Contemporary Challenges: The Global Crime and Security Journal (2025) Vol. 6

Research Article

"If I Have Nothing to Hide, I Have Nothing to Fear": A Critical Analysis of Surveillance and Privacy in the Digital Age regarding UK, EU, and US Law

Jared Higgins

Received: 01 February 2025 / Accepted: 10 June 2025

©TheAuthor(s), 2025

Abstract

Debate on digital surveillance typically centres on the familiar claim that "those with nothing to hide have nothing to fear", a claim that continues to justify extensive monitoring programs across the UK, EU and US. This essay shows that in practice, the idea that law-abiding individuals have no meaningful privacy interests overlooks the wide range of information-based harms that surveillance can produce, each of which affects people irrespective of wrongdoing. The analysis examines the legal safeguards intended to limit state access to personal data, focusing in particular on ECHR jurisprudence concerning bulk interception, data retention and encryption. It argues that although these safeguards constrain some forms of state surveillance, they leave substantial gaps. Adopting a comparative approach, the essay highlights how private and foreign surveillance operate under weaker oversight yet generate extensive data flows that states can obtain indirectly, often without activating domestic protections. The essay concludes that these structural weaknesses, combined with the business models of the modern internet, make it increasingly difficult to control information-based harms, raising the broader question of whether such harms are becoming an unavoidable feature of contemporary digital life.

The 'nothing to hide' argument has been described as 'the most common retort against privacy advocates'.[777] It suggests that state surveillance programs only threaten the privacy of criminals; as such, law-abiding citizens should have nothing to fear.[778] The Snowden leaks demonstrate the scale of information that can be gathered via the internet; as such, many remain wary of these powers.[779] Despite this, the argument continues to surface in privacy discourse.[780]

This essay will critically evaluate the 'nothing to hide' argument in light of surveillance in the digital age. It will first summarise why digital surveillance powers have emerged, how the 'nothing to hide' argument applies to these, and the risk they pose. It will then outline the stringent rules developed to limit state surveillance powers in the UK. It will argue that whilst law-abiding citizens do have things which they would prefer to keep private, the safeguards in place are largely successful in preventing 'information-based harms'. That said, there are several key shortcomings in preventing foreign and private surveillance, through which these rules can be circumvented and the potential for harm is exacerbated. These are weaknesses around which the modern internet is built, thus potentially difficult to solve. It begs the question: are information-based harms the price we pay for 'information technology'?

I. 'If I have nothing to hide, I have nothing to fear'

The internet has created significant challenges for law enforcement agencies worldwide. A UK report into surveillance powers in 2014 stated that *'the infrastructure of the internet can make it difficult to attribute communications to their sender and so offers a "cloak of anonymity" for communications.'*[781] This is amplified by certain privacy-enhancing tools, such as 'virtual private networks' (VPNs) and end-to-end encryption.[782] Tragedies such as the Westminster Bridge attack have brought stories

[777] Daniel Solove, ""I've Got Nothing to Hide" and Other Misunderstandings of Privacy" *San Diego Law Review* 44 (2007): 747, https://ssrn.com/abstract=998565.
[778] Ibid.,753.
[779] Vide Glenn Greenwald, *No Place to Hide – Edward Snowden, the NSA and the Surveillance State* (Mcclelland & Stewart, 2015).
[780] HL Deb 4 November 2015 vol 601, col 990.
[781] David Anderson, 'A Question of Trust: Report of the Investigatory Powers Review', *Independent Reviewer of Terrorism Legislation*, para. 4.17, https://assets.publishing.service.gov.uk/media/5a7f9b66ed915d74e622b7ca/IPR-Report-Web-Accessible1.pdf.
[782] Ibid., para. 4.21, 4.48, 4.49.

of how perpetrators used encrypted messaging services (such as WhatsApp) to plan their attacks to evade detection by law enforcement. One former head of the Government Communications Headquarters (GCHQ) would warn that US platforms were becoming *'the command and control networks of choice'* for terrorists.[783] In response to such threats, governments have long sought powers to monitor the internet to detect, investigate and prosecute crimes.

