

Privacy, Security and Politics: Current Issues and Future Prospects

Benson, V & Turksen, U

Published PDF deposited in Coventry University's Repository

Original citation:

Benson, V & Turksen, U 2017, 'Privacy, Security and Politics: Current Issues and Future Prospects' *Communications Law - Journal of Computer, Media and Telecommunications Law*, vol 22, no. 4, 22(4), pp. 125-132 <u>https://www.bloomsburyprofessional.com/uk/journal/communications-law-17467616/</u>

ISSN 1746-7616

Publisher: Bloomsbury Professional

Copyright © and Moral Rights are retained by the author(s) and/ or other copyright owners. A copy can be downloaded for personal non-commercial research or study, without prior permission or charge. This item cannot be reproduced or quoted extensively from without first obtaining permission in writing from the copyright holder(s). The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the copyright holders.

105 106 107 108 110 111 111 112	100 101 102 104 105	98 97 95	90 91 92 94	89 88 87 86	85 83
 Ito J See n 10, para 5. Ito Bidd, para 11. See n 14, Editors Codebook, 74. Public Order Act 1986 s 18. Public J Sea and 298. Public		reassignment or identity, martial or civil partnership status, pregnancy, race, religion, sex or sexual orientation' Where it refers both to disability and mental health. See n 23 (Pt U recommendation 38. See Alex Dyke (IBBC Redio Solent) Ofcom Broadcast Bulletin, Issue 292, 9 See Alex Dyke (IBBC Redio Solent) Ofcom Broadcast Bulletin, Issue 292, 9 November 2015. Consultation, 29 September 2016, point 9 http://www.impress.press/downloads/ Consultation, 29 September 2016, point 9 http://www.impress.press/downloads/ Elle/Code/equalities-and-human-rights-commission.pdf accessed 27 October 2017.	3:2.1 "They must not violate human rights, incide hate and the infringement of lawful right against peoples, nations, nationalities, denominations and races." See, for example, Armenian Code of Conduct for Media Representatives, principle 5.3. 'Not to advocate war, violence or pornography in any form." Editors Code, of 1.2. Standards, Code, of 4.4. Crime and Disorder Act 1998, s 28(4), and see R v Rogers [2007] 2 AC 62 for its application. The Standards Code, principle 5.3. 'Not to advocate war, violence or pornography in any form." Editors Code, of 1.4. Crime and Disorder Act 1998, s 28(4), and see R v Rogers [2007] 2 AC 62 for its application. See 11533-16. Miller v Mail Online, prat 15 https://www.ipso.co.uk/tulings-and-see lawful to a priorable member Act 1941 presorts and actions are disability and make prejudicial or peiorative reference to a preson on the basic of that newcork sea disability enders and the service of that newcork sea disability enders and the new preson on the basic of that newcork sea disability enders and the new preson on the basic of that newcork sea disability enders and the new preson on the basic of that newcork sea disability enders and the new preson on the basic of that newcork sea disability enders and the new preson on the basic of that newcork sea disability enders and the new preson on the basic of that newcork sea disability enders and the new preson on the basic of that newcork sea disability enders and the new preson on the basic of that new preson the new preson on the basic of that new preson the new preson on the hask of that new preson the new preson on the hask of that new preson the new preson on the basic of that new preson the new preson the new preson on the hask of that new preson the new preson preson on the hask of that new preson the new preson the new preson on the hask of that new preson the	Luxembourg Press Council's Code of Ethics, art 1(c' 'prohibitionol racia), ethici, religious and ledological discrimination." See Bulgaria Media Code 2004, para 2.5.2; Cuidelines of the Netherlands Press Council, "Publications only state the ethnic origins, nationality, race, religion and sexual inclination of goups and individuals if this is deemed net necessary for a proper understanding of the facts and circumstances that are reported on.' See Journalist' Association of Serbia's Code of Ethics, art 1X1 'In reporting crimes, national, racial, religious, teological and publical affiliation, as well as sexual orientation, social and marital status of suspects or victims, are mentioned only in case when the orientation, citizenship or status are directly related to the type and nature of a committed crimical offset." See for example, National Association of Hungarian Journalist' Ethics Code,	See MPRESS: The Independent Monitor for the Press CIC Regulatory Scheme, See MPRESS: The Independent Monitor for the Press Recognition Panel in respect of the application for recognition from MPRESS: The Independent Monitor for the Press CIC http://presserecognitionpanel.org.uk/wp-content/ updads/ 2016/07/IMPRESS: Regulatory-Scheme.pdf, accessed 20 October 2017. Ionathan Heavood and Bright Moris: Press codes and the spirit of equalities legislation: implementing Leveson' (2016) 21 CL 29, 29.
 131 Santards Code, 2.4. 152 See N728; 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing DF 95/46 CE (Ceneral Data Protection Regulation), epg 17, Coogle Spain SL, Coogle Incv Vepraia Española de Protección de Datos, C-131/12. 155 Standards Code, cl 3.3. 156 See n 145, 233. 	 www.lpsi.co.uk/press-surfuction/usin/anice-uk/purinaliss-intra-culorssociar- media-guidance, accessed 2 November 2017. 142 Guidance, para 7.27. 143 Ibid, para 7.28. 144 User generated content', ONAethics website, undated https://ethics.journalists org/optics/user-generated-content/, accessed 24 October 2017. 145 New technologies, new technolycus' ch lo David Cordon et al (eds), Controversies in Media Ethics (3rd eth, Routledge, 2011) 218-19. 146 See Croatia Journalist' Association Code of Honor, principle 23. 147 Ibid: Council of Mass Media Finland, Amer to guide/iners. Material generated by the public on a news website; Online News Association, Greece. 148 See n 144. 149 Guise 2.12. 150 Guidence, para 2.12. 	 Sandards Code, public interest proviso. Sandards Code, public interest proviso, point (i). Gandards Code, public interest proviso, point (i). Sandards Code, public interest proviso, point (i). TMPRESS Publishes Draft Standards Code,' IMPRESS website, 18 August 2016, https://mpress.press/news/dtaft-standards-code.html, accessed 24 October 2017. Standards Code, cl 7.2(b). Bandards Code, cl 7.2(b). Bida, cl 3.3. Hot Guidance for Journalists: Using Material from Social Media (IPSO, 2017) https:// https://dxiance.org/optic/sandards/code/sandards/code/ 141 Guidance for Journalists: Using Material from Social Media (IPSO, 2017) https:// https://dxiance/sandards/code/sandards/code/sandards/code/ 141 Guidance for Journalists: Using Material from Social Media (IPSO, 2017) https:// https://dxiance/sandards/code/sandards/co	 Kan Harris, 'Newspaper industry releases revised 'Editors' Code', more comfore for tabiodis, nothing for the public,' Hacked Off website, 4 December 2015 http://hackinginquiry.org/comment/newspaper-industry-releases-revised-editors- code-more-comfort-for-tabloids-nothing-for-the-public/, accessed 23 October 2017. Inserting s 4 3B into the Employment Rights Act 1996. Tal Editors' Code, public interest proviso, point 2. See n 23 fPt, para 4,24,3 version of the editors' code of practice' (2016) 27 Entertainment Law Keview 92-97, 97. Bidd 	 Bid, el Z. Bid, el Z.	 Editors' Code, cl 3 Januards Cude, cl 3 - Z(a). Editors' Code, cl 10(a); Sandards Code, cl 5 - Z(a). Editors' Code, cl 10(a); Sandards Code, cl 5 - Z(a). See Editors' Code, public interest proviso, point 5 (in regards to 'override the normality paramout'i interest of children under 16); Sandards code, cl 3 1. (photograph or interview child under 16 without consent) 3.2 (identify child under 16 without his consent). Editors' Code, cl 5.

