company-that-failed-to-keep-customers-information-safe.

58 Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/05/greater-manchester-police-fined-after-victim-interview-videos-go-missing.

59 Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/05/record-fine-for-firm-behind-nearly-100-million-nuisance-calls.

60 Available at https://ico.org.uk/media/action-weve-taken/mpns/2014783/mpn-true-telecom-20170906.pdf.

61 Available at: https://ico.org.uk/media/action-weve taken/mpns/2014674/home_logic_uk_ltd_mpn.pdf.

62 Available at: https://ico.org.uk/media/action-weve-taken/mpns/2014482/mpn-moneysupermarket-ltd-20170720.pdf.

© 2017 Law Business Research Ltd

Individual data subjects have the right under the DPA to notify a data controller to cease or not to begin processing their personal data for the purposes of direct marketing. Under the ePrivacy UK Regulations, an organisation must obtain prior consent before sending a marketing message by automated call, fax, email, SMS text message, video message or picture message to an individual subscriber. There is a limited exemption for marketing by electronic mail (both email and SMS) that allows businesses to send electronic mail to existing customers provided that they are marketing their own goods or services; such goods and services 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. The same maximum fine (of £500,000) also applies to breaches of the ePrivacy UK Regulations.

Under the ePrivacy UK Regulations, location data (any data that identifies the geographical location of a person using a mobile device) can be used to provide value-added services (e.g., advertising) only if the user cannot be identified from the data or the customer has given prior consent. To give consent, the user must be aware of the types of location data that will be processed, the purposes and duration of processing those data, and whether the data will be transmitted to a third party to provide the value-added service.

Consent of the user of the relevant terminal equipment for the placement of cookies is required, unless the cookie is strictly necessary to provide an online service requested by the 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). In practice, steps have been taken by most reputable UK websites to comply with these consent requirements, ranging from banner notices with tick boxes, boxes that require an active step to make them disappear to one-time banners or pop-overs giving brief information and allowing the user to take steps to disable the site's cookies if they wish to do so before continuing to use the site.[63] Between April 2016 and March 2017, the ICO received 195 reports regarding breach of cookies rules via their website, a slight decrease from 210 received in the previous financial year ending March 2016.[64] Its current approach is to focus on sites that are not doing enough to raise awareness of cookies or to obtain their users' consent, particularly those most visited sites in the UK. However, according to the ICO, cookies remain a 'low' consumer threat, as the number of reported concerns about cookies was 195 compared to 167,018 received concerns about nuisance calls, text messages and emails.[65] A variety of different approaches can be seen across those countries that have implemented the consent rules, although there is a general trend towards an implied consent approach rather than a strict express consent approach.

The GDPR introduces a higher level of consent, stating that consent should be a clear affirmative act establishing a freely given, informed and unambiguous indication of the data subject's agreement to the processing of personal data. Silence or inactivity does not constitute consent, and consent needs to be obtained for each processing purpose.[66] Further, the data subject must have the right to withdraw consent at any time.[67] This means companies that

63 Available at: https://ico.org.uk/action-weve-taken/cookies.

64 Available at: https://ico.org.uk/action-weve-taken.

65 Ibid.

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

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

© 2017 Law Business Research Ltd

use banners that do not interrupt the user's interaction with the website (rather than those that provide notice and infer consent from continued use, for example) may need to revise this approach.

Data breach notification

Currently, there are no mandatory data breach notification requirements under the DPA, except that the ICO has an expectation to be notified of data breaches in certain circumstances (e.g., the data breach involves a large volume of personal data or sensitive personal data).

The GDPR introduces a new data breach notification obligation on data controllers requiring notification to the supervisory authorities without undue delay and not later than 72 hours after becoming aware of a breach, unless the data security breach is unlikely to result in a risk to the rights and freedoms of the data subject. If the personal data breach results in a high risk to the rights and freedoms of a natural person, the data controller must inform the natural person of the data breach without undue delay.[68] The GDPR also requires a data processor to notify the data controller if it becomes aware of a personal data breach. An infringement of these provisions can lead to an administrative fine up to €10 million or, in the case of an undertaking, up to 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher.[69]

Under the ePrivacy UK Regulations, providers of public electronic communications services (mainly telecom providers and ISPs) are required to inform the ICO within 24 hours of a personal data security breach and, where that breach is likely to adversely affect the personal data or privacy of a customer, that customer must also be promptly notified. The Draft ePrivacy Regulations intend to align this deadline with the time period set under the GDPR (72 hours) for consistency. This should be kept under review as the Draft ePrivacy Regulation is finalised.

Data retention, interception and disclosure of communications data

The legislation in this area has been the subject of much change and controversy over the past year. The powers of government authorities to intercept communications, acquire communications data and interfere with communications equipment was previously regulated by a patchwork of legislation, including the Regulation of Investigatory Powers Act 2000 (RIPA), and, until recently, the EU Data Retention Directive and DRIPA. The Investigatory Powers Act 2016 (IPA) overhauls and, in some cases, extends the scope of RIPA, but has not yet repealed RIPA in its entirety.

RIPA imposes a general prohibition on the interception of communications without the consent of both the sender and recipient, unless a warrant is issued by the Secretary of State (interception warrant) or the lawful monitoring permitted under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 can be complied with for employers monitoring employee emails. Interception warrants can be requested by a limited number of individuals heading various security and law enforcement bodies, by HMRC or by another state under a mutual assistance treaty. The grounds for

68 General Data Protection Regulation: Articles 33 and 34.

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

© 2017 Law Business Research Ltd

issuing warrants are that the interception is in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic wellbeing of the UK.

Under RIPA, public telecommunications service providers who provide (or intend to provide) services to more than 10,000 users may be required to maintain interception capabilities on receipt of a notice from the Secretary of State (interception capability notice). In certain circumstances, contributions will be made towards the costs of implementing intercept capabilities or responding to warrants. There is a similar prohibition on the disclosure of communications data (e.g., subscriber, traffic and location data); however, no warrant is needed to allow disclosure. Disclosure can be made on request by a far wider range of public bodies, and the grounds on which requests can be made are far broader, including that the request is in the interests of public safety, for the purpose of protecting public health, or for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

On 8 April 2014, the CJEU held in *Digital Rights Ireland*[70] that Directive 2006/24/EC (Data Retention Directive) was invalid as it violated an individual's right to privacy and was disproportionate to its aims. Under the Data Retention Directive, public communications providers (e.g., providers of fixed-network telephony, mobile telephony and internet access, internet email or internet telephony) had to retain traffic, subscriber and, where relevant, location data (but excluding content data) for a period of 12 months.[71] The declaration of invalidity meant that the UK's implementing subordinate legislation, the Data Retention (EC Directive) Regulations 2009, no longer had a basis in primary law and was itself vulnerable to a finding of illegality. The government decided to reintroduce data retention laws as primary legislation by passing DRIPA. In this regard, the UK stands in stark contrast to the rest of Europe, where Germany, the Czech Republic, Romania, Austria, Cyprus, Belgium, Ireland and Bulgaria had already deemed similar provisions unlawful.

DRIPA came into force on 17 July 2014 (with a sunset clause forcing automatic expiry of its provisions on 31 December 2016) following a fast-tracked procedure that saw it pass all stages of Parliament within four days (a process that often takes months or even years) on the basis that its enactment was required for continued national security. DRIPA addressed two key issues: the obligation to retain communications data by communications providers and the extraterritorial expansion of powers under RIPA.[72] DRIPA also clarified that interception capability notices under RIPA may be issued to telecommunications providers outside the UK in relation to conduct outside the UK.

