Privacy, Security and Politics: Current Issues and Future Prospects

Benson, V & Turksen, U

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
https://www.bloomsburyprofessional.com/uk/journal/communications-law-17467616/

ISSN 1746-7616

Publisher: Bloomsbury Professional

83 See s 3.3.6.
84 See *IMPRESS: The Independent Monitor for the Press CIC Regulatory Scheme*, version 3, para 2.2. Supplied in documentation to Press Recognition Panel in respect of the application for recognition from IMPRESS: The Independent Monitor for the Press CIC http://pressrecognitionpanel.org.uk/wp-content/uploads/ 2016/07/ IMPRESS-Regulatory-Scheme.pdf, accessed 20 October 2017.
85 Jonathan Heawood and Brigit Morris, 'Press codes and the spirit of equalities legislation: implementing Leveson' (2016) 21 CL 29, 29.
86 Luxembourg Press Council's Code of Ethics, art 1(c) 'prohibition…of racial, ethnic, religious and ideological discrimination.'
87 See Bulgaria Media Code 2004, para 2.5.2; Guidelines of the Netherlands Press Council, 'Publications only state the ethnic origins, nationality, race, religion and sexual inclination of groups and individuals if this is deemed necessary for a proper understanding of the facts and circumstances that are reported on.'
88 See Journalists' Association of Serbia's Code of Ethics, art IV.1 'In reporting crimes, national, racial, religious, ideological and political 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 criminal offense.'
89 See for example, National Association of Hungarian Journalists' Ethics Code, s 2.1. 'They must not violate human rights, incite hate and the infringement of lawful rights against peoples, nations, nationalities, denominations and races.'
90 See, for example, Armenian Code of Conduct for Media Representatives, principle 5.3. 'Not to advocate war, violence or pornography in any form.'
91 Editors' Code, cl 12; Standards Code, cl 4.
92 Crime and Disorder Act 1998, s 28(4), and see *R v Rogers* [2007] 2 AC 62 for its application.
93 See 11533-16, Miller v Mail Online, para 15 https://www.ipso.co.uk/rulings-and-resolution-statements/ ruling/?id=11533-16, accessed 2 November 2017.
94 It reads: 'Publishers must not make prejudicial or pejorative reference to a person on the basis of that person's age, disability, mental health, gender reassignment or identity, marital or civil partnership status, pregnancy, race, religion, sex or sexual orientation…'
95 Where it refers both to disability and mental health.
96 See n 23 (Pt L) recommendation 38.
97 See Alex Dyke (BBC Radio Solent) Ofcom Broadcast Bulletin, Issue 292, 9 November 2015.
98 Equalities and Human Rights Commission response to IMPRESS draft Standards Consultation, 29 September 2016, point 9 http://www.impress.press/downloads/file/code/equalities-and-human-rights-commission.pdf accessed 27 October 2017.
99 Clause 4.1.
100 See the over-emphasis of nationality in some recent road tragedies in *Daily Mail*, Rachel Burford,' Our lives changed in the blink of an eye': Heartache for the family of a mother and three children killed by a Polish lorry driver, 30, as horrifying footage shows the moment he crashed into them after scrolling on his phone at 50mph, http://www.dailymail.co.uk/news/article-3889596/Polish-lorry-driver-30-killed-mother-three-children-scrolling-mobile-phone-change-music-jailed-ten-years.html#ixzz4yb19Ipee, accessed 4 November 2017.
101 See 02741-15 *Greer v The Sun* https://www.ipso.co.uk/rulings-and-resolution-statements/ruling/?id=02741-15, accessed 4 November 2017.
102 Ibid, para 9.
103 Ibid.
104 'About Standards Investigations,' IPSO website, undated https://www.ipso.co.uk/press-standards/about-standards-investigations/ accessed 5 November 2017.
105 See n 10, para 5.
106 Ibid, para 11.
107 See n 14, Editors Codebook, 74.
108 Public Order Act 1986, s 18.
109 Ibid, ss 29A and 29B.
110 Ibid, ss 29AB and 29B.
111 Hacked Off, n 6 in response to consultation on original draft of the Standards Code.
112 Editors' Code, cl 2; Standards Code, cl 7.1.
113 Standards Code, cl 7.2(b).
114 Editors' Code, cl 3; Standards Code, cl 5.2(c).
115 Editors' Code, cl 10(i); Standards Code, cl 7.2(a).
116 Editors' Code, cl 10(ii); Standards Code, cl 5.2(a).
117 See Editors' Code, public interest proviso, point 5 (in regards to 'over-ride the normally paramount interests of children under 16); Standards code, cl 3.1. (photograph or interview child under 16 without consent) 3.2 (identify child under 16 without his consent).
118 Editors' Code, cl 5.
119 Ibid, cl 7.
120 Ibid, cl 8.
121 Ibid, cl 9.
122 Ibid, cl 15(ii).
123 Ibid, cl 16.
124 Standards Code, cl 8.3.
125 See n 14 Editors' Codebook, 96; Standards Code, public interest proviso; Guidance, para 0.11-0.13.
126 Editors' Codebook, 96-98;
127 Ibid, 98; Guidance, para 0.25 - 0.29.
128 See 'History of the Code', Editors Code of Practice Committee http://www.editorscode.org.uk/history _of_the_code.php accessed 24 October 2017.
129 Evan Harris, 'Newspaper industry releases revised "Editors' Code", more comfort for tabloids, 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.
130 Inserting s 43B into the Employment Rights Act 1996.
131 Editors' Code, public interest proviso, point 2.
132 See n 23 (Pt K, para 4.24). See also discussion in M Keppel-Palmer, 'The emperor's new clothes: IPSO's version of the editors' code of practice' (2016) 27 *Entertainment Law Review* 92-97, 97.
133 Ibid.
134 Standards Code, public interest proviso.
135 Guidance, paras 0.18 to 0.20.
136 Standards Code, public interest proviso, point (i).
137 'IMPRESS Publishes Draft Standards Code,' IMPRESS website, 18 August 2016, https://impress.press /news /draft-standards-code.html, accessed 24 October 2017.
138 Standards Code, cl 7.2(b).
139 Ibid, cl 3.3.
140 Ibid, cl 2.1.
141 *Guidance for Journalists: Using Material from Social Media* (IPSO, 2017) https://www.ipso.co.uk/press-standards/guidance-for-journalists-and-editors/social-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/topics/user-generated-content/, accessed 24 October 2017.
145 'New technologies, new techniques' ch 6 in David Gordon et al (eds), *Controversies in Media Ethics* (3rd edn, Routledge, 2011) 218-19.
146 See Croatia Journalists' Association Code of Honor, principle 25.
147 Ibid; Council of Mass Media Finland, *Annex to guidelines: Material generated by the public on a news website*; Online News Association, Greece.
148 See n 144.
149 Clause 2.1.
150 Guidance, para 2.12.
151 Standards Code, 2.2.
152 See n 128.
153 See Norwegian Press Association Ethical Code of Practice for the Press, cl 4.16.
154 See Reg (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Dir 95/46/EC (General Data Protection Regulation), reg 17; *Google Spain SL, Google Inc v Agencia Española de Protección de Datos*, C-131/12.
155 Standards Code, cl 3.3.
156 See n 145, 233.