Privacy, security and politics: current issues and future prospects

Vladlena Benson and Umut Turksen

Privacy is an essential prerequisite to the exercise of individual freedom, and its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based in this country.¹

Overview

Individual privacy and national security have been regarded as notions with a conflicting impact. As seen in the UK general election 2017, security has taken a prominent role on the envertise Party agenda while public perceptions on privacy were split. This article reviews the election manifestos of three political parties on privacy and security. We use the pre-election YouCov survey of 2017 UK respondents to understand the views of the public by age groups and gender. While there is general support for legislation aimed at strengthening national security and crime prevention, such as the Investigatory Powers Act 2016, the younger segment of the UK population is increasingly concerned with the infringement of their privacy (both in traditional and online settings). These contrasting views may explain the outcome of the general election in 2017, and offer open questions for legislators.

The online privacy debate mutates in postelection Britain

The terrorism threat level in the UK has been 'severe' since 2014, and with four terror and several major cyber-attacks in recent months? it is likely to remain as such in the immediate future.³ The use of encrypted communication by terrorists has led to increasing pressure upon companies to allow law enforcement agencies to bypass well-established privacy safeguards.⁴ In addition, the recent cyber-attack that crippled the NHS demonstrated why cybersecurity is a vital issue and one that can affect the well-being and economy of an entire country. These events reminded people what is at stake when deciding what data gathering and surveillance powers the government should have in the context of public safety and national security.

around government surveillance, powers to bypass security forthcoming proposed legislative changes. giants, including social media firms, remain to be answered by proposed control and financial penalties for digital economy mechanisms of individual online and communication profiles debate on privacy laws in the UK is evolving. Yet the questions this context of both private and public security settings where the businesses, commercial advantage¹⁰ and state functions.¹¹ It is in an economic and a sentimental value for us but also value for in the 'digital woods'' as a 'virtual treasure trove' not only have The consequent digital foot-print, assets and behaviour left behind and digital presence increase with the activities people pursue. thett has been reported to be at epidemic levels in 2017.° Unline themselves vulnerable to criminal activity.' For example, identity want their privacy to be protected because they are also making tutions (eg banks, travel agencies) as a matter of necessity, they government (eg the NHS, HMRC) and non-government instireadily impart their personal/private information and data to both of suspects.⁶ While citizens increasingly use online services and surveillance evidence can lead to a collapse of the prosecution security.5 Thus, the failure to collect and retain such data or in criminal investigations, public protection and ensuring national Surveillance and communications data are seen as vital elements

This article aims to provide insights as to the differences between three political parties in their approaches to the UK online security and privacy following the 2017 general election¹². In doing so it identifies main concerns and areas of uncertainty.

The Introduction

In the UK, there is no dedicated statute on privacy as such, and thus relevant legal provisions need to be extracted from a number of international, regional and national legal instruments, and the jurisprudence of the European Court of Human Rights (ECHR) including the International Covenant on Civil and Political Rights 1966; the European Convention on Human Rights 1950; the UK Human Rights Act 1998 (HRA)¹¹ the Data Protection Act 1998; the Regulation of Investigatory Powers Act 2000; the

it is worth paying attention to the definition provided by Privacy them is communicated to others',16 for the purposes of this article themselves when, how, and to what extent information about traditionally defined as 'the ability for people to determine for they do not provide a definition of privacy. While privacy is to give us the ability to invoke our rights against undue interfe-International rence and significant power imbalances in the context of privacy Regulation (GDPR) 2016.15 While these instruments are meant the European Union 2007;¹⁴ and the EU General Data Protection Investigatory Powers Act 2016; the Treaty on the Functioning of

which many other human rights are built.¹⁷ protection of human dignity, serving as the foundation upon Privacy is a fundamental right, essential to autonomy and the

interference by public (eg state)¹⁸ and private entities. individual autonomy, and thus warrant special protection from implications for complex and disparate areas of our lives and religion, dignity and self-fulfilment. They have relevance in and include inter alia freedom of thought, expression, conscience, These other rights, which often complement each other, may

the technical side of privacy protection as well as the legal impliof both promises made prior to the election and the recent cyber cyber security interventions over the forthcoming years.²³ backdoor access, etc) as opposed to a well thought-out strategy of sporadic tines for social media, restrictions on car hire, WhatsApp of legislation²² driven by cyber and terrorist attacks (proposals of again another knee-jerk reaction in the form of the introduction of encrypted messaging services.²¹ Thus, we are witnessing yet spaces so as to monitor citizens' internet use – above all, their use intelligence agencies an unprecedented overt access to private proposed legal provisions would give British law enforcement and prevention with scant attention to human rights implications. The legislative agenda in the context of national security and crime terrorist attacks²⁰ have propelled privacy issues to the political and levels of security monitoring in the world, yet the recent cyber and cations are not clear.¹⁹ The UK already has one of the highest and terrorist attacks over the summer. Yet the understanding of lative changes on privacy are set into motion under the influence Now that the UK general election is behind us, the wheels of legis

Background: pre-election positions

the 2017 general election. All key parties tocused on security the context of Brexit, security was used as a bargaining chip in a time of constant change and with the ongoing uncertainty in how to achieve it and handle individual rights to privacy. cyber-security in their agenda, they offered different views on online. While all political parties emphasised the importance of assurance by changing the ways individual data is managed than 100 crime and justice related policies between them.²⁴ In Conservatives, Labour and Liberal Democrats, proposed more In their respective manifestos, three political parties, the

The Conservative Party

privacy that the word appeared six times in the manifesto.25 internet activity, the Conservatives seemed so concerned about that allows government to access detailed records of everyone's Despite having introduced the Investigatory Powers Act 2016 individual data privacy and took a bold position on cyber-security The Conservative Party manifesto had the most to say about