In the UK, many digital surveillance powers are found within the Investigatory Powers Act (IPA) 2016. This creates powers of 'bulk surveillance', the defining feature of which is that they allow public authorities *'to have access for specified purposes to large quantities of data, a significant portion of which is not associated with current targets.'*[784] For example, the Act creates the power to issue 'bulk warrants', allowing for the interception, compelled disclosure and retention of large quantities of data.[785] It also contains 'data retention' provisions, requiring telecommunications operators to store certain data for a period of time.[786] This data can then be used to reconstruct the activities of suspects, victims and vulnerable people; '*it ties suspects and victims to a crime scene and helps locate vulnerable people at risk of imminent harm.'*[787] These powers *'ensure the intelligence services and law enforcement have the powers they need to keep pace with a range of evolving threats from terrorists, hostile state actors, child abusers and criminal gangs.'*[788]

The justification for such wide-reaching surveillance powers is often a variation of "if I have nothing to hide, I have nothing to fear". For example, one MP in a parliamentary debate on the draft IPA said: *'we should unite against extremism using all modern*

[783] Ben Quinn, James Ball and Dominic Rushe, "GCHQ chief accuses US tech giants of becoming terrorists' 'networks of choice" *The Guardian,* November 3, 2014 https://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan.

[784] David Anderson, Report of the Bulk Powers Review (Cm 9326, 2016) para 1.5.

[785] Investigatory Powers Act 2016, pt 6.

[786] Ibid., pt 4.

[787] UK Government, "Government Note on the European Court of Justice Judgement (Press Briefing)" *UK Government*, accessed May 9, 2024, https://assets.publishing.service.gov.uk/media/5a7d7923ed915d2d2ac0929e/DRIPgovernmentNoteECJjudgment.pdf.

[788] "Investigatory powers enhanced to keep people safer," *Gov.UK,* April 25, 2024, https://www.gov.uk/government/news/investigatory-powers-enhanced-to-keep-people-safer#:~:text=Urgent%2C%20targeted%20changes%20made%20to,from%20terrorists%2C%20hostile%20state%20actors%2C.

tools appropriately, and if there is nothing to hide, there is nothing to fear…'[789] This argument typically suggests that state surveillance programs will result in a very limited disclosure of information - which is unlikely to be threatening to the privacy of law-abiding citizens. Instead, such programs are seen as primarily targeting individuals involved in illegal activities, whose privacy interests are considered negligible or non-existent. Moreover, any security interest in preventing crime outweighs *'whatever minimal or moderate privacy interests law-abiding citizens may have in these particular pieces of information*.'[790]

This argument is controversial. In a debate on the IPA, Lord Strasburger argued, *'do we not all have something to hide that we would prefer to keep to ourselves? That is why we shut the toilet or bedroom door behind us.'*[791] For example, there are things we instinctively feel are private - such as our religion, political persuasion or sexual proclivities - information that could be used to blackmail, demean or single people out for disadvantageous treatment by unscrupulous governments.[792] As such, it is seemingly counterintuitive to suggest that anyone truly 'has nothing to hide'.[793]

Solove advances a broad 'taxonomy of privacy', outlining the various harms that can emerge from breaches of privacy. In the context of 'bulk interception', this might include the chilling effect of knowing that one is being surveilled, potentially undermining freedom of expression. [794] Conversely, the harms posed by data retention may include increasing people's vulnerability to potential abuse of their information. Information 'insecurity' describes problems caused by the way our information is handled and protected.[795] Van den Hoven describes these as "information-based harms", citing the example of World War II: *'when the Nazis occupied The Netherlands and found a well-organized population registration very conducive to their targeting*