Following the passage of DRIPA, MPs Tom Watson and David Davis and leading civil rights group Liberty mounted a legal challenge against DRIPA over the legality of the GCHQ's bulk interception of calls and messages via the judicial review procedure whereby a judge assesses the legality of a decision taken by a public body (in this instance, Parliament). The legality of DRIPA was questioned on the basis that the data retention provisions in the first part of the Act were introduced following the CJEU's declaration that similar provisions in the Data Retention Directive were declared invalid.

In July 2015, the High Court declared the DRIPA data retention provisions to be incompatible with EU law on the basis that they interfered with Articles 7 and 8 (the public's

70 Digital Rights Ireland and Seitlinger and others, Joined Cases C-293/12 and 594/12, 8 April 2014.

71 *Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others.*

72 Data Retention and Investigatory Powers Act 2014.

© 2017 Law Business Research Ltd

right to respect for private life and communications and to the protection of personal data) of the EU Charter of Fundamental Rights.[73] Particular criticism was made regarding the emergency nature of the legislation as well as its fast-tracked path through Parliament. In November 2015, the Court of Appeal referred the case to the CJEU as to whether the CJEU's judgment in Digital Rights Ireland laid down mandatory requirements of EU law with which Member States must comply.

The CJEU held on 21 December 2016 that the ePrivacy Directive and the Charter of Fundamental Rights preclude laws that require a general and indiscriminate retention of data. However, laws that place targeted data retention obligations on service providers for the purpose of fighting serious crime are permitted provided that the safeguards protecting Article 7 and 8 rights are maintained (as specified in Digital Rights Ireland). The CJEU held that national data retention laws fall within the scope of the ePrivacy Directive. Member States may, to fight serious crime, impose general data retention obligations on providers of electronic communications services, provided that:

a any such laws are clear, precise and provide sufficient guarantees against misuse of the data;

b define the circumstances and conditions under which authorities will be allowed access to the data (in general, access will only be granted in relation to serious crime, as opposed to ordinary crime or civil proceedings);

c are subject to prior review by a court or other independent body (except in urgent cases); and

d the retained data must be retained within the EU and irreversibly destroyed at the end of the retention period.

The CJEU has referred the case back to the UK Court of Appeal.

Although DRIPA would itself have expired in accordance with its sunset clause, its spirit survives in the IPA, which received royal assent on 29 November 2016, just in time before DRIPA's scheduled expiry on 31 December 2016. The IPA provides a new legal framework to govern the use and oversight of investigatory powers of the executive branch. Among other things, it:

a includes new powers for UK intelligence agencies and law enforcement to carry out targeted interception of communications, bulk collection of communications data and bulk interception of communications;

b introduces an Investigatory Powers Commission (IPC) to oversee the use of all investigatory powers, alongside oversight provided by the Intelligence and Security Committee of Parliament and the Investigatory Powers Tribunal;

c requires a judge serving on the IPC to review warrants authorised by a secretary of state for accessing the content of communications and equipment interference before they come into force (commonly referred to as a 'double lock' feature);

d requires communication service providers (CSPs) to retain UK internet users' internet connection records for one year;

e permits police, intelligence officers and other government department managers to see the internet connection records as part of a targeted and filtered investigation, without a warrant;

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

© 2017 Law Business Research Ltd

f imposes a legal obligation on CSPs 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);

g places the Wilson Doctrine (a convention whereby police and intelligence services are restricted from intercepting communications of Members of Parliament) on a statutory footing for the first time, as well as safeguards for people such as journalists, lawyers and doctors involved in other sensitive professions;

h provides local government some investigatory powers, for example to investigate someone fraudulently claiming benefits, but not access to internet connection records;

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

j creates a new criminal offence for a CSP or someone who works for a CSP to reveal that data have been requested.

Only the data retention portions of the IPA have been enacted so far, meaning the other parts of the UK interception statutory regime (e.g., those provisions regulating access to communications data) are still governed by the legacy RIPA legislation. The government's intention is to repeal RIPA in its entirety in accordance with a yet-to-be-released implementation timetable. In light of the CJEU's response to the Court of Appeal's reference in *R (Davis & Watson)*,[74] it remains to be seen to what extent the IPA will survive as it currently sits on the statute books.

Protection for children

Currently, there is no legislation that specifically and expressly deals with the protection of children online in the UK. The Article 29 Data Protection Working Party's opinion on the protection of children's data states that businesses dealing with children's data should give regard to what is in the best interests of the children and the child's right to privacy.[75] Under the DPA, to fulfil the principle that children's data are processed 'fairly', stronger safeguards should be in place, and age-appropriate language is required for privacy notices to ensure that children's lack of maturity or understanding is not exploited.

The ICO has indicated,[76] in relation to the collection of personal data from children online, that consent of a parent or guardian will normally be necessary to collect personal data from children under the age of 12 (this would be raised to 13 under the new Data Protection Bill). However, whether consent will be valid, and the nature of the consent, will depend on the complexity of the data usage and the degree of risk associated with sharing the information in question. For example, the publication of photos of a child, and potentially of friends and family, would require a more specific form of parental consent and control (such as requiring the parent to register and actively consent on the site, and provide additional identification such as a credit card number), in comparison with requesting a child's email address for the sole purpose of sending a fan club newsletter that he or she has requested (in which case, a tick box consent on the site for the child to tick and clear unsubscribe instructions may be considered more appropriate).

74 Ibid.

75 Article 29 Data Protection Working Party – Opinion 2/2009 on the protection of children's personal data.

76 ICO's Personal Information Online – Code of Practice.

© 2017 Law Business Research Ltd

Parental or guardian consent is recommended by the ICO when the collection of information from a child is likely to result in:

a disclosure of the child's name and address to a third party, for example as part of the terms and conditions of a competition entry;

b use of a child's contact details for marketing purposes;

c publication of a child's image on a website that anyone can see;

d making a child's contact details publicly available; or

e the collection of personal data about third parties (e.g., where a child is asked to provide information about his or her family members or friends).

In May 2015, the ICO announced that it would review 50 websites and applications to comprehend exactly what information was routinely taken from children, how this was communicated to them and what parental permission was requested. This approach was mirrored by several other global bodies in an attempt to publish a combined report on the matter.[77] The results of this combined effort, reported in September 2015, raised concerns regarding 41 per cent of the material considered. Indeed, only 31 per cent of websites and applications had effective controls to limit the collection of data from children.[78] The ICO has stated that it will provide further guidance on the processing of children's data by the end of 2017.

Under the GDPR, children are defined as vulnerable natural persons who merit specific protection with regard to their personal data.[79] Consent to the processing of personal data in connection with the provision of online services to children (below the age of 16, unless a Member State provides, as the UK has done, for a lower age, which cannot not be lower than 13) is required to be given by a holder with parental responsibility.[80] The GDPR also introduces a 'right to be forgotten', which will make it necessary for certain service providers, such as social media services, to delete any personal data processed or collected when the user was a child.[81]

The Child Exploitation and Online Protection Centre (CEOP) works to prevent exploitation of children online; it is made up of a large number of specialists who work alongside police officers to locate and track possible and registered offenders. CEOP was previously affiliated with the Serious Organised Crime Agency; however, following its abolishment under the Crime and Courts Act 2013, the Centre became part of the National Crime Agency (NCA).[82] CEOP also offers training, education and public awareness in relation to child safety online.

Internet safety for children in the UK is also monitored by the UK Council for Child Internet Safety (UKCCIS), a group of 200 organisations collaborating to keep children safe online. Established in 2010, the UKCCIS, *inter alia*, provides advice for schools and colleges and creates guides for parents whose children are using social media.[83] It has published an Internet Safety Strategy for children in the UK.[84]

77 ICO website – News and Events.

78 Ibid.

79 General Data Protection Regulation: Recitals 38 and 75.

80 General Data Protection Regulation: Article 8.

81 General Data Protection Regulation: Article 17

82 Crime and Courts Act 2013.

83 Available at: UK Council for Child Internet Safety (UKCCIS): www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.