> General Data Protection Regulation. with the forthcoming regulatory changes stipulated by the EU detail about how this would be done and whether it would align by a new data protection law'.²⁶ Yet the manifesto provided little the party 'will deliver protections for people's data online, backed The manifesto pledged data safety through new legislation, stating

new challenges for data compliance.28 is unclear, it adds yet another level of uncertainty and potentially comply with the new GDPR that comes into force in May 2018. Because the Conservatives' position on their new data privacy law the welfare of children and younger people – are protected.' logy, while ensuring that our security and personal privacy – and society, we need to harness the power of fast-changing technotion remains opaque: 'For the sake of our economy and our The manifesto emphasises that privacy is important but its regula-Any organisation handling EU consumer data will be forced to

states: more similar to that governing the offline world²⁹. The manifesto The Conservatives have set out plans to make online regulation

the right regulatory frameworks that will protect our security future to our country; but we also need government to create to set up and run modern businesses, bringing the jobs of the need a government to make Britain the best place in the world If we are going to respond to rapid changes in technology, we online younger people in an age when so much of life is conducted and personal privacy, and ensure the welfare of children and

protection. yet make online service providers share responsibility for privacy bring individual privacy to the forefront of the technology debate, The Conservatives promised to develop a digital charter that will

should think carefully before trying to justify this move. terrorist organisations and hostile state actors – the government services are particular targets for hackers, cyber criminals and from cyber-attacks – and that public sector and government Telegram. Given the increasing challenge of keeping data sate messages including popular services such as WhatsApp and personal data, undermining the secure nature of encrypted nications and data.³⁰ This would mean creating a backdoor to required to give the government access to any encrypted commu-There is also an indication that technology companies will be

Conservative Manifesto goes further: turn 18. Erasing millions of profiles across more than 20 social companies to delete information about young people when they around safety for children online, and to require social media Another hallmark promise from the Conservatives revolved platforms with data storage across the world is a tall order. The

secure way. media platforms to delete information held about them at the of their own data, including the ability to require major social We will give people new rights to ensure they are in control an expectation that personal data held should be stored in a age of 18, the ability to access and export personal data, and

for more privacy control: 'We will institute an expert Data Use and other communications companies.³¹ There is also a proposal user preterences could be seen as a big burden for social media do not want their data deleted, or want to keep part of it. Such It is not clear, however, what the legal position would be if users

> to its manifesto. by a party otherwise so keen to make the digital economy central issues,³⁴ equating the internet with gambling is a big step to take some evidence of links between social media and mental health to the approach taken with the gambling industry.33 While there is companies to fund online safety and protection campaigns, similar introduce an industry-wide levy from internet and communication Conservatives went further still by suggesting that they would also the nature of data use and how best to prevent its abuse'.³² The and Ethics Commission to advise regulators and parliament on

the regulation of emergent technologies: To sum up the position, the Conservatives admit falling behind on

ging our laws and regulations to keep pace.35 new norms in the space of years rather than decades; challenchallenges [..]. They accelerate the pace of change - ushering in digital technology pose significant practical and philosophical The opportunities and threats arising from the advance of

The Labour Party

Government would keep the GDPR in its current format. underpin these rules; however, it seems very likely that a Labour ning strong data protection rules to protect personal privacy." ments do not impede cross-border data flows, whilst maintaito growing the digital economy and ensuring that trade agree-Very little substantive details were provided on what laws would The Labour Party Manifesto stated that: 'Labour is committed privacy are bound to come across a rather opaque manifesto. Those keen to find out more about Labour's position towards data

tial ambassador would contribute to data privacy issues. to liaise with technology companies, promoting Britain as an substantive detail on how the position and the role of this poten-'attractive place for investment'.³⁶ However, there was not much The manifesto proposed an appointment of a digital ambassador

align any future policy to it. is well aware of the human rights jurisprudence and intends to an individual freedom'.³⁷ The latter promise indicates that Labour the circumstances demand that our collective security outweighs tive' 'judicial oversight over how and when they are used, when proportionately and only when necessary and 'reintroduce' 'effec at times compromised, it promised to apply investigatory powers Although it admitted that individual rights and civil liberties are Labour's position on cyber-security also lacked definition

peyond'.40 tion agreements with our intelligence partners in Europe and to continue to 'maintain the cross-border security co-operathe 100,000 strong petition to hold it back.³⁹ Labour proposed statute largely without the public discussion and in defiance of five Labour MPs voted against the Bill.³⁸ Thus the Bill became a the Investigatory Powers Bill was virtually non-existent. Only Party opposition to the oversweeping powers introduced by However, in contrast to its stance in the manifesto, the Labour

The Liberal Democrats

records. They also proposed to create a digital 'bill of rights' to the unrestricted collection of communications data and internet with the electorate.41 They promised to end the mass surveillance powers of the Investigatory Powers Act 2016 and opposed whereby their efforts on ensuring societal security did not resonate The Liberal Democrats stood on the other end of the spectrum,

the EU and the acquis therein. on Brexit is an evidence of the Liberal Democrats' commitment to encryption mechanisms.⁴² The pledge to hold another referendum sing to counter the Conservatives' efforts to create back doors to rights would be and how they would be protected while promitheir online data. The manifesto failed to articulate what such protect individuals' privacy and to exercise more control over

What is the way forward?

covert investigations and operations have profound implications 2016 will deliver the desired results.44 and to what extent the provisions of the Investigatory Powers Act as well as future law and policy reform, it is important to assess if society.43 Second, in the interests of legitimacy and accountability for the relationship between citizen and the state in a democratic of the Investigatory Powers Act 2016 are used. This is because observed, it will be important to monitor if and how the provisions the interests of social cohesion and ensuring that the rule of law is interconnected world and one that is yet to be realised. First, in be 'the safest place to be online' is an ambitious claim in such an will even work. The Conservatives' promise that the UK would protected online and whether some of the measures proposed same time, there are serious questions about how our data is proportionate use of cyber-surveillance should look like. At the electorate a few options to consider. An important one is what a privacy and digital surveillance, the main parties have given the With such a variety of what are often vague positions on data

UK public perception on privacy

by companies as well as fake news and propaganda, they were concerned about cyber-crime, cyber-attacks, and misuse of data government surveillance. While the latter age group were more younger generation (18-24) versus older internet users (65+) over Age differences influenced the greater concerns expressed by the services) were of equal concern to both male and female citizens classified information or disrupting the function of websites and the internet to disrupt life in Britain (eg online theft and leaking of state surveillance were more worrying for male than female list. However, when analysed by gender groups, concerns about priate content accessible to children and fake news topped the such as cyber-crime, companies misusing private data, inapprolance clearly was not the biggest concern overall; rather issues Government. The results⁴⁷ revealed that UK Government surveilconcerned about the online surveillance of UK citizens by the UK were asked whether when using the internet they were Adults) shows polarised views on state surveillance.⁴⁶ Respondents YouCov during this time (n = 2017, male 48% female 52% CB ning to the sphere of privacy rights. The survey data collected by and oversight', partly thanks to the recent jurisprudence pertai-Powers Act 2016 'dramatically increase safeguards on privacy said that, the new legislative provisions under the Investigatory retention and analysis by the latest technological tools. Having widest margin of discretion) depends on mass data collection nance of national security (the context in which the state has the position has remained firm, with the conviction that the maintethe opinions of the electorate. Nevertheless, the government's tory changes.⁴⁵ Driven by the new privacy lobby – instigated insti be unusual for the British public to be so acutely aware of regulapublic opinion in the run up to the general election. It is said to surveillance came to the limelight and dominated the media and The government plans for a more widespread, intrusive and cover respondents (see fig 1). On the other hand, cyber-attacks that use gated largely by the Liberal Democrats – the privacy debate stirred