[789] HL Deb 4 November 2015 vol 601, col 990.
[790] Solove,*""I've Got Nothing to Hide" and Other Misunderstandings of Privacy"*, 752-753.
[791] HL Deb 20 November 2023 vol 834, col 637.
[792] Ibid.
[793] David H Flaherty, "Visions of Privacy: Past, Present and Future" in *Visions of Privacy, Policy Choices for the Digital Age,* eds. Colin J Bennett and Rebecca Grant (University of Toronto Press 1999), 31.
[794] Solove, *""I've Got Nothing to Hide" and Other Misunderstandings of Privacy",* 758.
[795] Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (January 2006): 477–564. https://ssrn.com/abstract=667622.

and deportation of the Jews in Holland.'[796] Given these concerns, many reject the 'nothing to hide' argument; broadly, law-abiding citizens do have things to hide, and thus might reasonably have things to fear.

These criticisms are largely successful in rebutting the 'nothing to hide' argument. For one, the statement 'I have nothing to hide' is deeply flawed; most law-abiding citizens *do* have things that they wish to hide. Moreover, breaches of privacy can lead to tangible information-based harms, thus providing valid fears. A more accurate statement would thus be that we all have things to hide, hence we all have things to fear from surveillance. That said, these criticisms ultimately fail to show that the threat to privacy outweighs the need for surveillance programs. It is generally accepted that the state will carry out surveillance programs in our collective interests as part of the 'social contract'[797] for which many human rights instruments recognise privacy as a 'qualified right' permitting some degree of interference.[798] Rather, the existence of such 'information-based harms' makes the case for stringent rules on how data is collected, processed or disseminated. We already have a strict legal framework to control surveillance powers, designed to allay 'fears' about abuse. It remains to be seen whether these measures are effective in preventing 'information-based harms', to which this essay now turns.

II. Surveillance Law and 'Information-Based Harms'

The UK is a signatory to the European Convention on Human Rights (ECHR), Article 8(1) of which outlines the right to 'private and family life, home and correspondence'. Despite this, surveillance is not prohibited; Article 8(2) permits interference with this right, 'so long as it is in accordance with the law and is necessary in a democratic society.' Broadly, to be 'in accordance with the law' there must be some basis in domestic law for the surveillance, and that the law must meet certain quality requirements: accessibility, foreseeability of consequences, and compatibility with the

[796] Jeroen van den Hoven, "Information Technology, Privacy and the Protection of Personal Data" in *Information Technology and Moral Philosophy*, eds. Jeroen van den Hoven and John Weckert (Cambridge University Press 2008), 312.

[797] Andrew Murray, *Information Technology Law* (Oxford University Press, 2020), 681.

[798] cf US Constitution; Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR); International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

rule of law.[799] Surveillance 'necessary in a democratic society' has been understood as requiring that it is a 'proportionate means of achieving a legitimate aim'. This creates a wide 'margin of appreciation' for national authorities in choosing how best to achieve the legitimate aim of protecting national security and has been applied differently in respect of different forms of digital surveillance.[800]

A. Bulk interception

Given the difficulties faced by states in countering online threats, the European Court of Human Rights (ECtHR) has accepted the use of bulk interception powers as being consistent with Article 8.[801] That said, *'in operating such a system the margin of appreciation afforded to them must be narrower and a number of safeguards will have to be present'* given the considerable risk that these powers may be used to undermine rights to privacy.[802] These safeguards require that domestic law should prescribe the procedure to be followed for examining, utilising, and storing the data obtained, and the precautions to be taken when communicating the data to other parties. Additionally, it should set out a limit on the duration of the bulk interception measures and the circumstances in which intercepted data will be erased or destroyed.