84 Click Clever Click Safe: The first UK Chid Internet Safety Strategy available at: https://www.ceop.police.uk/Documents/UKCCIS_Strategy_Report.pdf.

© 2017 Law Business Research Ltd

Website and software operators may apply for the Kitemark for Child Safety Online. This has been developed through collaboration between the BSI (the UK's national standards body), the Home Office, Ofcom, and representatives from ISPs and application developers. The BSI will test internet access control products, services, tools and other systems for their ability to block certain categories of websites (e.g., sexually explicit, violent or racist activity).

Cybersecurity

Cyberattacks are becoming increasingly problematic in the global financial and regulatory landscape. Government Communication Headquarters (GCHQ) stated that more than 80 per cent of UK companies reported a security breach in 2014. More worryingly, PricewaterhouseCoopers reported that the total amount of global incidents escalated to 42.8 million in 2015, a 48 per cent increase from 2013.[85]

The Computer Misuse Act 2000 (as amended by the Police and Justice Act 2006) sets out a number of provisions that make hacking and any other forms of unauthorised access, as well as denial of service attacks and the distribution of viruses and other malicious codes, criminal offences. Further offences exist where an individual supplies 'tools' to commit the above-mentioned activities.

The government has consolidated its focus on cybersecurity through the establishment of the National Cyber Security Programme with a dedicated pool of funds stretching to £1.9 billion over eight years until 2021.[86] Following the passage of the Crime and Courts Act 2013, the government brought the National Cyber Crime Unit (NCCU) under the remit of the NCA. The NCCU brings together cybercrime response operations and uses information on cybersecurity threats collected from the private sector via the Cyber-Security Information Sharing Partnership (known as CISP). A recent policy survey[87] reported that 68 per cent of large corporations reported a cyber breach in 2016, with 37 per cent experiencing a breach at least once per month, and with the most costly breach amounting to £3 million. To address this, the government has begun offering cybersecurity advice directly to businesses through publications such as the '10 Steps to Cyber Security', and by establishing an information-sharing partnership whereby the government and industry can exchange information about cybersecurity threats, and 58 per cent of businesses have undertaken five or more of the '10 Steps to Cyber Security'.[88] To reduce the risk of cyberattacks, the government established the Computer Emergency Response Team in March 2014[89] to take a lead in administrating the UK's response to national cybersecurity incidents. It has put an increasing emphasis on cyber skills, education and research to raise its cybersecurity strategy over the coming years. This includes ensuring that school children leave education with a basic understanding of cybersecurity, supporting a Cyber Higher Apprenticeship programme and launching Cyber First, which aims to identify and educate individuals to become the

85 Cybersecurity Regulation and Best Practices in the US and UK – Section 1.

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

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

88 Available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf.

89 Available at: www.gov.uk/government/news/uk-launches-first-national-cert.

© 2017 Law Business Research Ltd

UK's cybersecurity experts.[90] In addition, in October 2016, the government opened the National Cyber Security Centre, which now forms part of GCHQ and offers an authoritative voice on information security in the UK,[91] with one of its mandates being to produce advice in conjunction with the Bank of England to enable financial institutions to improve their management of cybersecurity.

At a European level, the European Parliament adopted the Network and Information Security Directive (NISD) in July 2016, which is the first EU-wide legislation on cybersecurity. The aim of the NISD is to enhance network and information system security in essential economic and digital services. It introduces, *inter alia*, mandatory breach notification requirements and minimum security requirements.[92] While the GDPR's aim is to protect personal data, the NISD focuses on protecting essential infrastructure, and is therefore not limited to personal data.

The NISD imposes obligations on two types of organisations: 'essential service operators' within the energy, transport, banking, financial market infrastructure, health, drinking water and digital infrastructure sectors; and 'digital service providers,' including entities such as online marketplaces, online search engines and cloud computing service providers. These companies must now report breaches of cybersecurity to the national competent authorities without undue delay where the relevant incident would have a significant impact on the core services provided by that company. The NISD had been stuck in negotiations between EU lawmakers and Member States over which sectors the Directive should cover; after months of negotiations, it was decided that digital platforms such as search engines, social networks and cloud computing service providers will be subject to the Directive's remit, albeit with 'lighter touch' requirements. The Directive aims to ensure a uniform level of cybersecurity across the EU as part of the Commission's wider Digital Agenda for Europe.

Member States have until 9 May 2018 to transpose the NISD into national law. In August 2017, the Department for Digital, Culture, Media and Sport released a public consultation on the proposed legislation that would implement the NISD. The NISD's implementation into UK law is part of a wider project by the government to invest £1.9 billion over five years in their National Cyber Security Strategy, ensuring the UK is up to date on cybersecurity protections. The consultation states:

- *a* the provisions will apply to operators of essential services with thresholds designed to capture the most important operators in their sector due to, for example, their size;
- *b* the legislation would be regulated by the National Cyber Security Centre, which would act as the UK's main point of contact as required by the NISD. However, this would be supported by an industry-specific regulator for, for example, the Transport and Business Energy and Industrial Strategy, Ofcom and NHS Digital;
- *c* operators caught must develop minimum levels of security, as well as evidence that these higher standards have been met; and
- *d* harsher penalties will be imposed to mirror the GDPR, with fines up to the higher of €20 million or 4 per cent of annual worldwide turnover.

90 The UK Cyber Security Strategy 2011-2016: Annual Report (Aprils 2016): www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

91 National Cyber Security Centre prospectus available at: www.gov.uk/government/publications/national-cyber-security-centre-prospectus.

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

© 2017 Law Business Research Ltd

The consultation ended 30 September 2017, after which the government is due to respond to any feedback by December 2017.

IV SPECTRUM POLICY

i Development

The current EU regulatory framework for spectrum has been in force since 2003 following the introduction of the Telecoms Reform Package. This regulatory framework, in particular the Framework Directive (2002/21/EC) and the Authorisation Directive (2002/20/EC), requires the neutral allocation of spectrum in relation to the technology and services proposed by the user (e.g., mobile network operators and radio broadcasters). Following on from the Telecoms Reform Package, the Commission required Member States to adopt measures including greater neutrality in spectrum allocation, the right of the Commission to propose legislation to coordinate radio spectrum policy, and to reserve part of the spectrum from the digital dividend (from the switchover to digital television services) for mobile broadband services through the Better Regulation Directive and the Citizens' Rights Directive. In 2016, Ofcom developed a framework for spectrum sharing, highlighting the importance of considering the circumstances of each potential opportunity, covering its costs and benefits.

In 2010, the Commission produced a Radio Spectrum Policy Programme (RSPP) detailing its key policy objectives and establishing general principles for managing radio spectrum in the internal market. The RSPP focuses on eliminating the digital divide, efficiently using spectrum, and promoting investments, competition and innovation. The RSPP also defines a road map for the next steps in the EU Radio Spectrum Policy, which was approved on 14 March 2012 and which focuses on the spectrum needs for 4G wireless broadband systems.[93]

In the UK, Ofcom is responsible under the Act for the optimal use of the radio spectrum in the interests of consumers. This includes, *inter alia*, monitoring the airwaves to identify cases of interference, and taking action against illegal broadcasters and the use of unauthorised wireless devices. The 2016 framework established three key elements when identifying potential sharing opportunities in certain bands: characteristics of use for all users that inform the initial view of the potential for sharing, and what tools may be relevant; barriers that may limit the extent of current or future sharing, despite the liberalisation of licences and existing market tools such as trading or leasing; and regulatory tools and market and technology enablers that match the characteristics of use and barriers to facilitate new and more intense sharing.[94]

ii Flexible spectrum use

As the uses of the radio spectrum have increased, the allocation of spectrum by the regulator has developed from a centralised system, where use was determined by the regulator, to a market-based approach, where users compete for spectrum. Currently, auctions are the primary market tool used to implement the allocation.