126

Which of the following issues you are concerned about? Gender Differences

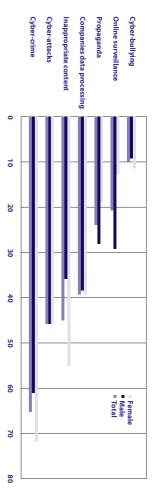
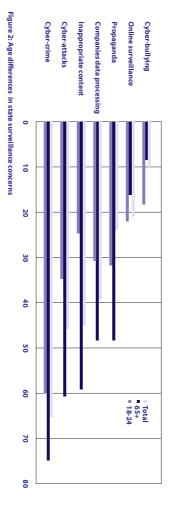


Figure 1: Gender differences in state surveillance concerns

Which of the following issues you are concerned about? Age groups



much less concerned about UK Government surveillance than the younger users (as seen in fig 2).

Dissimilarities in the public's attitude as to whether national security overshadowed privacy concerns were revealed in the survey. When asked whether more should be done to protect the privacy of ordinary people, even if this put some limits on what the UK Government could do to fight crime or protect national security, only 26 per cent of the public agreed. While 30 per cent of younger adults supported the statement, the older generation appeared much less concerned (19%).

A similar divide was evident in the opinions of the older generation in favour of giving more support to 'the UK Covernment to fight crime or protect national security, even if this means the privacy of ordinary people suffers'. This was supported by 50 per cent of older people, versus only 17 per cent of younger individuals favouring security over privacy. Furthermore, the survey gathered views regarding the Investigatory Powers Act 2016 which allows the UK Coovernment agencies to access data such as the content of messages stored on specific computers, mobile devices and networks. This kind of targeted surveillance requires a warrant signed off by an independent judge. When asked about support to this form of targeted surveillance by UK Covernment ragencies, 52 per cent of respondents gave a positive answer. The age group difference was still prominent, with 33 per cent

> of younger individuals compared to 69 per cent of respondents aged 65 + favouring targeted surveillance. Mass data retention was also backed by the UK population as a whole at 38 per cent, which increased to 52 per cent for the 65+ age group compared to 25 per cent for the younger generation. Overall, the perception of the Investigatory Powers Act 2016 was that the Act generally makes us all safer as perceived by 47 per cent, with a predictable rise to 65 per cent of supporters among older respondents. The 2017 data showed general support for the UK Government priority for national security when it came to surveillance versus privacy.⁴⁸

Implications for practice

The respect for privacy and the right to privacy enable us to 'protect ourselves and society against arbitrary and unjustified use of power, by reducing what can be known about us and done to us, while protecting us from others who may wish to exert control'.⁴⁹ With the increased use of online technology, individuals store personal information, express personal opinions, interact with each other and conduct business. Recent theoretical models of personal information privacy emphasise continued loss of control over personal information between parties transacting online³⁰. In online transactions users are losing out to service providers. This transfer of control now includes third

> parties (eg content aggregators, agencies and government) as well as forth parties (eg malicious entities, hostile states and hacktivists) Accordingly, the concept of privacy is no longer confined to 'what happens behind dosed doors' and include personal information in all forms (digital or otherwise).⁵¹ So, given the fundamental importance and value placed on informational autonomy²² and privacy, what should be the limits of public and government interference in this sphere?

The ECHR jurisprudence demostrates that the margin of appreciation conferred to the state authorities in this regard depends on the circumstances of each case. The court's review of interference with privacy would also depend on the actor (public or private) on whom the obligation or duty to respect privacy was placed.⁵³ As is the case for protection of private data under the CDRR⁵⁴ the government is under a duty to act positively to prevent an interference with the Article 8 guarantees by another private individual and/or a company. In the event of an interference being necessary, such interference must be prescribed by law.⁵⁵ and pursue a legitimate aim clearly and precisely.⁵⁷ there must also be appropriate safeguards in place in order to protect citizens form arbitrary interference and abuse.⁵⁷ The exceptions for interference are confined to areas stipulated by Article 8 (2) of the HRA 1998:

There shall be no interference by a public authority with the evercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the inputs and freedoms of others.

In the context of national security, the state may justify its interference with ease as the margin of appreciation widens in this context.³⁶ However, this does not provide a blank sheet to the government. There are still a number of thresholds and safeguards in place with regards to surveillance, search, interception and investigation of criminal activity.³⁶ For example, oversight and authorisation by a court may be required⁶⁷ (as is the case in the UK®) whereby a sunset clause and review of the interference on individual privacy can be monitored and a fair balance can be struck between the security interest of the state and the privacy of individuals. It is also well established that citizens who have been subject of unauthorised surveillance and other forms who have been in their privacy are entitled to an effective legal remedy.⁶²

The exception pertaining to the interest of the economic wellbeing of the country' was considered in Powell and Rayner v UK,⁶⁴ whereby the court acknowledged that a fait balance has to be struck between the competing interests of the individual and of the community as a whole. The court ruled that noise levels emanating from aircraft traffic did not violate Article 8, and could be justified owing the economic interest of the country. As e-commerce and online transactions and business activity are common features of our current economy, it would not be difficult to infer that interference in online privacy can be justified (subject to safeguards) under this heading.

In the context of crime prevention and law enforcement, necessity and proportionality tests would be applied in light of the seriousness and gravity of the crime involved. For instance, in *Murray v UK* (a case involving terrorist offences),st the ECHR ruled *Murray v UK* (a case involving terrorist offences),st the ECHR ruled that the recording of personal details and the taking of a photograph without a person's consent in the context of a house entry and search did not violate Article 8. Later, in *Tele2 Sverige and Watson* cases, the Court of Justice of the EU (CJEU) confirmed that *Watson* cases, the Court of Justice of the EU (CJEU) confirmed that

> access by competent national authorities to retained data must be restricted solely to fighting serious crime, and subject to prior review by a court or an independent administrative authority.⁶⁵

As a brief consideration of the legal principles that apply to respect for privacy or the interference in privacy (as the case may be) demonstrates, there are numerous boundaries within which any legal and regulatory reform can take place.⁶ These boundaries can be considered as positive obligations, and justification benchmarks placed on both state authorities and private entities (persons and organisations).⁶⁷

