Policy Overview

Data Policies: Regulatory Approaches for Data-Driven Platforms in the UK and EU

Arne Hintz
Jessica Brand

IT for Change | April 2019

This report was produced as part of the research project ‘Policy frameworks for digital platforms - Moving from openness to inclusion’. The project seeks to explore and articulate institutional-legal arrangements that are adequate to a future economy that best serves the ideas of development justice. This initiative is led by IT for Change, India, and supported by the International Development Research Centre (IDRC), Canada.

Authors

Arne Hintz is Senior Lecturer at the School of Journalism, Media, and Culture at Cardiff University and co-Director of Data Justice Lab.

Jessica Brand is Research Assistant at Data Justice Lab.

Research coordination team

Principal Investigator: Anita Gurumurthy
Co-investigators: Deepti Bharthur, Nandini Chami
Editorial Support: Mridula Swamy, Amruta Lakhe
Design: Meenakshi Yadav, Prakriti Bakshi

IT for Change

IDRC | CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

Data Policies: Regulatory Approaches

for Data-Driven Platforms in the UK and EU

Arne Hintz

Jessica Brand

Data Justice Lab, Cardiff University

Page left intentionally blank

1. Introduction

With the proliferation of social media platforms, cloud services, and the so-called 'sharing economy', our online interactions increasingly rely on a small number of concentrated businesses that provide (or limit) access to online services, regulate interactions between users, and make decisions on what content is fit to be published, shared, and found. The core role of platforms in contemporary society has led to understandings of our current social configuration as 'platform society' (van Dijk, 2016) and 'platform capitalism' (Srnicek, 2016). However, the rapid emergence of platforms has also led to a policy vacuum, and their social, political, and economic consequences remain unregulated. This points to a need for policy development (Belli & Zingales, 2017).

The collection, analysis, and sharing of user data requires particular attention – in part, because it has significant implications for users and for state-business-citizen relations, and in part, because it affects the core business model of commercial platforms. Consumer, communication, and service platforms collect and monetize a vast range of data, often without the knowledge of their users. Platforms are a 'data mine' (Andrejevic, 2012) where personal data is systematically extracted, processed, and combined with additional datasets in order to create detailed profiles of people that are valuable to both the business sector and the state. Platforms are thus an integral part of contemporary 'surveillance capitalism' (Zuboff, 2015) that is defined by an accumulation logic and driven by the ability to predict and change human behavior to gain revenue based on the mass collection of personal data. Citizens are increasingly sorted, categorized, and assessed according to this data (Lyon, 2015).

Platforms are a 'data mine' where personal data is systematically extracted, processed, and combined with additional datasets in order to create detailed profiles of people that are valuable to both the business sector and the state

This report will review how data collection and analysis on platforms is regulated and will investigate recent trends and developments. It will focus on a particular jurisdiction – the United Kingdom (UK) – to offer a perspective on an advanced economy where platforms play a significant role in social and economic life. Further, the UK has demonstrated the political dimension of data collection via platforms with the recent Cambridge Analytica/ Facebook scandal (Greenfield, 2018). Yet, it also offers insights into the contradictory aspects of policy development with some laws enhancing, and others, restricting data collection, and into the interplay between national and regional policy. Despite the recent decision by the British government to leave the European Union (EU), the UK remains bound by European law and will do so for the near future, at least. This report therefore addresses both UK and EU policy developments that affect data collection, analysis, and sharing on platforms.

Rather than provide a comprehensive analysis, we focus on particular cases that demonstrate different dimensions of contemporary policy reform. At the national level, the Investigatory Powers (IP) Act and the Digital Economy (DE) Act have recently been adopted in the UK and provide comprehensive rules for the types and extent of access by the government and state institutions to personal data on platforms. At the EU level, the General Data Protection Regulation (GDPR), which came into effect in May 2018, sets a new policy framework for platforms by regulating their abilities to collect, analyze and share user data, and creates significant new requirements constraining the data activities of platforms. This report provides an overview of key debates regarding these new laws and assesses their implications for platforms. By mapping issues and debates, it offers the necessary background to a more detailed investigation into policy dynamics, reform, and alternatives that the research team is currently conducting.