93 Available at:https://ec.europa.eu/digital-single-market/en/radio-spectrum-policy-programme-roadmap-wireless-europe.

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

© 2017 Law Business Research Ltd

Spectrum trading was introduced in the UK for the first time in 2004, and is permitted under the Wireless Telegraphy Act 2006 and associated regulations. Originally, the trading of spectrum was subject to a multi-stage process that, *inter alia*, required a decision by Ofcom about whether to consent to the trade. However, the Wireless Telegraphy (Mobile Spectrum Trading) Regulations 2011, directed at making more efficient use of the available spectrum, and improvements in mobile services to meet the demand for faster and more reliable services for consumers, made significant changes to this process, removing the need to obtain the consent of Ofcom for proposed trades in most cases. In addition, under the Regulations, the licensee can transfer all or part of the rights and obligations under its licence. A partial transfer, or 'spectrum leasing', can be limited to a range of frequencies or to a particular area. Ofcom also plans to simplify the process for time-limited transfers in line with the Revised Framework Directive.

In July 2013, Ofcom lifted the restrictions on spectrum currently licensed for 2G to allow the provision of 3G and 4G services and the trading of spectrum. Ofcom also amended the terms of current 3G licences so that the licences become indefinite as well as allowing users to trade spectrum. In return, mobile operators pay annual fees for the 900MHz and 1800MHz spectrum bands, which are those used to provide voice and data services using a mix of 2G, 3G and 4G technologies. In September 2015, Ofcom concluded that mobile operators should pay a combined annual total of £80.3 million for the 900MHz band and £119.3 million for the 1800MHz band, which is 13 per cent lower than Ofcom's earlier proposals in February 2015. The latest fees take into account the operator's requirement to provide voice coverage across 90 per cent of the UK landmass as well as the outcome of the spectrum auction in Germany, which concluded in June 2015.[95] The fee increase came into effect in two stages on 31 October 2015 and 31 October 2016, with annual payments now in effect.

In September 2013, the Ministry of Defence announced that Ofcom would be made responsible for the award of 190MHz of spectrum across current military bands, 2.3GHz and 3.4GHz, for civil use as part of the Public Sector Spectrum Release programme. This was due to be auctioned in December 2015, but following the Commission's investigation into the merger between Telefónica UK Limited and Hutchison, and Ofcom subsequently receiving letters from both Telefónica and Hutchison stating their intention to bring judicial review against Ofcom's decision to commence the auction before the Commission's decision on their proposed merger, Ofcom delayed the auction process. In October 2015, Ofcom published an information memorandum providing information for parties considering bidding in the awards process, but no spectrum has yet been awarded to any party.[96] In July 2017, Ofcom published a statement announcing auctions of the following spectra later in 2017: 190MHz in two frequency bands, 40MHz in the 2.3GHz band and 150MHz in the 3.4GHz band.[97]

In addition to the 2.3HGz and 3.4GHz bands, Ofcom continues to work with the government to consider which further spectrum used by the public sector may be available.

95 Available at: http://media.ofcom.org.uk/news/2015/annual-licence-fees-mobile-spectrum.

96 Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/71717/pssr-statement.pdf.

97 Available at: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2017/ofcom-sets-rules-for-mobile-spectrum-auction.

© 2017 Law Business Research Ltd

In April 2014, Ofcom published its spectrum management strategy setting out the approach to, and priorities for, spectrum management over the next 10 years.[98] The strategy noted, in particular, the increasing use of wireless services across the UK and the need to meet the increased demands with which the spectrum is faced. Ofcom proposed that it use a combination of market forces and regulations to support its strategic goals, which includes increasing the quality of radio frequency performance, providing greater information on spectrum use, repurposing some spectrum bands and providing for shared access to spectrum. As part of this, in September 2015 Ofcom published a consultation on using 10MHz of existing spectrum for new applications to be utilised for the IoT enabling M2M communications. Ofcom's aim was to encourage M2M applications to use spectrum that would enable them to connect wirelessly over longer distances. Following on from the September 2015 consultation, on 23 March 2016 Ofcom released a statement confirming that spectrum within the 55–68MHz, 70.5–71.5MHz and 80.0–81.5MHz bands could be used for IoT services and M2M applications.[99]

iii Broadband and next-generation mobile spectrum use

Ofcom issued a call for information on spectrum above 6GHz in January 2015, which ended in February 2015.[100] Following on from this call, in April 2016 Ofcom consulted on improving spectrum access for consumers in the 5GHz band. The results of the consultation remain to be seen, but Ofcom has subsequently set out plans to open up a 'sub-band' within the 5GHz frequency range for Wi-Fi, which would increase the number of 80MHz channels available for Wi-Fi from four to six to accommodate data-hungry applications and ease congestion. These extra channels, which are already being used in the US, could be opened up within the next few years.[101] In March 2017, Ofcom published a statement on its decision to open up the 5.8GHz band and make implementing regulations; this was predominantly due to increasing demand for Wi-Fi and the role of spectrum in addressing demand.[102]

The technology is expected to provide more capacity at faster speeds for mobile services on smartphones such as video streaming, email and social networking sites.

iv White space

Following an earlier consultation, 2011 saw Ofcom set out the use of free spectrum, or 'white space', made available from the UK's switch from analogue to digital TV and radio, for applications such as mobile broadband (particularly in rural areas) and enhanced Wi-Fi. Ofcom has estimated that the bandwidth available is equivalent to the spectrum available to current 3G services. The UK is the first country in Europe to progress its plans. 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

98 Available at http://stakeholders.ofcom.org.uk/binaries/consultations/spectrum-management-strategy/statement/statement.pdf.

99 A full copy of the statement is available at: www.ofcom.org.uk/__data/assets/pdf_file/0029/78563/vhf-iot-statement.pdf.

100 Laying the foundations for next generation mobile services, update on bands above 6GHz, Ofcom, 20 April 2015. Available at: http://stakeholders.ofcom.org.uk/binaries/consultations/above-6ghz/5G_CFI_Update_and_Next_Steps.pdf.

101 Available at: http://media.ofcom.org.uk/news/2016/speeding-up-wi-fi.

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

© 2017 Law Business Research Ltd

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.

Ofcom has released a statement that certain white space devices (WSDs) that operate automatically and without manual configuration are licence-exempt on the condition that they do not interfere with existing users.[103] In February 2015, Ofcom published a consultation on proposals for authorising other types of WSDs on a licensed basis.[104] This followed a pilot for innovative white space equipment that began in December 2013; none of the WSDs tested during the pilot demonstrated that they were capable of operating without some degree of manual configuration. Following the consultation, Ofcom decided to authorise manually configurable WSDs on a licensed basis while equipment that meets Ofcom's licence exemption regulations is developed. Ofcom will then review whether a licensing regime is still required by the end of 2018. Ofcom expects that the transitional licensing regime will enable the deployment of WSDs to begin sooner in the UK. However, to balance the likelihood that such manually configured WSDs have caused interference to incumbent users of the UHF TV band, Ofcom plans to introduce certain technical and non-technical licence conditions.[105] The final version of the European Telecommunications Standards Institute (ETSI) Harmonised European Standard for WSDs[106] has been published and delivered to the Commission. In February 2015, Ofcom published a statement allowing the commercial use and deployment of white space broadband technology, harnessing the unused parts of the radio spectrum in the 470MHz to 790MHz frequency band.[107]

Ofcom is also in the early stages of developing spectrum sharing. White space spectrum with a frequency in the spectrum bank 470MHz to 790MHz, which is not being used at particular times, is the key to developing such sharing. This would be enabled by location-aware wireless devices or databases that provide information on white space availability. Likewise, Ofcom set out in its Spectrum Management Strategy that it would place particular emphasis on spectrum sharing. In July 2015, Ofcom published a consultation in an attempt to identify barriers to sharing, include regulatory tools to facilitate further sharing and set out how sharing would be considered on a case-by-case basis. Since the consultation closed, nothing further has been published in relation to spectrum sharing.[108]

The DSM proposals include proposals relating to spectrum management that would, if adopted in their current form, have a significant impact in the UK (see Sections II.v and V.iv for more details).

v Spectrum auctions

The last spectrum auction was initially proposed to be in 2015, when licences were to be awarded in the 2.3GHz and 3.4GHz spectrum bands. The auction was postponed to 2016, and a total of 190MHz of high-capacity spectrum was to be made available in two bands,

103 Implementing TV White Spaces, Ofcom, 12 February 2015. Available at: http://stakeholders.ofcom.org.uk/binaries/consultations/white-space-coexistence/statement/tvws-statement.pdf.