It also requires additional 'end-to-end safeguards': independent authorisation, supervision, independent ex-post facto review, and ongoing assessment of the necessity and proportionality of the measures being taken.[803] Previous UK surveillance laws have fallen short of these standards. For example, the ECtHR noted 'fundamental deficiencies' in bulk interception powers under section 8(4) of the Regulation of Investigatory Powers Act 2000, lacking sufficient end-to-end safeguards to provide adequate and effective guarantees against the risk of abuse.[804] The IPA has sought to address this – for example, it adds the need for a bulk warrant to be granted personally by the Secretary of State and approved by a Judicial Commissioner[805] (the 'double-lock'). As such, the bulk warrant provisions of the IPA have so far withstood

[799] *Kruslin v France* (1990) 12 EHRR 547 [27].
[800] *S and Marper v United Kingdom* (2009) 48 EHRR 50 [102].
[801] *Big Brother Watch v United Kingdom* (2022) 74 EHRR [340].
[802] Ibid., [347].
[803] *Big Brother Watch v United Kingdom* (2022) 74 EHRR [348]-[350].
[804] Ibid., [425].
[805] Investigatory Powers Act 2016, s 142.

judicial scrutiny.[806]

B. Data Retention

Concerns about proportionality and safeguards against abuse have also led to the repeal of various 'data retention' laws. The case of *Podchasov v Russia* concerned a Russian law which required the continuous automatic storage of all internet communications for six months in Russia, affecting all users of internet communications, even in the absence of reasonable suspicion. The ECtHR was '*struck by the extremely broad duty of retention provided by the contested legislation',* concluding that the interference was '*exceptionally wide-ranging and serious.'*[807] Moreover, as this content was practically available to Russian authorities in lieu of authorisation, the law lacked adequate safeguards against arbitrariness and abuse.[808] Consequently, it contradicted 'the very essence of the right to respect for private life under Article 8 of the Convention' and 'overstepped any acceptable margin of appreciation'.[809] Drawing on the jurisprudence of the ECtHR, the European Court of Justice (ECJ) ruled that the EU's 'Data Retention Directive' was a disproportionate interference with privacy rights under the EU's Charter of Fundamental Rights. This is as it did not contain any objective criteria limiting access to data, whilst failing to establish any time limits on the retention of that data. At the same time, it applied to all 'subscribers and registered users' of electronic communication, thus entailing an interference with the fundamental rights of practically the entire European population. For similar reasons, the High Court found data retention powers under Part 4 of the IPA to be invalid.[810]

C. Encryption

The ECtHR in *Podchasov* also commented on the impact of degrading or discouraging the use of encryption (specifically end-to-end encryption (E2EE)). Whilst noting that

[806] *R (on the application of National Council for Civil Liberties) v Secretary of State for the Home Department* [2023] EWCA Civ 926 [2023] EMLR 22 [128].
[807] *Podchasov v Russia* App no 33696/19 13 (ECtHR, February 2024) [70].
[808] Ibid., 73.
[809] Ibid., 80.
[810] *R (on the application of National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department* [2018] EWHC 975 (Admin) [2018] 3 WLR 1435.

encryption can be used by criminals, it also noted that weakening encryption through the use of 'backdoors' would undermine the security of all users; backdoors technically allow for routine, indiscriminate surveillance of all users and can be exploited by cybercriminals.[811] In light of the above, the Court concluded that a statutory obligation to decrypt end-to-end encrypted communications risked amounting to a requirement that providers of such services weaken the encryption mechanism for all users and was therefore disproportionate to the legitimate aims pursued.[812]

D. Effective?

Whilst it is debatable whether the ECtHR has struck the right balance, these rules somewhat mitigate the risk of information-based harms emerging. For example, knowledge that bulk interception and data retention powers are limited, requiring strong safeguards against abuse, encourages people to communicate freely over the internet. As a party to the ECHR, the government should, in principle, be trusted to comply with these rules.[813] Some support for this might be found in the fact that – even in the context of secret, ultimately unlawful surveillance measures – the ECtHR has found no evidence of the UK government abusing surveillance powers.[814] At the same time, the availability of strong encryption tools provides an additional layer of protection against government overreach; the success of which is demonstrated by ongoing attempts to ban or undermine encryption tools.[815] This, ultimately, seems to assuage some of the 'fears' emerging from digital surveillance.