The report begins with a critical assessment of the previous regulatory architecture in the UK, which was marked by the lack of a comprehensive approach, significant policy gaps and the lack of transparency. It then summarizes the core characteristics of, and debates on, contemporary policy reform, focusing on the three laws mentioned above. It demonstrates that policy development is far from consistent and that the emerging regulatory framework for platforms is marked by competing interests and approaches.

2. Charting the Digital Policy Landscape

So far, the data extraction industry of platforms, data trackers and data brokers has largely been allowed to operate in a context of self-regulation and tentative interpretations of user consent. In some jurisdictions, platforms and apps are required to seek acceptance from users for the ways in which these companies track their browsing habits and use their data. For example, the EU Directive on Privacy and Electronic Communications from 2002 (and amended in 2009) required 'explicit consent' from those who visit websites for the installation of 'cookies' that may identify, track, and profile them. However, this model of user consent has, in practice, required users to agree to the comprehensive collection of their data if they wish to partake in digital life through the most widely used platforms and services. The model places the burden of privacy protection on the individual and 'merely legitimises the extraction of personal data from unwitting data subjects' (Edwards & Veale, 2017, p. 49).

Yet, the data activities of platforms are affected by a broad regulatory context that includes data protection policies and allows for data access by state actors, such as law enforcement and intelligence agencies. In the UK, the Data Protection Act of 1998 controls access to, and use of, personal data, and provides limitations for data collection and sharing. However, it includes substantial exemptions for the protection of 'national security' and the prevention or detection of crime. Several other laws have specified access to data for such purposes. The Regulation of Investigatory Powers Act (RIPA) from 2000, as amended by the Data Retention and Investigatory Powers Act 2014, allows a Secretary of State to authorize the interception not only of the communications of a specific individual but also of wide-ranging and vaguely defined types of traffic in bulk. The Telecommunications Act 1984 offers the Secretary of State interception powers in communications networks, and the Intelligence Services Act 1994 provides the legal basis for the surveillance activities by GCHQ, the British intelligence agency. While it limits GCHQ's lawful activities to 'interests of national security', such interests have traditionally been interpreted broadly in UK law. More recent legislation, such as the Wireless Telegraphy Act 2006, has updated and extended older powers for the interception of communication (Hintz & Brown, 2017). A number of oversight bodies review these surveillance capabilities and their implementation. They include, on a one-off basis, the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing and the Independent Reviewer of Terrorism Legislation (appointed by the Secretary of State); and on an ongoing basis, the Information Commissioner (ICO); the Intelligence Services Commissioner; the Interception of Communications Commissioner; and the Intelligence and Security Committee (ISC) of Parliament. The Investigatory Powers Tribunal (IPT) has exclusive jurisdiction to hear complaints about the intelligence agencies or about interception.

These national rules, institutions, and processes are embedded in regional and international policy, such as the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which was incorporated into UK law in the Human Rights Act 1998. Article 8 of the Convention guarantees everyone's 'right to respect for his private and family life, his home and his correspondence' (Council of Europe, 1950). Regional courts, such as the European Court of Human Rights (ECHR), can hear complaints about surveillance and advise on its lawfulness. Directives adopted by the European Commission – such as the Data Retention Directive from 2006 – have to be implemented by all member states and thus, have far-reaching consequences for national law. The Data Retention Directive required telecommunications services to retain communications data – such as, who communicates on the internet with whom, at what time, and from what IP address – for up to two years. It was revoked in 2014 by the Court of Justice of the European Union but was effectively continued by the UK government at the national level when it adopted the Data Retention and Investigatory Powers (DRIP) Act. Following a legal challenge, this Act was ruled unlawful by the European Court of Justice in 2016 (Hintz & Brown, 2017).