104 Available at: http://stakeholders.ofcom.org.uk/consultations/white-space-coexistence.

105 Ibid.

106 ETSI EN 301598 V.1.0.0(2014-02).

107 Available at http://stakeholders.ofcom.org.uk/consultations/white-space-coexistence.

108 Available at: www.ofcom.org.uk/content/about/annual-reports-plans/ann-plans/Annual_Plan_Statement.pdf.

© 2017 Law Business Research Ltd

2.3GHz and 3.4GHz, which are those particularly suited to high-speed mobile broadband services. Ofcom planned to set reserve prices totalling £70 million for the spectrum. Most notably, there was to be no cap on the amounts bidders could buy, as Ofcom believes that buying large blocks has the potential to support fast download speeds, helping pave the way for 5G.[109] However, following the Commission's decision to block the proposed acquisition of O2 by CK Hutchison (H3G), Ofcom published a further consultation in November 2016 on competition measures and on specific aspects of auction design for the award of the 2.3GHz and 3.4GHz spectrum bands.[110] Ofcom subsequently announced the following spectrum caps in July 2017: a cap of 255MHz on the 'immediately useable' spectrum that any one operator can hold as a result of the auction; and a cap of 240MHz on the overall amount of mobile spectrum a single operator can hold as a result of the auction.

The aim of these is to ensure the reduction of BT/EE and Vodafone's overall share of mobile spectrum – the caps should have little impact on other bidders and will not restrict the amount that any other bidder could win.[111]

Prior to this postponed auction, the most prominent auction took place in February 2013, where Ofcom announced the results for the auction of the 800MHz and 2.6GHz bands. The auctioned spectrum, which was previously used for digital TV and wireless audio devices, was cleared by retuning TV signals in July 2013 and is now used for further 4G mobile services. After more than 50 rounds of bidding, Vodafone, O2 (Telefónica), EE and Hutchison 3G UK secured various bands of the newly released spectrum. Consequently, all major mobile networks in the UK started to provide 4G services from September 2013 in addition to EE. The next major auction in Ofcom's calendar, addressed in their latest Annual Report, is the auction of the 700MHz band, which is due to take place in late 2018 or 2019.

As Ofcom's auction process is designed to promote competition and coverage, Ofcom attached a coverage obligation to one of the 800MHz lots that was won by O2 (Telefónica). The provider accepted the obligation to widen the coverage of its mobile broadband for indoor reception to at least 95 per cent of the population by the end of 2017.

To ensure competition between the national operators, Ofcom introduced a floor and cap on the amount of spectrum that each of the operators can win, and imposed safeguard caps to prevent an operator from holding too much spectrum. To diversify the market, Ofcom also reserved parts of the spectrum for a fourth national wholesaler. The reserved lots were won by Hutchison 3G UK.

Despite the fact that the government budgeted a surplus of £3.5 billion for the auctioned spectrum, it only raised a total of £2.34 billion.[112]

vi Emergency services bandwidth prioritisation

The Universal Services Directive, a further part of the Telecoms Reform Package, introduces several extended obligations in relation to access to national emergency numbers and the single European emergency call number (112). Prior to the Universal Services Directive, obligations to provide free and uninterrupted access to national and European emergency numbers applied

109 Available at: http://stakeholders.ofcom.org.uk/binaries/consultations/2.3-3.4-ghz-auction-design/statement/statement.pdf.

110 Ibid.

111 Available at: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2017/ofcom-sets-rules-for-mobile-spectrum-auction.

112 Available at: http://www.bbc.co.uk/news/business-21516243

© 2017 Law Business Research Ltd

to providers of publicly available telephone services only. Under this Directive, however, these obligations are extended to all undertakings that provide to end-users 'an electronic communication service for originating national calls to a number or numbers in a national telephone numbering plan', and the UK has mirrored this wording in its revisions to General Condition 4 under the Act. Such electronic CSPs are therefore required to ensure that a user can access both the 112 and 999 emergency call numbers at no charge (and without the use of any cards or coins) and, to the extent technically feasible, make caller location information for such emergency calls (meaning information indicating the geographical position of the terminal equipment of the caller) available to the relevant emergency response organisations. In a January 2015 report entitled 'Citizens and communications services', Ofcom stated that it was monitoring the effectiveness of steps by the industry to improve emergency caller location information on mobile calls.[113]

In 2013, the Home Office announced the Emergency Services Mobile Communications Programme, which plans to provide a dedicated emergency services network (ESN) that would provide the next generation communication system for emergency services. However, one of the lots, relating to a contracted agreement for an MNO to extend guaranteed signal coverage to ensure mobile coverage, was withdrawn in January 2015. The remaining contracts for the operation of the ESN were won by EE and Motorola Solutions, which will now work to provide the UK's emergency services with a 4G LTE mobile network, replacing the existing private terrestrial trunked radio (Tetra) system.

To meet its contractual obligations, EE has asked for a variation of its Spectrum Access 2,100MHz licence to permit the use of LTE technology in the unpaired frequencies 1899.9 to 1909.9MHz. Following consultation, Ofcom issued a statement granting the requested variation in January 2017.[114]

V MEDIA

The UK media and entertainment industry continues to feel the effects of the advent of digital content and converged media platforms. The transition from traditional forms of media distribution and consumption towards digital converged media platforms is changing the commercial foundations of the entertainment and media industry in the United Kingdom. Politicians, lawyers, economists and members of the industry are all grappling with new business models to monetise content and control frameworks to provide sufficient protection for the rights of content creators and consumers alike. The Commission's DSM Strategy has wide-ranging implications for the UK media sector (subject to changes to national law as a result of Brexit). Proposals of particular relevance to the media sector include the proposal for a regulation on cross-border portability of online content services, the proposal for amendments to the Audiovisual Media Services Directive and the Commission's September 2016 proposals concerning updates to the European copyright law regime. In May 2017, the Commission published its mid-term review of its DSM Strategy.[115]

113 Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/92248/Citizens-and-communications-services.pdf.

114 Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0027/91575/EE-2100-MHz-Variation-Consultation_final.pdf.

115 Available at: http://europa.eu/rapid/press-release_IP-17-1232_en.htm.

© 2017 Law Business Research Ltd

i Restrictions on the provision of service

The service obligations and content restrictions described for the UK communications landscape in Sections I to IV apply to providers of digital content and converged media platforms. The regulatory framework described in these paragraphs applies to network operators and content providers alike in the context of the transmission of digital content across these converged media platforms.

ii Superfast broadband

By the end of 2016, the government's rollout of superfast broadband had reached 4.3 million homes and businesses across the UK. The nationwide rollout is on track to extend superfast broadband to 95 per cent of UK homes and businesses by December 2017. The focus is now shifting to exploring ways to take superfast broadband to the most remote and hardest-to-reach places in the UK (i.e., the remaining 5 per cent).[116] Seven market test pilots ran between June 2014 and March 2016 to test ways to take broadband to remote communities. The government published its findings in February 2016.[117] This is consistent with the DEA, which provides for a USO whereby consumers may request a minimum download speed of 10Mbps.