That said, there are some issues with this argument. The jurisdiction of UK surveillance law is limited to activities carried out by UK government bodies, leaving significant gaps in protection. Notably, it does not extend to surveillance conducted by private companies or foreign governments - both of which are increasingly prevalent and facilitated by the global nature of the internet. This raises serious concerns, as private and foreign surveillance often operate with fewer safeguards and accountability measures, heightening the risk of information-based harms. The following sections

[811] *Podchasov v Russia* App no 33696/19 13 (ECtHR, February 2024) [77], [78].
[812] *Podchasov v Russia* App no 33696/19 13 (ECtHR, February 2024) [79].
[813] Hof's-Den Haag 14 maart 2017 NJF 2017/200 X appellanten en de Staat der Nederlanden (Neth.) para 3.4.
[814] *Big Brother Watch v United Kingdom* (2022) 74 EHRR [474].
[815] Chris Vallance, "UK amends encrypted message scanning plans" *BBC,* July 19 2020. https://www.bbc.co.uk/news/technology-66240006. accessed May 9, 2024

explore how these forms of surveillance present distinct challenges to individual privacy and may, in some cases, serve as indirect avenues for circumventing domestic legal protections.

III. Jurisdiction and information-based harm

A. Private Surveillance

The rise of 'private surveillance' via the internet carries significant privacy implications. Personal data is often collated to build a detailed profile of individuals' preferences, interests and aversions - information that is frequently sold to third parties.[816] This has been controversial; using Facebook user data, Cambridge Analytica was able to accurately predict political leanings and influence elections[817] – exposing UK citizen data to a 'serious risk of harm'.[818] For example, such information might be used in a discriminatory manner,[819] and 'nudging' via advertisements might represent a form of 'decisional interference'.[820] The Cambridge Analytica scandal demonstrates a real risk of information-based harms emerging from private surveillance. As such, data protection law has developed to limit private surveillance.

In the UK, data protection law is governed by the Data Protection Act 2018, which implements the EU's General Data Protection Regulation (GDPR). Broadly, data must be processed in accordance with certain criteria: consent, contractual necessity, legal obligation or public interests, and legitimate interests.[821] Moreover, it requires that data must be processed in accordance with a number of principles (such as fairness, lawfulness and transparency) and creates a list of 'data subjects rights'.[822] This

[816] Joint Committee on Human Rights*, The Right to Privacy (Article 8) and the Digital Revolution* (HC 122) 3.

[817] Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," *New York Times,* April 4, 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. accessed May 9, 2024.

[818] "Facebook agrees to pay Cambridge Analytica fine to UK" *BBC,* 30 October 2019, https://www.bbc.co.uk/news/technology-50234141.

[819] Joint Committee on Human Rights*, The Right to Privacy (Article 8) and the Digital Revolution* (HC 122) paras 79-92.

[820] Solove, ""I've Got Nothing to Hide" and Other Misunderstandings of Privacy" 759.

[821] Data Protection Act 2018, s 8; see also Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[822] Ibid., ss 12-14, 34-40.

mitigates information-based harm – for example, requiring that data is stored securely, in a form permitting identification for no longer than necessary, and allowing users a right to data erasure.[823] The effect of this is that it 'places more power at the user's end and extra responsibility at the business end.'[824] Whilst the GDPR has been hailed as the 'strongest privacy and security law in the world'[825], the wide range of lawful processing criteria allows greater liberty in collecting personal data than state surveillance regimes. Recently, the UK has signalled a shift away from GDPR in its draft 'Data Protection and Digital Information' Bill, which has been criticised as 'watering down' data protection rights.[826]

B. Foreign surveillance

Different legal jurisdictions have different privacy rules. This creates a problem for internet users: '*the rise of the global computer network is destroying … the ability of physical location to give notice of which sets of rules apply'.*[827] For example, internet users in the EU who store data with a US company may see their data being surveilled by US law enforcement. Under the US 'Clarifying Lawful Use of Overseas Data' (CLOUD) Act, US law enforcement agencies may subpoena data from US-based technology companies to provide data even if that data is stored overseas. This is significant, as the US lacks federal data protection laws, and non-US citizens lack constitutional privacy rights – allowing the US to operate a warrantless surveillance regime for foreign individuals under section 702 of the Foreign Intelligence Surveillance Act (FISA).[828] As such, these programmes lack stringent safeguards such as those laid down by ECtHR guidelines, increasing vulnerability to information-based harm.