The frequent interventions of courts demonstrate the role that judicial systems and court decisions have had in policy reform. This was the case, particularly, in the aftermath of the Snowden revelations which provided evidence of widespread data collection by state agencies. Campaign organizations such as Privacy International, Liberty, and Amnesty International successfully challenged GCHQ's surveillance practices at the Investigatory Powers Tribunal (IPT) and the European Court of Human Rights. Further, institutional reviews raised concerns with the legitimacy and legal grounding of state surveillance practices. For example, the Independent Reviewer of Terrorism Legislation criticized the legal framework as 'obscure', 'undemocratic' and 'intolerable' and called for a significant review and

re-development (Anderson, 2015, p. 13), and the Independent Surveillance Review of the Royal United Services Institute (RUSI) called for a 'democratic license' for the surveillance activities of intelligence agencies (RUSI, 2015, p. 97). At the international level, United Nations rapporteurs strongly condemned pervasive data collection. For example, former UN Special Rapporteur on Freedom of Expression and Opinion, Frank LaRue, has highlighted the right to privacy as an essential requirement for the realization of the right to freedom of expression (UN General Assembly, 2013). His successor, David Kaye, has emphasized the essential role of encryption and anonymity for people's rights to freedom of opinion and expression (Human Rights Council, 2015) and the Special Rapporteur on the right to privacy has criticized the surveillance practices and insufficient legal restrictions of countries such as the UK.

Policy processes are affected, moreover, by public opinion and by key stakeholders who influence the views held by policymakers. The aftermath of the Snowden revelations saw a significant increase in such efforts. Civil society organizations and campaign groups exerted pressure by organizing public debates, lobbying legislators, and expanding their membership. A coalition — Don't Spy on Us — combined this advocacy work towards a common campaign. In addition, internet companies were increasingly vocal in their criticism of large-scale data collection. Concerned about the implications of the Snowden revelations for user trust in their services, they focused more attention on data security and user privacy and advocated for policy reform. This introduced tensions into the relationship between governments and the corporate sector and weakened, to some extent, the powerful collusion between government and internet business (Wizner, 2017). These tensions in turn were reflected in strong pressure by British politicians and security agencies on companies to comply with data requests by the state. GCHQ Director Robert Hannigan called social media networks 'terrorists' command and control networks of choice' (Hannigan, 2014) and then-Prime Minister David Cameron demanded that they 'do more to co-operate with the intelligence agencies' (The Guardian, 2015, January 16). Both the British Prime Minister and the Home Secretary have called for limits to encryption and for legal backdoors to enable data monitoring by security agencies (Temperton, 2015).

Internet companies were increasingly vocal in their criticism of large-scale data collection. Concerned about the implications of the Snowden revelations for user trust in their services, they focused more attention on data security and user privacy and advocated for policy reform

All these pressures and activities led to a dynamic phase of policy reform at a time when the aftermath of the Snowden revelations coincided with the rise of platforms. While the former led to a review of data collection and analysis by state agencies, the latter required updates to data protection regulation. In the UK, the review of state powers culminated in comprehensive new draft legislation, presented in October 2015, to combine the fragmented legislative framework of data collection and analysis under one law. The Investigatory Powers Bill (IP Bill) was discussed for one year and was adopted by Parliament (and thus became the Investigatory Powers Act) in November 2016. Addressing a wide range of surveillance practices – from bulk data collection to 'computer network exploitation' (i.e., hacking) – it opened up many of the traditionally secret surveillance measures to public scrutiny and oversight. However, rather than limit state surveillance powers in light of the Snowden leaks, it confirmed, legalized, and even expanded existing practices. It has allowed the bulk interception of data that is generated, not least, on internet platforms; required the collection of 'internet connection records' (i.e., people's web browsing habits) and enabled a wide range of state authorities to view these without judicial approval; and allowed security agencies to hack into people's computers and mobile phones (Hintz & Brown, 2017).