It is estimated that faster broadband will not only improve profits for UK businesses, but will create an additional 56,000 jobs in the UK by 2024. The work involved in the current rollout is expected to provide a £1.5 billion boost to local economies, and by 2024 it is hoped that the government's current investments in faster broadband will be boosting rural economies by £275 million every month, or around £9 million every day.[118]

iii Internet-delivered video content

Digital content has driven new forms of consumption of, and interaction with, media and entertainment content in the UK. This is primarily taking place on the internet and, as in other parts of the world, the UK has seen a rapid rise in the use of Web 2.0 and internet-delivered content via converged media platforms.

iv European DSM Strategy and media

The DSM Strategy proposals include proposals to revise the Audiovisual Media Services Directive (AVMSD), which coordinates national legislation on all audiovisual media including both TV broadcasts and on-demand services. Currently, AVMSD provides levels of harmonisation in areas such as accessibility for people with disabilities, promoting and distributing European works, commercial communications and protection of minors. The proposed revisions extend its application to 'video-sharing platforms' that tag, organise and target advertising around content and introduce an obligation to ensure that these content providers implement measures to protect minors from access to harmful content. To ensure equality in the promotion of European works, the original draft directive obliges on-demand services to ensure 20 per cent of the works in their catalogues are European

116 Available at: http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN06643#fullreport.

117 Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/497369/BDUK_Market_Test_Pilots_-_Emerging_Findings_Feb_2016.pdf.

118 Ofcom – The Office of Communications Annual Report and Accounts for the period from 1 April 2013 to 31 March 2014.

© 2017 Law Business Research Ltd

(although this quota may increase to 30 per cent pursuant to the latest European Parliament resolution). Furthermore, the proposal allows Member States to require on-demand services to invest in local content.[119] At the time of writing, the legislation is pending the outcome of interinstitutional trilogue talks between the Council, the European Parliament and the Commission.

The Commission has also placed an emphasis on considering the role of online platforms and has published a communication that proposes ways to foster development for such platforms.[120] The communication highlights basic principles about how it will ensure its DSM objectives through piecemeal legislative action. This includes proposing to maintain the intermediary liability regime under the e-Commerce Directive, the consideration of deregulation of traditional communication services rules and proposals to ensure that platforms are accountable to some extent for their content. In its mid-term review, the Commission identified online platforms as one of the three emerging challenges, and has proposed to implement actions to tackle these challenges.[121]

On 9 December 2015, the Commission proposed legislative actions in areas including cross-border portability of online content services.[122] The new regulation on portability of online content services was published in the Official Journal on 30 June 2017,[123] and is due to apply from 1 April 2018.[124]

The main point of the compromise text is that the providers of online content services that are provided for payment must ensure the cross-border portability of their services such that subscribers may access and use the services when 'temporarily present' in another Member State. When verifying the subscriber's Member State of residence, the service provider must limit the means to verify residence to two means of verification in a list (such as, for example, an identity card and payment details).

On 25 May 2016, the Commission proposed a regulation prohibiting geo-blocking of the sale of goods and the provision of services in the EU.[125] A compromise text is now being discussed in the course of the trilogue of the Council and the European Parliament. It is important to note that the Commission's proposal excludes a number of services from the scope of the regulation: namely, audiovisual services and copyright-protected works such as music or e-books, except where the copyright-protected work is supplied to the customer in the premises of the trader or in a physical location where the trader operates.

119 Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016PC0287&from=EN.

120 'Online Platforms and the Digital Single Market; Opportunities and Challenges for Europe' SWD (2016) 172 available at: https://ec.europa.eu/digital-single-market/en/news/communication-online-platforms-and-digital-single-market-opportunities-and-challenges-europe.

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

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

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

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

125 'Proposal for a regulation of the European Parliament and of the Council on addressing on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No. 2006/2004 and Directive 2009/22/EC' SWD (2016) 173 and 174 available at: http://ec.europa.eu/DocsRoom/documents/16742.

© 2017 Law Business Research Ltd

On 14 September 2016, in addition to the telecoms proposals outlined in Section II.v, the Commission adopted new proposals for copyright reform as part of its DSM Strategy. The Commission released proposals for a regulation laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes (Copyright Regulation);[126] a directive on copyright in the DSM (Copyright Directive);[127] and proposals for an additional directive and regulation to implement the Marrakesh Treaty to Facilitate Access to Published Works for Persons who are Blind, Visually Impaired, or Otherwise Print Disabled (Marrakesh Treaty).[128]

The Copyright Regulation introduces a cross-border clearance mechanism for digital broadcasting by broadcasters and retransmission of broadcasts online. Currently, broadcasters transmit programmes on their services that they have licensed from others or produced themselves, but programmes will inevitably contain content that is protected by copyright and needs to be cleared for use. Through the Copyright Regulation, the Commission proposes to extend the 'country of origin' principle[129] – which has been in place for decades in respect of cable and satellite communications – to specific online services, including simultaneous online transmissions of a broadcast, 'catch-up' television services and associated ancillary services such as 'the making of' programmes. This means that broadcasters will only need to clear rights once, in the Member State from which their broadcast originates. However, it only applies to online broadcasts and does not apply to VOD services. The Copyright Regulation also proposes to extend the current system of mandatory collective management for retransmissions by cable of television and radio broadcasts from other Member States to other closed electronic communication networks, such as IPTV. This means that instead of negotiating individually with every rights holder, operators who offer packages of channels will be able to obtain licences from collective management organisations.

The Copyright Directive focuses on three areas. First, it introduces measures to achieve a well-functioning marketplace for copyright. These include proposals for:

a a new related right in publication that will allow publishers to charge fees for digital uses of the copyright works they have invested in the distribution of, including where small amounts of text are used in hyperlinks;

b a requirement on online user-uploaded content platforms to take measures to ensure the protection of user-uploaded works (e.g., by implementing content recognition

126 Available at: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-laying-down-rules-exercise-copyright-and-related-rights-applicable-certain.

127 Available at: https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market.

128 Proposal for a Regulation of the European Parliament and of the Council on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject-matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print disabled – COM (2016) 595, 14 September 2016; and Proposal for a Directive of the European Parliament and of the Council on certain permitted uses of works and other subject-matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print disabled and amending Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society – COM (2016) 596, 14 September 2016; available at: https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules.

129 Set out in the Satellite and Cable Directive (Directive 98/83/EEC), this principle allows broadcasters to clear rights for satellite broadcasting in one Member State and allows them to then make their satellite transmissions available in other Member States.

© 2017 Law Business Research Ltd

software) to address rights holders' concerns as to the 'value gap' (between the ease with which popular content is accessed online and the arguably meagre profit that rights holders reap from it); and

c a mechanism for increasing the transparency to rights holders of the exploitation of their works, with an alternative dispute resolution procedure to allow authors and performers to 'rebalance' contracts.

Second, it introduces measures to improve licensing practices and ensures wider access to content by:

a implementing legal mechanisms to facilitate easier licensing of 'out-of-commerce' works (which are works that are not available to the public through customary channels of commerce and cannot be reasonably expected to become available) by cultural institutions to aid cultural institutions in making these works, which have significant cultural and educational value, available to the public; and

b requiring Member States to set up impartial bodies to assist in the negotiation of licensing agreements between audiovisual rights holders and VOD platforms.