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 Conservative 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 YouGov 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 post-election 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[2] 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 cyber-security 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.

Surveillance and communications data are seen as vital elements in criminal investigations, public protection and ensuring national security.[5] Thus, the failure to collect and retain such data or surveillance evidence can lead to a collapse of the prosecution of suspects.[6] While citizens increasingly use online services and readily impart their personal/private information and data to both government (eg the NHS, HMRC) and non-government institutions (eg banks, travel agencies) as a matter of necessity, they want their privacy to be protected because they are also making themselves vulnerable to criminal activity.[7] For example, identity theft has been reported to be at epidemic levels in 2017.[8] Online and digital presence increase with the activities people pursue. The consequent digital foot-print, assets and behaviour left behind in the 'digital woods'[9] as a 'virtual treasure trove' not only have an economic and a sentimental value for us but also value for businesses, commercial advantage[10] and state functions.[11] It is in this context of both private and public security settings where the debate on privacy laws in the UK is evolving. Yet the questions around government surveillance, powers to bypass security mechanisms of individual online and communication profiles, proposed control and financial penalties for digital economy giants, including social media firms, remain to be answered by forthcoming proposed legislative changes.

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 election[12]. In doing so it identifies main concerns and areas of uncertainty.

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);[13] the Data Protection Act 1998; the Regulation of Investigatory Powers Act 2000; the

Investigatory Powers Act 2016; the Treaty on the Functioning of the European Union 2007;[14] and the EU General Data Protection Regulation (GDPR) 2016.[15] While these instruments are meant to give us the ability to invoke our rights against undue interference and significant power imbalances in the context of privacy, they do not provide a definition of privacy. While privacy is traditionally defined as 'the ability for people to determine for themselves when, how, and to what extent information about them is communicated to others',[16] for the purposes of this article, it is worth paying attention to the definition provided by Privacy International:

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

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

Now that the UK general election is behind us, the wheels of legislative changes on privacy are set into motion under the influence of both promises made prior to the election and the recent cyber and terrorist attacks over the summer. Yet the understanding of the technical side of privacy protection as well as the legal implications are not clear.[19] The UK already has one of the highest levels of security monitoring in the world, yet the recent cyber and terrorist attacks[20] have propelled privacy issues to the political and legislative agenda in the context of national security and crime prevention with scant attention to human rights implications. The proposed legal provisions would give British law enforcement and intelligence agencies an unprecedented overt access to private spaces so as to monitor citizens' internet use – above all, their use of encrypted messaging services.[21] Thus, we are witnessing yet again another knee-jerk reaction in the form of the introduction of legislation[22] driven by cyber and terrorist attacks (proposals of sporadic fines for social media, restrictions on car hire, WhatsApp backdoor access, etc) as opposed to a well thought-out strategy of cyber security interventions over the forthcoming years.[23]

Background: pre-election positions

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

The Conservative Party

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

The manifesto pledged data safety through new legislation, stating the party 'will deliver protections for people's data online, backed by a new data protection law'.[26] Yet the manifesto provided little detail about how this would be done and whether it would align with the forthcoming regulatory changes stipulated by the EU General Data Protection Regulation. [27]

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

The Conservatives have set out plans to make online regulation more similar to that governing the offline world[29]. The manifesto states:

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

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

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

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

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

It is not clear, however, what the legal position would be if users do not want their data deleted, or want to keep part of it. Such user preferences could be seen as a big burden for social media and other communications companies.[31] There is also a proposal for more privacy control: 'We will institute an expert Data Use and Ethics Commission to advise regulators and parliament on the nature of data use and how best to prevent its abuse'.[32] The Conservatives went further still by suggesting that they would also introduce an industry-wide levy from internet and communication companies to fund online safety and protection campaigns, similar to the approach taken with the gambling industry.[33] While there is some evidence of links between social media and mental health issues,[34] equating the internet with gambling is a big step to take by a party otherwise so keen to make the digital economy central to its manifesto.

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

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

The Labour Party

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

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

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

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

The Liberal Democrats

The Liberal Democrats stood on the other end of the spectrum, whereby their efforts on ensuring societal security did not resonate with the electorate.[41] They promised to end the mass surveillance powers of the Investigatory Powers Act 2016 and opposed the unrestricted collection of communications data and internet records. They also proposed to create a digital 'bill of rights' to protect individuals' privacy and to exercise more control over their online data. The manifesto failed to articulate what such rights would be and how they would be protected while promising to counter the Conservatives' efforts to create back doors to encryption mechanisms.[42] The pledge to hold another referendum on Brexit is an evidence of the Liberal Democrats' commitment to the EU and the *acquis* therein.

What is the way forward?

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

UK public perception on privacy

The government plans for a more widespread, intrusive and covert surveillance came to the limelight and dominated the media and public opinion in the run up to the general election. It is said to be unusual for the British public to be so acutely aware of regulatory changes.[45] Driven by the new privacy lobby – instigated instigated largely by the Liberal Democrats – the privacy debate stirred the opinions of the electorate. Nevertheless, the government's position has remained firm, with the conviction that the maintenance of national security (the context in which the state has the widest margin of discretion) depends on mass data collection, retention and analysis by the latest technological tools. Having said that, the new legislative provisions under the Investigatory Powers Act 2016 'dramatically increase safeguards on privacy and oversight', partly thanks to the recent jurisprudence pertaining to the sphere of privacy rights. The survey data collected by YouGov during this time (n = 2017, male 48% female 52% GB Adults) shows polarised views on state surveillance.[46] Respondents were asked whether when using the internet they were concerned about the online surveillance of UK citizens by the UK Government. The results[47] revealed that UK Government surveillance clearly was not the biggest concern overall; rather issues such as cyber-crime, companies misusing private data, inappropriate content accessible to children and fake news topped the list. However, when analysed by gender groups, concerns about state surveillance were more worrying for male than female respondents (see fig 1). On the other hand, cyber-attacks that use the internet to disrupt life in Britain (eg online theft and leaking of classified information or disrupting the function of websites and services) were of equal concern to both male and female citizens. Age differences influenced the greater concerns expressed by the younger generation (18-24) versus older internet users (65+) over government surveillance. While the latter age group were more concerned about cyber-crime, cyber-attacks, and misuse of data by companies as well as fake news and propaganda, they were