Brexit effects on privacy

dence and business continuity in the Brexit process. trameworks on digital economy firms, and aims to ensure contiimpact of the withdrawal from the EU's legislative and regulatory individuals. On the other hand, the government recognises the achieve high data protection standards and ensure privacy of UK nisms in the post-Brexit era. The government's ambition is to data protection regulation and the EU information-sharing mecha challenges, the UK is going ahead with forging the future of its a growing volume of jobs; in 2015 it created around two million GVAA or £118.4 billion in 2015. The digital economy provides digital economy contributed just over 7 per cent of the British cannot be underestimated.69 According to the recent statics, the The importance of the digital sector to the British economy the functioning of and prospect for the British digital economy. mental consequences for UK security and ultimately damage tion of the existing data sharing relationships would have detrithe UK Government acknowledges that any significant modifica order to avoid compromise of national security. This means that data sharing between UK and the EU need to be maintained in border law enforcement agencies.68 Existing mechanisms for is a need to continue data sharing processes between crosseffective law enforcement, the UK Government feels that there Driven by the growth concerns for the digital economy and jobs, evidencing a steady increase year on year.⁷⁰ Amidst these

The final emphasis is on the assurance of cross-border cooperation by law enforcement agencies. The Minister of State for Digital, Matt Hancock, summarised these objectives as follows: 'Our goal is to combine strong privacy rules with a relationship that allows flexibility, to give consumers and businesses certainty in their use of data.'⁷¹

In contrast, in 2016 the House of Commons highlighted the UK government's position towards digital economy regulation strategy as follows: 'The government has, in general, taken a hands-off approach to regulation, wanting to stimulate growth of the digital economy'.

In August 2017, the government's position is focused on transforming UK-EU relationship into a 'new, deep and special partnership' for exchanging and protecting personal data which:

continues safely to exchange data in a 'properly regulated way';

- ensures business confidence and provides certainty for individuals;
- continues to cooperate in the regulatory space between the EU and the UK on current and future data protection issues, while avoiding the imposition of additional financial liability on businesses;

emphasises individual privacy protection; and

establishes Britain as a leader in data protection, while maintaining UK sovereignty.

of cyber threats. The consultation follows the government's tructure providers to take steps to address the increasing number the Security of Network and Information Systems Directive (NIS consideration of evidence."22 Indeed, on 8 August 2017 the UK leaves the EU. European Union in relation to the digital environment even after it the UK Government to maintain standards consistent with the will take effect in May 2018,75 and both confirm the intention of Data Protection Regulation (GDPR). Both pieces of legislation Bill that will implement the provisions of the European General announcement of its intention to introduce a new Data Protection NIS Directive⁷⁴ will require certain categories of critical infras-Directive),73 commonly known as the Cybersecurity Directive. The Government launched a consultation on its plans to implement forge its new UK-EU data exchange model 'based on objective application of security mechanisms, the government plans to Echoing the words of the manifesto concerning 'evidence-based

that they have a duty of transparency towards the individuals to the EU. The proposed legislation imposes a number of standards or charity established in the EU that uses information about living In contrast, the GDPR will apply to any business, public authority decided by individual Member States, and are yet to be finalised. to the competent authority. However, the specific details will be implement appropriate security measures, and to notify incidents Economy Report 2016-17, which stated that: This is in direct opposition to the recommendations of the Digital EU partners to develop world-leading data protection standards on modern data protection laws, and has worked closely with data relationship should continue'.¹ The UK is leading the way whom the information relates. According to Mr Hancock, 'our sations must not only keep personal information secure, but upon organisations to which it applies. It specifies that organiservices to citizens in the EU, or monitors citizens' behaviour in apply to any business located outside the EU that offers goods and individuals, whether employees, customers or suppliers. It will also infrastructure sectors. Broadly, it will require these organisations to financial market infrastructures, health sector, water and digital 'operators of essential services' in the energy, transport, banking, The NIS Directive will not apply to all organisations, but only to

ment rights. of the consumer first, although not at the expense of employput the interests—in terms of quality, choice, cost and safetyflexible enough to adjust to disruption. It should, in our view, Regulation should be based on agreed principles, and also

other EU secondary legal instruments pertaining to privacy, digital Rights), thus binding on the UK as a signatory, the PDGR and 1950, is adjudicated at Strasbourg (the European Court of Human rights instrument, the European Convention on Human Rights and if so how it will operate. While the main regional human jurisdiction of the Court of Justice of the EU will apply to the UK, Importantly, in the aftermath of Brexit it is not clear whether the

data and economy, are adjudicated by the CJEU.

fundamental rights of EU citizens – in a state of uncertainty. plethora of areas – including digital economy, privacy, and other CJEU. Subseqently, the UK Government's current stance leaves a fundamental rules governing it, including the jurisdiction of the allow the UK to access the Single Market without accepting the the jurisdiction of its courts. It is very unlikely that the EU would Market then they will have to comply with EU law and accept However, if UK companies want to operate in the EU Single diction of the CJEU would end once the UK leaves the EU.⁷ The Prime Minister, Theresa May, made it clear that the jurisi-

challenges in the time of transformation **Technical controls and compliance**

should be vigilant in these markets'.78 power is not abused, we recommend that existing regulators regime, stating: 'to protect consumers and to ensure that market report 'Online platforms and the digital single market' issued by development of world leading data protection standards. The has shown that working closely with the EU partners facilitates The leading position of the UK on modern data protection 2016 argued against the creation of a platform-specific regulatory The House of Lords Select Committee on the European Union in

government: regime governing privacy in the cyberspace. According to the privacy. In this article we provided evaluation of the current legal objectives to use intelligence prioritising national security over companies as well as providing a difficult obstacle for government the potential misuse of their personal information by commercial generation (18-24 years) who were significantly concerned over These views were reflected in the YouGov survey for the younger superficial influence over how their personal information is used mation lies critically with the latter, leaving individual users with providers.' Thus far the imbalance of control over personal informore collaborative approach to regulation that involves users and in which compliance solutions can be developed, to ensure a Digital Economy⁷⁹ advised that the government explore ways A further proposal from the Parliamentary Committee on the

be unhindered in the future as we leave the EU. business and all relationships. We want the secure flow of data to In the modern world, data flows increasingly underpin trade,

protection rules, is in our mutual interest." data relationship between the UK and EU, based on aligned data and concur with the Minister for Digital that, 'a strong tuture privacy regulation and its societal and technical implications, We offer a critical assessment of the changing position of UK

Professor Vladlena Benson

Coventry Law School, Coventry University Prof Umut Turksen Cyber Security Innovation Centre, University of West London

