

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

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

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.

- 83 See s 3.3.6.
- 84 See IMPRESS: *The Independent Monitor for the Press CIC Regulatory Scheme*, version 3, para 2.2; *Applied 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 Haswood and Brigit Morris, 'Press codes and the spirit of equality legislation: implementing Leveson' (2016) 21 *CLJ* 29, 29.
- 86 Luxembourg Press Council's Code of Ethics, art 11(c) prohibition... of racial, ethnic, religious and ideological discrimination.'
- 87 See *Belgian Media Code 2004*, para 2.5; *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 VI, '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 3, 'Not to advocate war, violence or pornography in any form.'
- 91 *Editors' Code of 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/finding-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 (P 1) recommendation 38.
- 97 See *Alan Dyke (BBC Radio Solent) Ofcom Broadcast Bulletin*, Issue 29/2, 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/equalsities-and-human-rights-commission.pdf>, accessed 27 October 2017.
- 99 Clause 4.1.
- 100 See the over-emphasis of 'rationally' in some recent road tragedies in *Daily Mail*, Rachel Barford, 'Our lives changed in the blink of an eye: the tragic for the family of a mother and three children killed by a Polish taxi 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-taxi-driver-30-kill-mother-three-children-scrolling-mobile-phone-change-must-jailed-ten-years.html#ixzz4yb19jpcw>, accessed 4 November 2017.
- 101 See 02741-15 *Greer v The Sun* [https://www.ipso.co.uk/finding-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 29A8 and 29B.
- 110 *Ibid.*, ss 29A8 and 29B.
- 111 See 02741-15 *Greer v The Sun* [https://www.ipso.co.uk/finding-and-resolution-statements/ruling/?id=02741-15], accessed 4 November 2017.
- 112 *Ibid.*, para 9.
- 113 *Editors' Code*, cl 2; *Standards Code*, cl 7.1.
- 114 *Standards Code*, cl 7.2(b).
- 114 *Editors' Code*, cl 3; *Standards Code*, cl 5.2(a).
- 115 *Editors' Code*, cl 10(0); *Standards Code*, cl 7.2(a).
- 116 *Editors' Code*, cl 10(0); *Standards Code*, cl 5.2(a).
- 117 See *Editors' Code*, public interest proviso, point 5 (in regards to 'override 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(f).
- 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.editorcode.org.uk/history_of_the_code.php, accessed 24 October 2017.
- 129 *Evan Harris*, 'Newspaper industry releases revised 'Editors' Code', *morning.com* for tablets, nothing for the public', *Hacked Off* website, 4 December 2015 <http://hackedoff.org/comment/newspaper-industry-releases-revised-editors-code-more-comfort-for-tablets-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 (P 4), para 4.24. See also discussion in M Koppel-Falmer, 'The emergence of a new culture: 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 Publishers 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 7.26.
- 144 'User generated content', ONKethis website, undated <https://ethis.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

Wadlena Benson and Unut 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.

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 months¹ it is likely to remain as such in the immediate future.² 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.³ 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.⁴ Thus, the failure to collect and retain such data or surveillance evidence can lead to a collapse of the prosecution of suspects.⁵ 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.⁶ For example, identity theft has been reported to be at epidemic levels in 2017.⁷ Online and digital presence increase with the activities people pursue. The consequent digital foot-print, assets and behaviour left behind in the 'digital woods'⁸ as a 'virtual treasure trove'⁹ not only have an economic and a sentimental value for us but also value for businesses, commercial advantage¹⁰ 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 (ECtHR) 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 attacks²⁰ 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 legislation²² 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 overreaching 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 that 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 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 results⁴⁷ 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

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

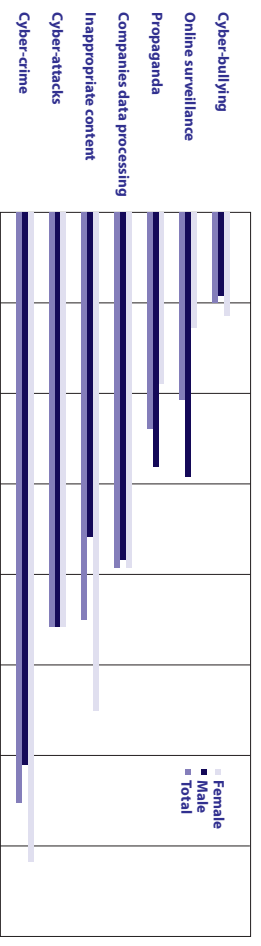


Figure 1: Gender differences in state surveillance concerns

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

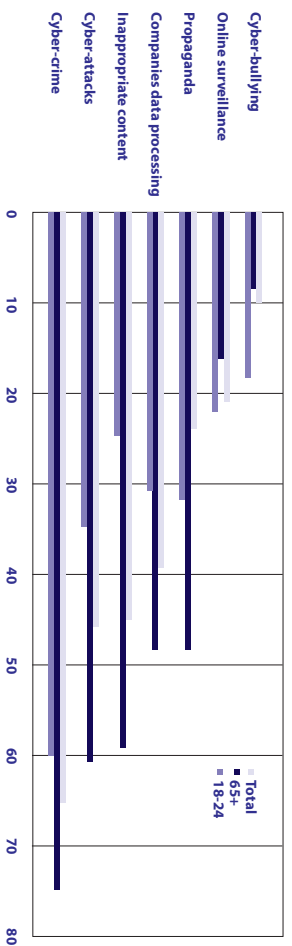


Figure 2: Age differences in state surveillance concerns

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

Disparities in the public's attitude as to whether national security overshadows 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

parties (eg content aggregators, agencies and government) as well as both 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 autonomy⁵² 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 from 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 required⁶⁰ (as is the case in the UK⁶¹) 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 interests 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, necessary 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 *Telci Szvege 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 statistics, the digital economy continued just over 7 per cent of the British GVA 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;

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'.⁴⁸ 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.⁴⁹ In online transactions users are losing out to service providers. This transfer of control now includes third