---

[823] Ibid., ss 12-14, 34-40.

[824] Ramya Mohanakrishnan, "What Is GDPR and Why Is It Important?" *Spiceworks,* February 16, 2023. https://www.spiceworks.com/it-security/security-general/articles/what-is-gdpr/. accessed May 9, 2024.

[825] "What is GDPR, the EU's new data protection law?" *GDPR.EU*, accessed May 9, 2024, https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU.

[826] "How the new Data Bill waters down protections" Public Law Project*,* November 28, 2023, https://publiclawproject.org.uk/resources/how-the-new-data-bill-waters-down-protections/. accessed May 9, 2024

[827] David R. Johnson and David Post, "Law and borders: the rise of law in cyberspace" *Stanford Law Review* 48, no.5 (1996):1370, https://doi.org/10.2307/1229390.

[828] Foreign Intelligence Surveillance Act 1987 92 Stat. 1783

Concerns about the rights of EU citizens beyond borders culminated in the ECJ revoking the EU-US 'safe harbour' agreement.[829] Under this agreement, the US was recognised as a country with '*adequate'* protections for personal data, thus allowing for the free flow of personal data. *Inter alia*, the Court noted the lack of an effective remedy where citizens' rights have been infringed as being incompatible with their rights under Article 45(1) of the General Data Protection Regulation (GDPR).[830] The European Commission recently reinstated the US adequacy standing after an overhaul of the US legal framework, including a newly established 'Data Protection Review Court'. It remains to be seen whether the EU-US 'Data Protection Framework' will be overturned by a potential *'Schrems III'* case; however, it should be noted that the US House of Representatives recently re-approved section 702 of FISA – thus, powers for warrantless surveillance of foreign citizens remain.[831]

C. Loopholes?

Both private surveillance and surveillance by foreign governments create significant risks of information-based harm. At the same time, they present a potential loophole for the UK government. For example, the UK is party to a 'mutual trust' agreement with the US, allowing UK law enforcement agencies to send interception and production orders, authorised under UK law, directly to the US service providers, where there are no federal data protection laws.[832] Concerns have been raised about intelligence sharing under the 'Five Eyes' security alliance; that information gathered by foreign intelligence agencies and 'offered' to UK intelligence agencies effectively sidestepping domestic surveillance laws.[833]

The risk also remains that private surveillance might be used as a proxy for state

[829] European Commission, *Commission Decision 2000/520/EC*, Official Journal L 215, August 25, 2000.
[830] Case C - 311/18 *Data Protection Commissioner v Facebook Ireland Ltd* [2021] 1 WLR 751 [186].
[831] Nick Robins-Early, "House votes to reapprove law allowing warrantless surveillance of US citizens," *The Guardian*, April 12, 2024, https://www.theguardian.com/us-news/2024/apr/12/fisa-surveillance-act-reauthorized.
[832] cf Jessica Shurson, "Law Enforcement Access to Encrypted Data Across Borders" in *Transformations in Criminal Jurisdiction: Extraterritoriality and Enforcement*, eds. Micheál Ó Floinn et al., (Bloomsbury, 2023).
[833] Haroon Siddique, "Concerns over rise in requests for UK to share intelligence despite torture risks," *The Guardian,* March 27, 2024, https://www.theguardian.com/world/2024/mar/27/concern-rise-requests-uk-share-intelligence-despite-torture-risks#:~:text=The%20human%20rights%20group%20Reprieve,or%20extraordinary%20rendition%20was%20. accessed May 9, 2024.

surveillance. Whilst data protection rules mitigate information-based harm, these are less stringent than those required for state surveillance. This is concerning, as the effect may be the same; compelled disclosure under the IPA could result in a significant amount of personal data being made available to law enforcement bodies. This is a particularly pertinent issue: in early 2025, the UK Home Office issued a Technical Capability Notice (TCN) under the IPA, requiring Apple to create a backdoor into its Advanced Data Protection (ADP) service, which offers end-to-end encryption for iCloud data.[834] Apple subsequently removed the ADP feature from its services in the UK, leaving UK individuals at a greater risk of information-based harms. As such, data collected by private companies could serve as the soft underbelly of individual privacy.