Notes

- MacAskill E, Privacy campaigners win concessions in UK surveillance report uk-surveillance-report-makes-concessions-to-privacy-lobby The Guardian, 14 July 2015, https://www.theguardian.com/world/2015/jul/14,
- Shaw D, Scotland Yard, UK terror level severe 'for at least five years', BBC New More than 1000 cyber attacks were reported to the National Cyber Security Centre since it opened in 2016. BBC News, 'Cyber-security: More than uk-41478608 1,000 attacks reported in UK', 3 October 2017, http://www.bbc.co.uk/news/
- Stantord B, The Complexities of Contemporary Terrorism Trials Laid Bare, 5 September 2017, http://www.bbc.co.uk/news/uk-41157175

22

- Home Office, Counter-terrorism Communications data, 17 March 2015 https://www.gov.uk/government/collections/communications-data. It has Criminal Law & Justice Weekly, 9 September 2017, vol 181.
- about crime. Coleman and McCahill, Surveillance and Crime, (Sage, 2010). without some form of surveillance it would not be possible to gain information been argued that surveillance and crime have been intimately connected
- This was the case in the context of terror suspects in Spain. Fox News, 'Barcelona terror attack suspect freed by judge, three others ordered held', 2.2 lona-attacks-to-testify-in-court.html. August 2017, http://www.foxnews.com/world/2017/08/22/4-suspects-in-barce
- Nurse J, 'Optional Data Disclosure and the Online Privacy Paradox: A UK Perspective', in Tryfonas T, (eds) Human Aspects of Information Williams and Nurse refer to this as the 'Privacy Paradox'. Williams M and (Springer, 2016). Security, Privacy, and Trust, Lecture Notes in Computer Science, vol 9750,
- News, 23 August 2017, http://www.bbc.co.uk/news/business-41011464. G Kovacs, 'Tracing the trackers', February 2012, www.ted.com/talks/gary. Peachey K and Johnston C, 'Identity theft at epidemic levels, warns Cifas', BBC
- com&utm_content=awesm-publisher. campaign=&utm_medium=on.ted.com-static&utm_source=facebook kovacs_tracking_the_trackers.html?awesm=on.ted.com_Kovacs&utm
- Businesses use such information to target costumers and improve their services and products.

28 27 25 24

26

29

10

- = and gather evidence for prosecution. The overview of the party manifesto naturally gives weight to the two main State agencies use such information to profile, predict and prevent illegal activity
- 12 as a coalition partner from 2010-15). Parties like the SNP provide a distinctly substantial - 8 MPs elected in 2015 and 12 in 2017 (notwithstanding its position parties likely to form a government. However, the consideration of the Lib Derr position shows a polar difference in relation to the rest, whilst its weight is less 35 in 2017, are a committed pro-EU/ECHR party etc. Yet, the SNP manifesto did regional flavour to their politics, but they did have elected 56 MPs in 2015 and 30
- 13 The European Convention on Human Rights was incorporated into the nationa Art 8 which provides that: '1. Everyone has the right to respect for his private tindings legislation of the United Kingdom by the Human Rights Act 1998, Ch 42, Sch 1 not focus on national security nor privacy, and therefore is not included in the

ω 1

ယ္သ 32

- accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of the rights and freedoms of others'. the prevention of disorder or crime, for the protection of health or morals, or for and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in
- Article 16 91, http://eur-lex.europa.eu/legal-content/EN/ TXT/?uri = celex%3A12012E%2FTXT.

4

- The GDPR will come into force on 25 May 2018, http://www.eugdpr.org
- Westin A, Privacy and Freedom, (Bodley Head, 1970) p 23.
- Privacy International, https://www.privacyinternational.org/node/54
- 19 In 2015 the Intelligence and Security Committee asserted that the law failed 686. Fenwick H, Fenwick on Civil Liberties and Human Rights, (Routledge, 2017) p

37 38

Ibid, p 77.

manifesto 2017

35 36

The Labour Party Manifesto 2017, http://www.labour.org.uk/index.php/

- new laws were criticized by civil rights groups, see Liberty 'Undemocratic, Transparent Legal Framework, HC 1075, 12 March 2015. Subsequent proposed Intelligence and Security Committee, 'Privacy and Security: A Modern and legal powers to govern emergent platforms such social networks and media behind technological developments, and thus emphasised the need to for
- Pantucci R, 'Terror by Text', BBC, 4 September 2017, http://www.bbc.co.uk/ condemns Britain's snooping laws', 11 June 2015, https://www.liberty-humanunnecessary and - in the long run - intolerable: Covernment reviewer and--long-run--intolerable. rights.org.uk/news/press eleases-and-statements/"undemocratic-unnecessary
- 21 20 O'Sullivan F, 'Fortress Britain's Coming Crackdown', CityLab, 25 May iplayer/episode/b093pkt6/inside-out-london-terror-by-text

42 43

england.

Liberal Democrats Manifesto 2017, https://www.libdems.org.uk/manifesto

BBC News, Election 2017, http://www.bbc.co.uk/news/election/2017/results/ The election secured only eight parliamentary seats for the Liberal Democrat

Mac Giollabhui S, et al, 'Watching the watchers: conducting ethnographic

research on covert police investigation in the United Kingdom', (2016)

41

manifesto 2017

40 39

The Labour Party Manifesto 2017, http://www.labour.org.uk/index.php/

nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper The Guardian, 19 November 2016, https://www.theguardian.com/world/2016; MacAskill E, "Extreme surveillance" becomes UK law with barely a whimper' Mag UK, 1 December 2016, http://uk.pcmag.com/ip-act/86389/feature/ Newton T,' How did Labour vote on the Investigatory Powers Act', PC

how-did-labour-vote-on-the-investigatory-powers-act.

down/528105/ accessed 25 August 2017. It has been reported that intelligence 2017, https://www.citylab.com/life/2017/05/fortress-britains-coming-crack-44 MacAskill, E. (2016) 'Extreme surveillance' becomes UK law with Qualitative Research, vol 16, no 6, 630-45.