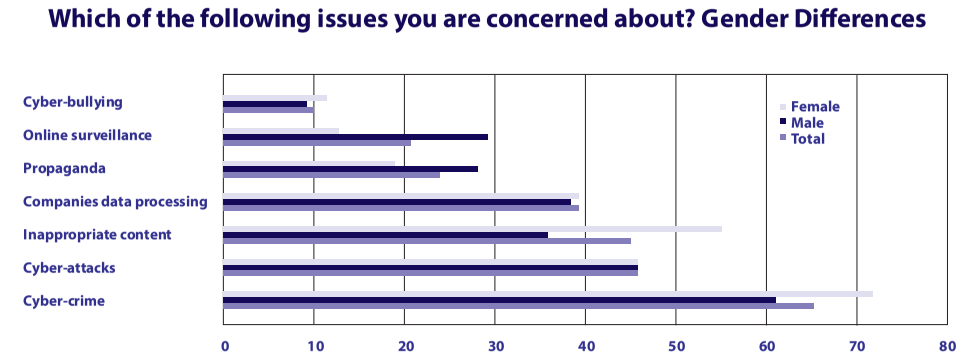

Figure 1: Gender differences in state surveillance concerns

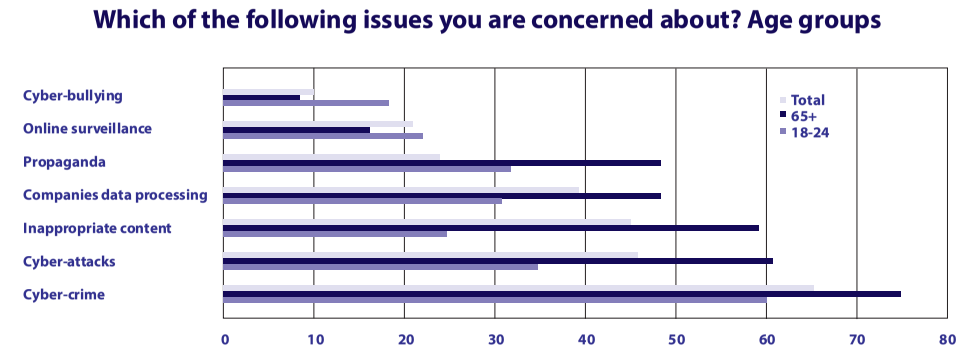

Figure 2: Age differences in state surveillance concerns

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 Government 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 Government 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 Government agencies, 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 online[50]. 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 closed doors' and include personal information in all forms (digital or otherwise).[51] So, given the fundamental importance and value placed on informational autonomy[52] and privacy, what should be the limits of public and government interference in this sphere?

The ECHR jurisprudence demonstrates 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 GDPR,[54] 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;[56] 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 exercise 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 rights 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.[58] 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.[59] For example, oversight and authorisation by a court may be required[60] (as is the case in the UK[61]) 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 interests 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 of interference in their privacy are entitled to an effective legal remedy.[62]

The exception pertaining to the interest of 'the economic well-being of the country' was considered in *Powell and Rayner v UK*,[63] whereby the court acknowledged that a fair 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),[64] 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 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.[66] 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

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

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.

Echoing the words of the manifesto concerning 'evidence-based' application of security mechanisms, the government plans to forge its new UK-EU data exchange model 'based on objective consideration of evidence.'[72] Indeed, on 8 August 2017 the UK Government launched a consultation on its plans to implement the Security of Network and Information Systems Directive (NIS Directive),[73] commonly known as the Cybersecurity Directive. The NIS Directive[74] will require certain categories of critical infrastructure providers to take steps to address the increasing number of cyber threats. The consultation follows the government's announcement of its intention to introduce a new Data Protection Bill that will implement the provisions of the European General Data Protection Regulation (GDPR). Both pieces of legislation will take effect in May 2018,[75] and both confirm the intention of the UK Government to maintain standards consistent with the European Union in relation to the digital environment even after it leaves the EU.

The NIS Directive will not apply to all organisations, but only to 'operators of essential services' in the energy, transport, banking, financial market infrastructures, health sector, water and digital infrastructure sectors. Broadly, it will require these organisations to implement appropriate security measures, and to notify incidents to the competent authority. However, the specific details will be decided by individual Member States, and are yet to be finalised. In contrast, the GDPR will apply to any business, public authority or charity established in the EU that uses information about living individuals, whether employees, customers or suppliers. It will also apply to any business located outside the EU that offers goods and services to citizens in the EU, or monitors citizens' behaviour in the EU. The proposed legislation imposes a number of standards upon organisations to which it applies. It specifies that organisations must not only keep personal information secure, but that they have a duty of transparency towards the individuals to whom the information relates. According to Mr Hancock, 'our data relationship should continue'.[76] The UK is leading the way on modern data protection laws, and has worked closely with EU partners to develop world-leading data protection standards. This is in direct opposition to the recommendations of the Digital Economy Report 2016-17, which stated that:

> *Regulation should be based on agreed principles, and also flexible enough to adjust to disruption. It should, in our view, put the interests—in terms of quality, choice, cost and safety—of the consumer first, although not at the expense of employment rights.*

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

The Prime Minister, Theresa May, made it clear that the jurisdiction of the CJEU would end once the UK leaves the EU.[77] However, if UK companies want to operate in the EU Single Market then they will have to comply with EU law and accept the jurisdiction of its courts. It is very unlikely that the EU would allow the UK to access the Single Market without accepting the fundamental rules governing it, including the jurisdiction of the CJEU. Subseqently, the UK Government's current stance leaves a plethora of areas – including digital economy, privacy, and other fundamental rights of EU citizens – in a state of uncertainty.

Technical controls and compliance challenges in the time of transformation

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

A further proposal from the Parliamentary Committee on the Digital Economy[79] advised that 'the government explore ways in which compliance solutions can be developed, to ensure a more collaborative approach to regulation that involves users and providers.' Thus far the imbalance of control over personal information lies critically with the latter, leaving individual users with superficial influence over how their personal information is used. These views were reflected in the YouGov survey for the younger generation (18-24 years) who were significantly concerned over the potential misuse of their personal information by commercial companies as well as providing a difficult obstacle for government objectives to use intelligence prioritising national security over privacy. In this article we provided evaluation of the current legal regime governing privacy in the cyberspace. According to the government:

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

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

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

Privacy, security and politics: current issues and future prospects

Notes

1 MacAskill E, Privacy campaigners win concessions in UK surveillance report, *The Guardian*, 14 July 2015, https://www.theguardian.com/world/2015/jul/14/uk-surveillance-report-makes-concessions-to-privacy-lobby.
2 More than 1000 cyber attacks were reported to the National Cyber Security Centre since it opened in 2016. BBC News, 'Cyber-security: More than 1,000 attacks reported in UK', 3 October 2017, http://www.bbc.co.uk/news/uk-41478608.
3 Shaw D, Scotland Yard, UK terror level severe 'for at least five years', BBC News, 5 September 2017, http://www.bbc.co.uk/news/uk-41157175.
4 Stanford B, The Complexities of Contemporary Terrorism Trials Laid Bare, *Criminal Law & Justice Weekly*, 9 September 2017, vol 181.
5 Home Office, Counter-terrorism – Communications data, 17 March 2015, https://www.gov.uk/government/collections/communications-data. It has been argued that surveillance and crime have been intimately connected without some form of surveillance it would not be possible to gain information about crime. Coleman and McCahill, *Surveillance and Crime*, (Sage, 2010).
6 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', 22 August 2017, http://www.foxnews.com/world/2017/08/22/4-suspects-in-barcelona-attacks-to-testify-in-court.html.
7 Williams and Nurse refer to this as the 'Privacy Paradox'. Williams M and Nurse J, 'Optional Data Disclosure and the Online Privacy Paradox: A UK Perspective', in Tryfonas T, (eds) *Human Aspects of Information Security, Privacy, and Trust, Lecture Notes in Computer Science*, vol 9750, (Springer,2016).
8 Peachey K and Johnston C, 'Identity theft at epidemic levels, warns Cifas', BBC News, 23 August 2017, http://www.bbc.co.uk/news/business-41011464.
9 G Kovacs, 'Tracing the trackers', February 2012, www.ted.com/talks/gary_kovacs_tracking_the_trackers.html?awesm=on.ted.com_Kovacs&utm_campaign=&utm_medium=on.ted.com-static&utm_source=facebook.com&utm_content=awesm-publisher.
10 Businesses use such information to target costumers and improve their services and products.
11 State agencies use such information to profile, predict and prevent illegal activity and gather evidence for prosecution.
12 The overview of the party manifesto naturally gives weight to the two main parties likely to form a government. However, the consideration of the Lib Dem position shows a polar difference in relation to the rest, whilst its weight is less substantial – 8 MPs elected in 2015 and 12 in 2017 (notwithstanding its position as a coalition partner from 2010-15). Parties like the SNP provide a distinctly regional flavour to their politics, but they did have elected 56 MPs in 2015 and 35 in 2017, are a committed pro-EU/ECHR party etc. Yet, the SNP manifesto did not focus on national security nor privacy, and therefore is not included in the findings.
13 The European Convention on Human Rights was incorporated into the national legislation of the United Kingdom by the Human Rights Act 1998, Ch 42, Sch 1, Art 8 which provides that: '1. Everyone has the right to respect for his private 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 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 rights and freedoms of others'.
14 Article 16 91, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.
15 The GDPR will come into force on 25 May 2018, http://www.eugdpr.org .
16 Westin A, *Privacy and Freedom*, (Bodley Head, 1970) p 23.
17 Privacy International, https://www.privacyinternational.org/node/54
18 Fenwick H, *Fenwick on Civil Liberties and Human Rights*, (Routledge, 2017) p 686.
19 In 2015 the Intelligence and Security Committee asserted that the law failed behind technological developments, and thus emphasised the need to for legal powers to govern emergent platforms such social networks and media. Intelligence and Security Committee, 'Privacy and Security: A Modern and Transparent Legal Framework, HC 1075, 12 March 2015. Subsequent proposed new laws were criticized by civil rights groups, see Liberty 'Undemocratic, unnecessary and – in the long run – intolerable: Government reviewer condemns Britain's snooping laws', 11 June 2015, https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/"undemocratic-unnecessary-and-—long-run—-intolerable.
20 Pantucci R, 'Terror by Text', BBC, 4 September 2017, http://www.bbc.co.uk/iplayer/episode/b093pkt6/inside-out-london-terror-by-text
21 O'Sullivan F, 'Fortress Britain's Coming Crackdown', CityLab, 25 May 2017, https://www.citylab.com/life/2017/05/fortress-britains-coming-crackdown/528105/ accessed 25 August 2017. It has been reported that intelligence services have been employing methods to counter encryption technologies 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 US and UK spy agencies defeat internet privacy and security', *The Guardian*, 9 June 2013, https://www.ihatefeds.com/Revealed_%20how%20US%20and%20UK%20spy%20agencies%20defeat%20internet%20privacy%20and%20security%20_%20World%20news%20_%20Guardian%20Weekly.pdf.
22 See White, citing the Preamble of the EU's Data Retention Directive (DRD), and Franziska Boehm & Mark D Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union' (30 June 2014), http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_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. White M, 'Protection by Judicial Oversight, or an Oversight in Protection?' (2017) *Journal of Information Rights, Policy and Practice*, vol 2, no 1, pp 1-2.
23 Note that 12 pieces of separate counter-terrorism legislation hit the statute books 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 Security Agenda*, (Altin Nokta Publishing, 2010). For the evolution of security-centred governance see, Norris M, 'Fifteen years on from 9/11, how the UK bypassed justice to become a counter-terrorism state', *New Statesman*, 11 September 2016, http://www.newstatesman.com/politics/uk/2016/09/fifteen-years-911-how-uk-bypassed-justice-become-counter-terrorism-state.
24 Garside R, 'Assessing the General Election Manifestos', Centre for Crime and Justice Studies, 26 May 2017, https://www.crimeandjustice.org.uk/publications/assessing-general-election-manifestos.
25 The Conservative Party Manifesto 2017, https://www.conservatives.com/manifesto.
26 Ibid.
27 Information Commmissioner's Office, Overview of the GDPR, https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.
28 The Conservative Party Manifesto 2017, https://www.conservatives.com/manifesto.
29 Benson, V, 'UK politicians are planning very different approaches to data privacy, security and surveillance', *The Independent*, 6 June 2017. Available at: http://www.independent.co.uk/life-style/gadgets-and-tech/what-will-the-uk-election-mean-for-online-privacy-a7775211.html.
30 See s 253(5) of the Investigatory Powers Act 2016. Also note that tech companies are already under pressure to remove and manage terror and extremist content. BBC News, 'Theresa May to warn tech firms over terror content', 20 September 2017, http://www.bbc.co.uk/news/uk-politics-41327816.
31 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 September 2017, https://zephoria.com/top-15-valuable-facebook-statistics/.
32 The Conservative Party Manifesto 2017, https://www.conservatives.com/manifesto.
33 Gambling Commission,' Overview of the measures in the ABB's Social Responsibility Code and NCF's "Playing Safe" statement of principles', 12 March 2014, http://www.gamblingcommission.gov.uk/PDF/board-papers/GCP1420-Overview-of-measures.pdf.
34 Griffiths M,' Does Internet and Computer "Addiction" Exist? Some Case Study Evidence', (2004) *Cyber Psychology & Behaviour*, vol 3(2), 211-18, and O'Keeffe G S and Clarke-Pearson K, 'The Impact of Social Media on Children, Adolescents, and Families', (2011) *Pediatrics* vol 127 No 4, 800-04.
35 Ibid.
36 The Labour Party Manifesto 2017, http://www.labour.org.uk/index.php/manifesto2017.
37 Ibid, p 77.
38 Newton T,' How did Labour vote on the Investigatory Powers Act', PC Mag UK, 1 December 2016, http://uk.pcmag.com/ip-act/86389/feature/how-did-labour-vote-on-the-investigatory-powers-act.
39 MacAskill E, '"Extreme surveillance" becomes UK law with barely a whimper', *The Guardian*, 19 November 2016, https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper.
40 The Labour Party Manifesto 2017, http://www.labour.org.uk/index.php/manifesto2017.
41 The election secured only eight parliamentary seats for the Liberal Democrats. BBC News, Election 2017, http://www.bbc.co.uk/news/election/2017/results/england.
42 Liberal Democrats Manifesto 2017, https://www.libdems.org.uk/manifesto.
43 Mac Giollabhui S, *et al*, 'Watching the watchers: conducting ethnographic research on covert police investigation in the United Kingdom', (2016) *Qualitative Research*, vol 16, no 6, 630-45.
44 MacAskill, E. (2016) 'Extreme surveillance' becomes UK law with