IV. Conclusion

This essay has demonstrated how the 'nothing to hide' argument is flawed in light of surveillance in the digital age. It has shown how the average person generally has things which they would rather keep private, and that breaches of this privacy can lead to 'information-based harms.' Whilst some degree of state surveillance may be necessary, stringent rules have developed to mitigate against the harms arising from this. That said, the internet has undermined the effectiveness of these, allowing for both extensive 'private' and foreign surveillance, both of which operate with lesser safeguards against information-based harm. Moreover, information gathered from such surveillance can be obtained by UK law enforcement, ostensibly circumventing the safeguards developed under surveillance law.

These problems are unlikely to go away. Much of what we can use on the internet is free, as a business model has evolved in which companies make money from selling advertising opportunities rather than charging individuals to use the service.[835] At the same time, we can connect with people worldwide because of data flows across borders. Tackling both private and foreign surveillance would likely be impossible

[834] J Joseph Menn, "U.K. Orders Apple to Let It Spy on Users' Encrypted Accounts," *The Washington Post*, February 7, 2025, https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/. accessed May 28, 2025.

[835] Joint Committee on Human Rights*, The Right to Privacy (Article 8) and the Digital Revolution* (HC 122) 3.

without curtailing the free and open nature of the internet.[836] Is this a price worth paying for privacy?

[836] vide Mark Lemley, "The Splinternet" *Duke Law Journal* 70, no.6 (2023), http://dx.doi.org/10.2139/ssrn.3664027.

Bibliography

BBC. “Facebook agrees to pay Cambridge Analytica fine to UK.“ *BBC*. October 2019. https://www.bbc.co.uk/news/technology-50234141 accessed 9 May 2024

Big Brother Watch v United *Kingdom* (2022) 74 EHRR

Case C – 239/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources [2015] QB 127

Case C - 311/18 Data Protection Commissioner v Facebook Ireland Ltd [2021] 1 WLR 751 [186]

Clarifying Lawful Overseas Use of Data Act 2018 Pub.L. 115–141 (2018)

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

European Commission. Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce. 2000/520/EC. Official Journal L 215, August 25, 2000

Data Protection Act 2018

Anderson, David. ‘A Question of Trust: Report of the Investigatory Powers Review’. Independent Reviewer of Terrorism Legislation. Para. 4.17. https://assets.publishing.service.gov.uk/media/5a7f9b66ed915d74e622b7ca/IPR-Report-Web-Accessible1.pdf

Anderson, David. *Report of the Bulk Powers Review* (Cm 9326, 2016).

Flaherty, David H. “Visions of Privacy: Past, Present and Future” in *Visions of Privacy, Policy Choices for the Digital Age.* eds. Colin J Bennett and Rebecca Grant. University of Toronto Press 1999

Foreign Intelligence Surveillance Act 1987 92 Stat. 1783 Hof’s-Den Haag 14 maart 2017 NJF 2017/200 X appellanten en de Staat der Nederlanden (Neth.)

Johnson, David R., and Post, David. “Law and borders: the rise of law in cyberspace.” *Stanford Law Review* 48, no.5 (1996). https://doi.org/10.2307/1229390

Kruslin v France (1990) 12 EHRR 547 [27]

Gov.UK. “Investigatory powers enhanced to keep people safer.” April 25, 2024. https://www.gov.uk/government/news/investigatory-powers-

enhanced-to-keep-people-safer#:~:text=Urgent%2C%20targeted%20changes%20made%20to,from%20terrorists%2C%20hostile%20state%20actors%2C accessed 9 May 2024

GDPR.EU. "What is GDPR, the EU's new data protection law?" accessed 9 May 2024. https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU. accessed 9 May 2024

Greenwald, G. *No Place to Hide – Edward Snowden, the NSA and the Surveillance State*. Mcclelland & Stewart, 2015.