34 It has been reported that there were over 2.01 billion monthly active Facebook users in June 2017 alone. Zephoria, 'The Top 20 Valuable Facebook Statistics', 17 Benson, V, 'UK politicians are planning very different approaches to data privacy security and surveillance', *The Independent*, 6 June 2017. Available at: http:// assessing-general-election-manifestos. The Conservative Party Manifesto 2017, https://www.conservatives.com/ Ibid. Griffiths M,' Does Internet and Computer "Addiction" Exist? Some Case Study Overview-of-measures.pdf. Gambling Commission,' Overview of the measures in the ABB's Social for-organisations/data-protection-reform/overview-of-the-gdpr/. The Conservative Party Manifesto 2017, https://www.conservatives.com/ lbid. bools between 2000 and 2015 following various terrorist attacks within and outside the UK. For a critical analysis of responses to terrorist attacks in the UK. US and Australia see, Turksen U., *Protection Seekers, States and the New* and Families', (2011) Pediatrics vol 127 No 4, 800-04. G S and Clarke-Pearson K, The Impact of Social Media on Children, Addescents Evidence', (2004) Cyber Psychology & Behaviour, vol 3 (2), 211-18, and O'Keefft 2014, http://www.gamblingcommission.gov.uk/PDF/board-papers/GCP1420-Responsibility Code and NCF's "Playing Safe" statement of principles', 12 March manifesto. The Conservative Party Manifesto 2017, https://www.conservatives.com/ September 2017, http://www.bbc.co.uk/news/uk-politics-41327816. content. BBC News, 'Theresa May to warn tech firms over terror content', 20 nies are already under pressure to remove and manage terror and extremist See s 253(5) of the Investigatory Powers Act 2016. Also note that tech compamean-for-online-privacy-a7775211.html. www.independent.co.uk/life-style/gadgets-and-tech/what-will-the-uk-electionmanifesto Information Commmissioner's Office, Overview of the GDPR, https://ico.org.uk Justice Studies, 26 May 2017, https://www.crimeandjustice.org.uk/publications, Garside R, 'Assessing the General Election Manifestos', Centre for Crime and titteen-years-911-how-uk-bypassed-justice-become-counter-terrorism-state 11 September 2016, http://www.newstatesman.com/politics/uk/2016/09/ UK bypassed justice to become a counter-terrorism state', New Statesman, centred governance see, Norris M, 'Fifteen years on from 9/11, how the Note that 12 pieces of separate counter-terrorism legislation hit the statute (2017) Journal of Information Rights, Policy and Practice, vol 2, no 1, pp 1-2. White M, 'Protection by Judicial Oversight, or an Oversight in Protection? June_2014.pdf, p 10, and arguing that the DRD was mainly created in reaction to the terrorist attacks in Madrid on 11 March 2004 and London on 7 July 2005 Court of Justice of the European Union' (30 June 2014), http://www.janalbrecht Franziska Boehm & Mark D Cole, 'Data Retention after the Judgement of the See White, citing the Preamble of the EU's Data Retention Directive (DRD), and security%20_%20World%20news%20_%20Guardian%20Weekly.pdf and%20UK%20spy%20agencies%20defeat%20internet%20privacy%20and%20 9 June 2013, https://www.ihatefeds.com/Revealed_%20how%20US%20 US and UK spy agencies defeat internet privacy and security', The Guardian, and investing in tech companies to 'covertly influence' their product design to ensure they are easier to access and exploit. Ball J et al, 'Revealed: how September 2017, https://zephoria.com/top-15-valuable-tacebook-statistics/ manifesto. Security Agenda, (Altin Nokta Publishing, 2010). For the evolution of security eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_services have been employing methods to counter encryption technologies

130

- 48 47 VGC (2017), 'Broad support for increased surveillance powers', YouGov plc. Available at: http://d25d2506slb94s.cloudfront.net/cumulus_uploads/documen 46 45 While it is beyond the scope of this article, it is worth considering that terro-YouGov, (2017) Broad support for increased surveillance powers, http:// Bakir V et al, 'Public Feeling on Privacy', Security and Surveillance, 2015. guoztocn1q/YGC,%20GB%20Surveillance%202017.pdf. https://sites.cardifi.ac.uk/dcssproject/files/2015/11/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf; Thomson et al, 'A socio lance, study finds', BBC News, 18 June 2015, http://www.bbc.co.uk/news/ ecological approach to national differences in online privacy concern: The role Available at: https://www.theguardian.com/world/2016/nov/19/ YGC,%20GB%20Surveillance%202017.pdf. d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/guozfocn1q/ uk-wales-politics-33184722. 51, Part A, pp 285-92; and Davies D, 'Public "acutely aware" of state surveil of relational mobility and trust', (2015) Computers in Human Behaviour, vol extreme-surveillance-becomes-uk-law-with-barely-a-whimper#_blank barely a whimper. The Guardian Surveillance. November 2016.
- on-the-transformation-of-law-enforcement/; Walker C, 'Journalist, Terrorist rism and other serious crimes can have an impact not only on the people's perception and acceptance of new laws but also how the law is enforced. See Lynch A, 'The Impact of Post-Enactment Review on Anti-Terrorism Laws: Four IMODEV, vol 2, http://ojs.imodev.org/index.php/RICO/article/view/19/94; and or Counter-Terrorist? The Perils of Invesitgative Journalism Post 9/11', (2015) secgovcentre.org/2015/07/the-thin-blue-line-and-the-impact-of-terrorismof Law Enforcement', Centre for Security Governance, 31 July 2015, http:// Findlay V, 'The Thin Blue Line and the Impct of Terrorism on the Transformation Jurisdictions Compared', (2012) The Journal of Legislative Studies, vol 18, issue 1
- 50 Benson, V., Saridakis, G., Tenakoon, H. (2015) «Information disclosure of social pp 63-81. Supra, Privacy International.
- pp.426-441, https://doi.org/10.1108/ITP-10-2014-0232. For a detailed analysis of privacy, human rights and security in the digital age media users: Does control over personal information, user awareness and security notices matter?», Information Technology & People, Vol. 28 Isue: 3,
- 5 Journal of Human Rights Practice, Vol. 9, Issue 1, pp. 104-118. Fenwick explains informational autonomy (a.k.a informational self-determinasee, Nyst C and Falchetta T, The Right to Privacy in the Digital Age, (2017)
- 52 about herself, Supra Fenwick H, p 687. tion) as the individual's interest in controlling the flow of personal information
- on Civil Liberties and Human Rights, (Routledge, 2017) pp 66-75.
 54 http://euri-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&h 53 For a comprehensive analysis of relevant jurisprudence see, Fenwick H, Fenwick
- ទ In Harman and Hewitt v UK (1992) 14 EHRR 657, the court held that the activi ties of MI5 in placing the applicants under surveillance were not in accordance Om = EIN.
- with the law.
- Camenzind v Switzerland (1999) 28 EHRR 458. Malone v United Kingdom (1984) 7 EHRR 14, [67].
- 57 57 59 Leander v Sweden (1987)9 EHRR 433.
- Bykov v Russian Federation, App no 4378/02, IHRL 3609 (ECHR 2009); Klass v Federal Republic of Cermany (1978) 2 EHRR 214; and Ludi v Switzerland (1993)

60 61 Funke v France (1993) 16 EHRR 297.