barely a whimper. The Guardian Surveillance. November 2016. Available at: https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper#_blank.

45 Bakir V *et al*, 'Public Feeling on Privacy', *Security and Surveillance*, 2015, https://sites.cardiff.ac.uk/dcssproject/files/2015/11/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf; Thomson *et al*, 'A socio-ecological approach to national differences in online privacy concern: The role of relational mobility and trust', (2015) *Computers in Human Behaviour*, vol 51, Part A, pp 285-92; and Davies D, 'Public "acutely aware" of state surveillance, study finds', BBC News, 18 June 2015, http://www.bbc.co.uk/news/uk-wales-politics-33184722.

46 YouGov, (2017) Broad support for increased surveillance powers, http://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/guozfocn1q/YGC,%20GB%20Surveillance%202017.pdf.

47 YGC (2017), 'Broad support for increased surveillance powers', YouGov plc. Available at: http://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/guozfocn1q/YGC,%20GB%20Surveillance%202017.pdf.

48 While it is beyond the scope of this article, it is worth considering that terrorism 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 Findlay V, 'The Thin Blue Line and the Impct of Terrorism on the Transformation of Law Enforcement', Centre for Security Governance, 31 July 2015, http://secgovcentre.org/2015/07/the-thin-blue-line-and-the-impact-of-terrorism-on-the-transformation-of-law-enforcement/; Walker C, 'Journalist, Terrorist or Counter-Terrorist? The Perils of Invesitgative Journalism Post 9/11', (2015) IMODEV, vol 2, http://ojs.imodev.org/index.php/RICO/article/view/19/94; and Lynch A, 'The Impact of Post-Enactment Review on Anti-Terrorism Laws: Four Jurisdictions Compared', (2012) *The Journal of Legislative Studies*, vol 18, issue 1, pp 63-81.

49 Supra, Privacy International.

50 Benson, V., Saridakis, G., Tenakoon, H. (2015) «Information disclosure of social media users: Does control over personal information, user awareness and security notices matter?», Information Technology & People, Vol. 28 Issue: 3, pp.426-441, https://doi.org/10.1108/ITP-10-2014-0232.

51 For a detailed analysis of privacy, human rights and security in the digital age see, Nyst C and Falchetta T, The Right to Privacy in the Digital Age, (2017) Journal of Human Rights Practice, Vol. 9, Issue 1, pp. 104-118.

52 Fenwick explains informational autonomy (a.k.a informational self-determination) as the individual's interest in controlling the flow of personal information about herself, Supra Fenwick H, p 687.

53 For a comprehensive analysis of relevant jurisprudence see, Fenwick H, *Fenwick on Civil Liberties and Human Rights*, (Routledge, 2017) pp 66-75.

54 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

55 In *Harman and Hewitt v UK* (1992) 14 EHRR 657, the court held that the activities of MI5 in placing the applicants under surveillance were not in accordance with the law.

56 *Malone v United Kingdom* (1984) 7 EHRR 14, [67].

57 *Camenzind v Switzerland* (1999) 28 EHRR 458.

58 *Leander v Sweden* (1987)9 EHRR 433.

59 *Bykov v Russian* Federation, App no 4378/02, IHRL 3609 (ECHR 2009); *Klass v Federal Republic of Germany* (1978) 2 EHRR 214; and *Ludi v Switzerland* (1993) 15 EHRR 173.

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

61 *Liberty v GCHQ* [2014] UKIPTrib 13_77-H. See also the Regulation of Investigatory Powers Act 2000.

62 Fenwick D, 'State Surveillance' in Fenwick H, *Fenwick on Civil Liberties and Human Rights*, (Routledge, 2017) ch 11.

63 *Powell and Rayner v UK* (1990) 12 EHRR 458. See also *MS v Sweden* (1999) 28 EHRR 313.

64 *Murray v UK* (1994) 19 EHRR 193.