HL Deb 4 November 2015 vol 601

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

Investigatory Powers Act 2016

Joint Committee on Human Rights*, The Right to Privacy (Article 8) and the Digital Revolution* (HC 122) 3

Lemley, M. "The Splinternet." *Duke Law Journal* 70, no.6 (2023). http://dx.doi.org/10.2139/ssrn.3664027

Menn, Joseph. "U.K. Orders Apple to Let It Spy on Users' Encrypted Accounts." *The Washington Post*. February 7, 2025. https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/. accessed 28 May 2025

Mohanakrishnan, Ramya. "What Is GDPR and Why Is It Important?" *Spiceworks,* February 16, 2023. https://www.spiceworks.com/it-security/security-general/articles/what-is-gdpr/. accessed 9 May 2024

Murray, Andrew. *Information Technology Law* (Oxford University Press, 2020)

Confessore, Nicholas. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." *New York Times,* April 4, 2018 https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. accessed 9 May 2024

Podchasov v Russia App no 33696/19 13 (ECtHR, February 2024)

Public Law Project. "How the new Data Bill waters down protections." November 28, 2023. https://publiclawproject.org.uk/resources/how-the-new-data-bill-waters-down-protections/. accessed 9 May 2024

Quinn, Ben, Ball, James, and Rushe, Dominic. “GCHQ chief accuses US tech giants of becoming terrorists ‘networks of choice.” *The Guardian,* November 3, 2014. https://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan accessed 9 May 2024

Robins-Early, Nick. “House votes to reapprove law allowing warrantless surveillance of US citizens.” *The Guardian*, April 12, 2024. https://www.theguardian.com/us-news/2024/apr/12/fisa-surveillance-act-reauthorized accessed 9 May 2024.

R (on the application of National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department [2018] EWHC 975 (Admin) [2018] 3 WLR 1435

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1;

Shurson, Jessica. “Law Enforcement Access to Encrypted Data Across Borders” in *Transformations in Criminal Jurisdiction: Extraterritoriality and Enforcement*, eds. Micheál Ó Floinn et al. Bloomsbury, 2023

Siddique, Haroon. “Concerns over rise in requests for UK to share intelligence despite torture risks.” The Guardian, March 27, 2024. https://www.theguardian.com/world/2024/mar/27/concern-rise-requests-uk-share-intelligence-despite-torture-risks#:~:text=The%20human%20rights%20group%20Reprieve,or%20extraordinary%20rendition%20was%20concerning.. accessed 9 May 2024

Solove, Daniel J. “A Taxonomy of Privacy.” *University of Pennsylvania Law Review* 154, no. 3 (January 2006): 477–564. https://ssrn.com/abstract=667622.

Solove, Daniel. “"I've Got Nothing to Hide" and Other Misunderstandings of Privacy” *San Diego Law Review* 44 (2007). https://ssrn.com/abstract=998565.

UK Government. “Government Note on the European Court of Justice Judgement (Press Briefing)”. https://assets.publishing.service.gov.uk/media/5a7d7923ed915d2d2ac0929e/DRIPgovernmentNoteECJjudgment.pdf. accessed May 9, 2024

S and Marper v United Kingdom (2009) 48 EHRR 50

US Constitution

Van den Hoven, Jeroen. “Information Technology, Privacy and the Protection of Personal Data” in *Information Technology and Moral Philosophy*, eds. Jeroen van den Hoven and John Weckert. Cambridge University Press 2008.

Vallance, Chris. “UK amends encrypted message scanning plans“(BBC, 19 July 2020) https://www.bbc.co.uk/news/technology-66240006 accessed 9 May 2024