Third, the Directive introduces measures to adapt exceptions and limitations to the digital and cross-border environment in relation to research organisations conducting text and data mining; the digital use of works and other subject matter for distance-learning educational purposes; and cultural heritage organisations making digital copies of their permanent collections for preservation purposes.

The European Parliament and the Council are now discussing these legislative proposals under the co-decision procedure. As such, it is unlikely that these proposals will become binding in Member States sooner than 2019 or 2020.

The directive designed to implement the Marrakesh Treaty introduces a new mandatory exception to the copyright rights harmonised under EU law, allowing people who are blind or otherwise print-disabled to access books and other content in formats that are accessible to them, including across borders. The regulation governs the exchanges of accessible format copies between the European Union and third countries that are parties to the Marrakesh Treaty. The regulation and directive implementing the Marrakesh Treaty were published in the Official Journal on 20 September 2017. The regulation will apply from 12 October 2018.[130] Member States must implement the directive by 11 October 2018.[131]

The Commission has also investigated the practices of six major US film studios (Disney, NBCUniversal, Paramount Pictures, Sony, Twentieth Century Fox and Warner Bros) with respect to clauses in their licensing agreements with telecommunications company Sky UK. On 26 July 2016, the Commission accepted commitments from Viacom-owned Paramount to end a probe into potentially anticompetitive film licensing contracts, but confirmed that it continues to investigate five other studios and Sky UK. As a result, Paramount has agreed to stop enforcing contractual clauses that prevent European consumers outside the UK and Ireland watching Paramount films on Sky's UK satellite and online channels; and prevent rival broadcasters from airing its pay-TV content in the UK. In practice, this means that

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

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

© 2017 Law Business Research Ltd

Paramount will no longer insert geo-blocking restrictions in its licensing contracts with broadcasters. The current probe deals only with Sky UK in the UK and Ireland, but the Commission is also investigating the British pay-TV operator's approach to consumers in France, Italy and Germany. Likewise, Paramount will not introduce or renew similar geo-blocking clauses in film licensing contracts with other broadcasters that operate in other European countries. Paramount will run the commitments package for five years, and it will cover both standard pay-TV and on-demand services, both online and by satellite. The effect of the Commission accepting the commitments is that the studio will not be required to pay a fine, nor to admit liability. Notably, the five other studios have not offered similar undertakings. On 6 February 2017, details were published of an appeal by Canal+ against the Commission's decision to accept commitments from Paramount.[132]

The case is ongoing. It is, as yet, unclear what effect a final decision against the studios will have on consumers, but it could have a profound effect on the film industry in Europe. However, in spite of these commitments and the ongoing investigations, broadcasters will be under no obligation to offer packages outside their territories following the decision. Indeed, given that copyright is granted on a national basis, and is not yet harmonised under EU law, broadcasters could face copyright-infringement cases if they offer films in territories in which they do not have a licence.

v Web 2.0

Web 2.0 is characterised as facilitating communication, information sharing, interoperability and collaboration for users of the internet. Users are empowered and encouraged to play a more active role in the creation and consumption of content, which has given rise to the concept of user-generated content (UGC). UGC has created issues of liability and ownership that have been addressed to some extent by legislation (see the references to the Digital Economy Act 2010 in Section III.iii) and in court. The application of the Digital Economy Act 2010 is reliant on the ability of copyright owners to notify ISPs of potential copyright infringement. To do this, copyright owners will send details of the infringement, including IP addresses, to ISPs. However, courts in the UK continue to cast doubt over the use of an IP address as evidence that an individual has downloaded content unlawfully. Given this, as well as US authorities suggesting that a provider of Web 2.0 content will not be liable for copyright infringement if it removes material from its site when notified by the copyright owner, along with the formal challenges to the Digital Economy Act 2010 (see Section III.iii), it remains to be seen how the Digital Economy Act 2010 will be interpreted in the UK in the future.

On 26 June 2012, Ofcom issued a consultation on the Online Infringement of Copyright (Initial Obligations) (Sharing of Costs) Order (Sharing of Costs Order), which was laid before Parliament. The consultation, which closed in September 2012, addressed how Ofcom should calculate the level of charges that participating copyright owners will have to pay to Ofcom for the costs of setting up and running a scheme for reporting online copyright infringement under an 'initial obligations code' for ISPs. However, in February 2013, the Sharing of Costs Order was withdrawn over concerns that it may not comply with the Treasury's Managing Public Money guidelines. In response to a freedom of information request, Ofcom disclosed that it had spent £1.8 million on taking action against online copyright infringements in accordance with the Digital Economy Act in 2011 and

132 Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2017:038:FULL&from=EN.

© 2017 Law Business Research Ltd

2012. Following the Treasury's announcement, the DCMS stated in May 2013 that technical changes to the draft Sharing of Costs Order were required. There has been no update at the time of writing.

On 19 July 2014, the coalition government announced the launch of Creative Content UK and pledged £3.5 million in funding. This is a programme between industry and ISPs to heighten awareness of copyright infringement online and introduce a subscriber alert programme. The subscriber alert programme, which was initially known as VCAP and has now evolved to encompass the 'Get It Right From A Genuine Site' campaign discussed above (see Section III.iii), involves owners sending evidence of copyright infringement to ISPs which will in turn issue letters of warning to their subscribers. Rather than being threatening, these letters are intended to be educational. A number of organisations such as Sky, BT, TalkTalk and Virgin Media have signed a memorandum of understanding that will underpin the Creative Content programme.

vi OTT delivery of content and live TV

An OTT platform is typically a platform that allows users to stream audiovisual content using the internet or mobile telephone networks. The key benefit of OTT delivery is that it allows a user to interact with the content because data can flow both ways in an IP network. OTT delivery is growing rapidly in the UK, and this growth is predicted to continue.

OTT delivery is utilised by a range of content providers in the UK, including PSBs (i.e., iPlayer, ITV Hub, All 4 and My5), cable and satellite platforms (e.g., both Virgin Media and BSkyB offer VOD products), mobile operators, online aggregators and standalone VOD platforms (e.g., Netflix, Amazon Prime and NowTV).

To further facilitate user access to internet-delivered services, the BBC, ITV, Channel 4, Channel 5, BT, TalkTalk and Arqiva collaborated on an open-technology offering called YouView, which enables viewers with Freeview or Freesat and a broadband connection to access catch-up and on-demand programming via their televisions.

According to Ofcom's Communications Market Report 2017, the amount of time UK adults spend watching live TV has fallen since 2010, with a decline in average daily viewing time of 36 minutes to three hours and 51 minutes per adult per day in 2016. However, live TV was still watched by 91 per cent of UK adults in an average week in 2016. The increased demand for on-demand and streamed content delivered over the internet is an important indication of the way in which people watch television. 67 per cent of adults use PSB online services such as BBC iPlayer, whereas subscription services such as Netflix and Amazon Prime are used by 45 per cent of adults. BBC iPlayer was the most popular choice, with 63 per cent of UK adults citing it, followed by ITV Hub (40 per cent) and YouTube (38 per cent). These figures apply even though from 1 September 2016 the law changed requiring online content watchers to pay for a TV licence to watch BBC iPlayer. Ofcom highlighted the growing gap between the live broadcast TV viewing habits of older and younger viewers, with over-64s watching an average of five hours and 44 minutes a day in 2016, up 50 minutes from 2006, whereas 16 to 24 year olds watched an average of one hour and 54 minutes, 41 minutes less than in 2006.[133]

The BBC Royal Charter was renewed in early 2017, where from 3 April 2017 a unitary Board replaced the two-tier structure of the BBC Trust and the BBC's Executive Board as

133 Available at:https://www.ofcom.org.uk/__data/assets/pdf_file/0017/105074/cmr-2017-uk.pdf.

© 2017 Law Business Research Ltd

the BBC's governing body. Ofcom also became the BBC's first external regulator, developing an 'Operating Framework' for the BBC that covers regulation of the BBC's performance, compliance with content standards and impact on competition.[134]

vii Mobile services

In its annual report for 2017 to 2018, Ofcom details how it will make spectrum in the 700MHz band available for mobile data use by May 2020. As this part of the spectrum is currently used for DTTV services and wireless microphone usage, making the band available will mean that DTTV and audio will no longer be able to use the spectrum. Ofcom is aiming to make the band available while safeguarding the benefits that DTTV and audio provide to consumers. It intends to work closely with stakeholders to develop a plan for the DTTV infrastructure modifications needed as well as working with government and industry and consumer groups.