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, 21 December 2016.

66 For summary of how jurisprudence pertaining to privacy has informed and moulded legal developments see, 'Justice, Freedom from Suspicion – Surveillance Reform for Digital Age,' October 2011, State Watch, http://www.statewatch.org/news/2011/nov/uk-ripa-justice-freedom-from-suspicion.pdf.

67 *X and Y v Netherlands* (1985) 8 EHRR 71, at [24] stating that protection Art 8 rights may require the state to put in place measures to govern relations between private persons.

68 HM Government, 'Security, law enforcement and criminal justice, A Future Partnership paper', http://www.statewatch.org/news/2017/sep/uk-post-brexit-security-justice-cooperation-paper-9-17.pdf.

69 House of Commons, Business, Innovation and Skills Committee, 'The Digital Economy', Second Report of Session 2016-17, https://publications.parliament.uk/pa/cm201617/cmselect/cmbis/87/87.pdf.

70 Department for Digital, Culture Media and Sport, Official Statistics – 'Digital Sector Economic Estimates 2016 – Key Findings', 26 Janaury 2016, https://www.gov.uk/government/publications/digital-sector-economic-estimates-january-2016/digital-sector-economic-estimates-2016-key-findings.

71 https://www.gov.uk/government/news/uk-outlines-proposals-for-shared-approach-on-data-protection.

72 The Labour Party Manifesto 2017. Available at www.labour.org.uk/manifesto

73 Department for Digital, Culture, Media and Sport and Matt Hancock MP, 'Consultation on the Security of Network and Information Systems Directive', 8 August 2017, https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive.

74 European Commission, Digital Single Market,The Directive on the security of network and information systems, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. For the NIS Directive see, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535.

75 https://www.gov.uk/government/collections/data-protection-bill-2017.

76 Stone, J, 'British data protection laws to stay "aligned" with the EU's after Brexit', *The Independent*, 23 August 2017, http://www.independent.co.uk/news/uk/politics/data-protection-rules-brexit-matt-hancock-eu-laws-rules-a7909156.html.

77 Morris, C, 'Reality Check: What is the European Court of Justice?' BBC News, 23 August 2017, http://www.bbc.co.uk/news/world-europe-40630322. Also see, http://www.bbc.co.uk/news/uk-politics-41012265.

78 The House of Lords Select Committee on the European Union, 'Online platforms and the digital single market', April 2016, https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf.

79 The House of Commons Business, Innovation and Skills Committee, 'The Digital Economy, Second Report of Session 2016-17', https://publications.parliament.uk/pa/cm201617/cmselect/cmbis/87/87.pdf.

Case Notes & Comments

Right of 'communication to the public': *Stichting Brein v Ziggo BV and XS4All Internet BV*, Court of Justice of the European Union, 14 June 2017

Introduction

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

The ruling, which follows the opinion of Advocate General Szpunar[2] states that the actions of the operators of an online sharing platform such as The Pirate Bay (TPB) in making available and managing access to protected works, and by indexing torrent files allowing internet users to locate and download these works through a peer-to-peer network, constitute a 'communication to the public' within the meaning of Article 3(1).

For the past decade 'communication to the public' has been an evolving topic subject to a series of decisions. The term is present not only in the InfoSoc Directive but also in Directive 2006/115/EC on rental right and lending right and on certain rights related to copyright.[3] Under Directive 2006/115/EC, this concept has been addressed in *Verwertungsgesellschaft Rundfunk GmbH*,[4] *PPL (Ireland)*,[5] and *SAGE*.[6] In the internet era, 'communication to the public' under the InfoSoc Directive has been considered in recent cases such as *Svensson and Others*,[7] *GS Media*,[8] and *BestWater International*.[9] While these cases considered the secondary communication of works through hyperlink, *Stichting Brein v Ziggo* concerned an original communication made on a peer-to-peer network. In addition, the present case is significant because the liability of internet providers for copyright infringement is considered for the first time at European level by the CJEU.[10] Previously all relevant CJEU decisions focused on related injunctions against these operators whose platforms were used by third parties to infringe.[11]

Background to the judgment

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

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

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

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

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

The decision was appealed to the Hoge Raad der Nederlanden (Supreme Court of the Netherlands), which established that TPB made protected works available to the public without the right holders' consent and that subscribers of Ziggo and XS4ALL infringed copyrights, but was undecided whether TPB made a 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:

1 Is there a communication to the public within the meaning of Article 3(1) of Directive 2001/29 by the operator of a website (TPB), if no protected works are available on that website, but a system exists … by means of which metadata on protected works which are present on the users' computers are indexed and categorised for users, so that the users can trace and upload and download the protected works?

2 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