15 EHRR 173.

- 62 Liberty v GCHQ [2014] UKIPTrib 13_77-H. See also the Regulation of tigatory Powers Act 2000.
- 63 Powell and Rayner v UK (1990) 12 EHRR 458. See also MS v Sweden (1999) 28 Human Rights, (Routledge, 2017) ch 11. Fenwick D, 'State Surveillance' in Fenwick H, Fenwick on Civil Liberties and
- Murray v UK (1994) 19 EHRR 193. EHRR 313.
- 65 Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Joined Cases C-203/15 and C-698/15
- 66 For summary of how jurisprudence pertaining to privacy has informed Surveillance Reform for Digital Age,' October 2011, State Watch, http://www 21 December 2016 and moulded legal developments see, 'Justice, Freedom from Suspicion -
- 67 statewatch.org/news/2011/nov/uk-ripa-justice-freedom-from-suspicion.pdf. X and Y v Netherlands (1985) 8 EHRR 71, at [24] stating that protection Art 8 private persons rights may require the state to put in place measures to govern relations between
- 68 Partnership paper', http://www.statewatch.org/news/2017/sep/uk-post-brexit-security-justice-cooperation-paper-9-17.pdf. HM Government, 'Security, law enforcement and criminal justice, A Future
- 69 House of Commons, Business, Innovation and Skills Committee, 'The Digital Economy', Second Report of Session 2016-17, https://publications.parliament
- 70 Department for Digital, Culture Media and Sport, Official Statistics – 'Digital Sector Economic Estimates 2016 - Key Findings', 26 Janaury 2016, https://www uk/pa/cm201617/cmselect/cmbis/87/87.pdf.
- https://www.gov.uk/government/news/ gov.uk/government/publications/digital-sector-economic-estimates-january-2016/ digital-sector-economic-estimates-2016-key-findings.
- The Labour Party Manifesto 2017. Available at www.labour.org.uk/manifesto uk-outlines-proposals-for-shared-approach-on-data-protection.
- 72 Directive', 8 August 2017, https://www.gov.uk/government/consultations/ Department for Digital, Culture, Media and Sport and Matt Hancock MP, 'Consultation on the Security of Network and Information Systems
- 74 network and information systems, https://ec.europa.eu/digital-single-market/en/ network-and-information-security-nis-directive. For the NIS Directive see, http:// European Commission, Digital Single Market, The Directive on the security of consultation-on-the-securit -of-network-and-information-systems-directive
- 75 https://www eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535. w.gov.uk/government/collections/data-protection-bill-2017 .
- Stone, J, 'British data protection laws to stay "aligned" with the EU's after Brexit' politics/data-protection-rules-brexit-matt-hancock-eu-laws-rules-a7909156.html. The Independent, 23 August 2017, http://www.independent.co.uk/news/uk/
- 78 23 August 2017, http://www.bbc.co.uk/news/world-europe-40630322. Also see, Morris, C, 'Reality Check: What is the European Court of Justice?' BBC News, http://www.bbc.co.uk/news/uk-politics-41012265.
- The House of Lords Select Committee on the European Union, 'Online platforms and the digital single market', April 2016, https://publications.parlia-
- uk/pa/cm201617/cmselect/cmbis/87/87.pdf. Economy, Second Report of Session 2016-17', https://publications.parliament. The House of Commons Business, Innovation and Skills Committee, The Digital ment.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf.

79

Case Notes & Comments

European Union, 14 June BV, Court of Justice of the Ziggo BV and XS4All Internet the public': Stichting Brein v **Right of 'communication to**

Introduction

2017

establishing the conditions under which an internet operator has the concept of the right of 'communication to the public' within (CJEU) handed down its long-awaited judgment in Stichting Brein On 14 June 2017, the Court of Justice of the European Union Netherlands). trom the Hoge Raad der Nederlanden (Supreme Court of the the request for a preliminary ruling under Article 267 TFEU responsibilities for copyright infringement. This judgment follows Article 3(1) of Directive 2001/29/EC (the InfoSoc Directive), and v Ziggo BV and XS4All Internet BV (C-610/15),1 clarifying further

the public' within the meaning of Article 3(1). through a peer-to-peer network, constitute a 'communication to sharing platform such as The Pirate Bay (TPB) in making available Szpunar² states that the actions of the operators of an online files allowing internet users to locate and download these works and managing access to protected works, and by indexing torrent The ruling, which follows the opinion of Advocate General

intringe." these operators whose platforms were used by third parties to dered for the first time at European level by the CJEU.¹⁰ Previously concerned an original communication made on a peer-to-peer communication of works through hyperlink, Stichting Brein v Zigge International.9 While these cases considered the secondary public' under the InfoSoc Directive has been considered in recent (Ireland),⁵ and SAGE.⁶ In the internet era, 'communication to the been addressed in Verwertungsgesellschaft Rundfunk GmbH, 4 PPI to copyright.³ Under Directive 2006/115/EC, this concept has EC on rental right and lending right and on certain rights related not only in the InfoSoc Directive but also in Directive 2006/115/ evolving topic subject to a series of decisions. The term is present all relevant CJEU decisions focused on related injunctions against liability of internet providers for copyright infringement is consinetwork. In addition, the present case is significant because the cases such as Svensson and Others,7 GS Media,8 and BestWater For the past decade 'communication to the public' has been an

Background to the judgment

3(1) of the InfoSoc Directive as follows: The right of 'communication to the public' is provided by Article

time individually chosen by them. members of the public may access them from a place and at a available to the public of their works in such a way that their works, by wire or wireless means, including the making to authorise or prohibit any communication to the public of Member States shall provide authors with the exclusive right

pretation to the discretion of the court.¹² the public' or 'making it available to the public', leaving the inter-1996, but it does not define what amounts to 'communication to Article 3(1) originated from Article 8 of the WIPO Copyright Treaty

distributed without the consent of the right holders.¹³ tree of charge, and 90 to 95 per cent of them are protected works access to musical and cinematographic works. The files shared are of the biggest and best-known file-sharing sites, which provides two main internet access providers in the Netherlands. TPB is one the interests of copyright holders, while Ziggo and XS4ALL are the Stichting Brein is a Dutch anti-piracy foundation, which safeguards

effective protection of copyrights.¹⁵ originators of the copyright infringements. Second, the blocking detendants in the main proceedings (and not TPB) who were the on two grounds.¹⁴ First, it was the recipients of the services of the Gravenhage (the Court of Appeal in The Hague) in January 2014 the court of first instance, was overturned by the Gerechtshof"sand XS4ALL block access to TPB. That application, granted by Gravenhage (District Court of The Hague) for an order that Ziggo In January 2012, Stichting Brein applied to Rechtbank's sought was not proportionate to the aim pursued, namely the

communication to the public within the meaning of Article 3(1) of Directive 2001/29. Therefore, in January 2015, the Supreme Court referred the two following questions to the CJEU: infringed copyrights, but was undecided whether TPB made a right holders' consent and that subscribers of Ziggo and XS4ALL (Supreme Court of the Netherlands), which established that IPB made protected works available to the public without the The decision was appealed to the Hoge Raad der Nederlanden

- Is there a communication to the public within the meaning of and categorised for users, so that the users can trace and works which are present on the users' computers are indexed a system exists ... by means of which metadata on protected (TPB), if no protected works are available on that website, but upload and download the protected works? Article 3(1) of Directive 2001/29 by the operator of a website
- N If Q1 is answered in the negative, do Article 8(3) of Directive 2001/29 and Article 11 of Directive 2004/48 offer any scope