VI THE YEAR IN REVIEW

i Brexit referendum

In the Brexit referendum on 23 June 2016, the United Kingdom voted to leave the EU by a vote of 51.9 per cent in favour of 'leave' to 48.1 per cent in favour of 'remain'. The government invoked Article 50 of the Treaty on European Union on 29 March 2017, thereby starting the period of negotiation between the United Kingdom and the EU on the terms of the United Kingdom's exit, with exit taking effect once those negotiations have concluded or after two years (if sooner), irrespective of what terms have been agreed. The government has since introduced the European Union (Withdrawal Bill) (commonly referred to as the Great Repeal Bill) in Parliament in which the government would repeal the European Communities Act 1972, end the jurisdiction of the CJEU over the UK, enshrine existing EU legislation into British law and permit the government to remove or amend EU laws that apply to the UK (whether directly effective or enshrined in UK law by a separate Act of Parliament) with secondary legislation via the 'Henry VIII clauses'. It is proposed that the Great Repeal Bill be passed into law before the actual Brexit date, but it currently includes commencement provisions that will enable ministers to bring it into force as and when they choose (the Great Repeal Bill refers throughout to an 'exit date', but no further specification is provided). It is anticipated that the final form of any ensuing legislation will be the subject of much debate. Practically, until we have more certainty about how Brexit is likely to look, we consider it prudent to continue to move forward as if existing EU legislation and EU legislation that comes into force prior to Brexit will continue to apply to the United Kingdom post-Brexit until we have more information about the post-Brexit status quo.

ii Commission proposals for a DSM Strategy

The Commission's ambitious DSM Strategy proposals (announced 14 September 2016) signpost that Europe's approach to digital market access is likely to:

a change significantly;
b dramatically enhance Europe's connectivity;
c rationalise its telecoms regulatory regime;

134 Available at: https://www.ofcom.org.uk/consultations-and-statements/ofcom-and-the-bbc.

© 2017 Law Business Research Ltd

d end unjustified geographical restrictions on content; and
e reform the European copyright regime in favour of European interests.

However, the proposals are ambitious both in terms of scale and cost: using the 5G Action Plan as an illustrative example, the Commission estimates that €500 billion in private investment will be required to deliver its 5G Action Plan, of which it is projected there will be a €155 billion shortfall based on current investment trends. The Commission has indicated that part of the intent of the reforms is to stimulate competition and investment in the sector, but has also proposed the creation of a European Broadband Fund (to comprise both private and public funds) to help make up this shortfall. This proposal has yet to be tabled, but if the Commission's ambitions are to be met, it seems that a substantial amount of new or reallocated public funding for next generation telecoms infrastructure is forthcoming. While the WiFi4EU initiative will be funded by the EU (for installation and equipment costs only) for an initial budgeted amount of €120 million, €70 million of this is reallocated funding from the Connecting Europe Facility. Only €50 million will be previously unallocated funds.

It will be important to closely follow the progression of these proposals through the European Parliament and Council of the Member States' co-decision procedure, as it is likely that certain of these proposals will be softened before they are adopted.

VII CONCLUSIONS AND OUTLOOK

Recent years have seen privacy debates continued both inside and outside the courtroom, highlighting the ever-evolving regulatory landscape and the ongoing legal controversies about the scope and extent of a citizen's right to privacy. The implementation of the GDPR has been a milestone in the area of data protection law, and companies will have to be in a position to be compliant with its provisions, which will come into force on 25 May 2018, especially in light of the introduction of high fines for breaches of the GDPR. A close eye should also be kept on the developments of the Draft ePrivacy Regulation as it continues through the legislative process.

Following its fast-tracked introduction in 2014, the DRIPA legislation was declared incompatible with EU law on the basis that its data retention provisions violated the right to respect for private life and the protection of personal data, and its replacement, the IPA, might have to be amended in light of the pending UK Court of Appeal's interpretation of the CJEU's findings in *R (Davis & Watson)*.

An EU–US Privacy Shield is now in place to provide a legal basis for transfers of personal data to the US from the EU (replacing the Safe Harbor framework), but is still the subject of further claims by privacy campaigners that it remains insufficient. Furthermore, the standard contractual clauses are also being challenged in the courts. These 'solutions' for transferring data will have to be updated to reflect the requirements of the GDPR in due course.

Brexit will undoubtedly have an influence on the policy and regulatory landscape in the UK and the EU27. The extent and nature of this will become clearer as more specific details emerge from the UK's domestic legislative proposals to implement Brexit and its Brexit negotiations with the EU27.

© 2017 Law Business Research Ltd

Appendix 1

ABOUT THE AUTHORS

JOHN D COLAHAN

Latham & Watkins LLP

John Colahan is based in Latham & Watkins' London office and divides his time with the Brussels office. He is a member of the global antitrust and competition practice, having previously been a legal adviser at the UK Cabinet Office and international competition law counsel at The Coca-Cola Company. John represents clients before the European Commission, national authorities in Europe and internationally, as well as conducting litigation in the European courts and numerous national courts. He has advised on a variety of international antitrust and regulatory matters, including structuring and implementation of international mergers, acquisitions and joint ventures, cartel enforcement, single firm conduct, regulatory access and compliance counselling. He has covered a wide range of markets including telecommunications and media.

GAIL CRAWFORD

Latham & Watkins LLP

Gail Crawford is a partner in Latham & Watkins' London office. Her practice focuses primarily on technology, data privacy and security, intellectual property and commercial law, and includes advising on technology licensing agreements and joint ventures, technology procurement, data protection issues, and e-commerce and communications regulation. She also advises both customers and suppliers on multi-jurisdictional IT, business process and transformation outsourcing transactions. Ms Crawford has extensive experience advising on data protection issues, including advising a global corporation with operations in over 100 countries on its compliance strategy, and advising a number of US e-commerce and web businesses as they expand into Europe and beyond. She also advises online businesses and providers of communications services on the impact of the UK and European restrictions on interception and disclosure of communications data.

LISBETH SAVILL

Latham & Watkins LLP

Lisbeth Savill is a partner in Latham & Watkins' London office and a member of its entertainment, sports and media practice. She focuses on commercial work in the media and entertainment sectors including financing, distribution and licensing arrangements for audiovisual content, and the purchase, sale and financing of entertainment companies. Her

© 2017 Law Business Research Ltd

clients cover a wide range of interests in the entertainment and media sectors including equity and debt financiers, major studios, independent producers, rights holders and distributors of film and television content. Lisbeth has been recognised as a leading lawyer in the film and television industries for many years. She is actively involved in issues important to the entertainment sector and is currently also the Deputy Chair of the British Film Institute, the lead body for film in the UK.

LATHAM & WATKINS LLP

99 Bishopsgate
London EC2M 3XF
United Kingdom
Tel: +44 20 7710 1000
Fax: +44 20 7374 4460
john.colahan@lw.com
gail.crawford@lw.com
lisbeth.savill@lw.com

www.lw.com

© 2017 Law Business Research Ltd

Strategic Research Sponsor of the
ABA Section of International Law

ISBN 978-1-910813-90-4

© 2017 Law Business Research Ltd