The IP Act was complemented the following year by the Digital Economy (DE) Act, which updates regulations on electronic communications infrastructure and services, as well as criminal justice issues such as copyright infringement. Key provisions of the Act include: the facilitation of data sharing between government departments, the requirement for websites that provide adult content to create age verification mechanisms, which are to be

overseen by an age-verification regulator, the requirement for internet service providers to block websites with adult content unless customers opt in to receiving this content, and an increase in the maximum sentence for internet copyright infringement. Data collection is affected, particularly, by the provisions for age verification -- which have led to concerns about the privacy implications of collecting user data -- and by the facilitation of bulk data sharing (Open Rights Group, 2016a).

Citizens' data rights are highlighted more explicitly in the government's "Digital Charter", which includes the provision that "personal data should be respected and used appropriately" (https://www.gov.uk/government/publications/digital-charter/digital-charter). Concerns regarding the collection and analysis of personal data also underpins plans for a new "Centre for Data Ethics and Innovation". Yet, such considerations have, so far, mainly led to normative frameworks.

Meanwhile at the EU level, policymakers have developed more restrictive frameworks to regulate data collection and use by commercial platforms, as part of a broader overhaul of European data protection rules. The General Data Protection Regulation (GDPR) in the European Union, which was adopted in 2016 and which came into effect on May 25, 2018, served as a milestone, as it expanded the protection of citizens' personal data, particularly with regard to internet platforms and cloud computing. More than previous data policies, it situates the data subject at the center of regulation (Floridi, 2017). It limits the use and sharing of personal data by companies inside the EU as well as the export of data outside the EU and it extends the scope of the EU data protection law to foreign companies processing data of EU residents. The regulation seeks to make new forms of automated and algorithmic decision-making more transparent; assigns citizens a right to explanation and to challenge outcomes of algorithmic decisions; requires impact assessments for potentially harmful data uses; and mandates data protection by design. Many elements of the GDPR have been controversial (see below, e.g., Edwards & Veale, 2017; Wachter, et al., 2017) but as a comprehensive regulatory framework, it fills some of the gaps in the regulation of the data economy and offers new directions for providing citizens with some control over their personal data.

3. Mapping the Implications of Policy Reform

The three new laws and regulations affect platforms in a variety of ways. In this section, we map several issues that have arisen and that will be explored in greater depth on further research.

3.1 Data Portability

The GDPR requires platforms to allow users to move their data across services, which may challenge the monopoly power of large platforms. As the Article 29 Working Party states, the 'primary aim of data portability is to facilitate switching from one service provider to another, thus enhancing competition between services (by making it easier for individuals to switch between different providers)' (A29WP, 2016). However, academic opinion is divided on this matter, with many observers disputing its efficacy (Zolynski, 2017). Proponents point to the ability to counter vendor lock-in, which is particularly prevalent among social networking sites. Graef et al (2013, p. 6) explain, 'For providers that rely heavily on data provided by users, restricting data portability is a way to tie users to their services.' Vanberg & Unver (2017, p. 6) note, 'This type of consumer lock-in could be seen as creating a more fragile marketplace, as it is open to exclusionary acts of dominant players.' As personal data must be received 'in a structured, commonly used and machine-readable format' and data subjects must be able to transmit them to another service, data portability can enhance interoperability between platforms. This would encourage platforms to cooperate and may weaken monopoly power (also see de Hert et al., 2017).

Critics of data portability claim that the scope of portability is too limited to have any real impact on platform power; partly because inferred and derived data is not included in the regulation. Particularly intrusive data activities, such as profiling, often utilize inferences from observed data such as Facebook clicks and likes. However, inferences of a system do not belong to the data subject but to the system that generate it (Edwards & Veale, 2017, p. 67).

3.2 Consent

While continuing to rely on the controversial construct of user consent for data collection and analysis, the GDPR expands and refines the notion by defining consent as an ongoing and actively-managed choice, rather than a one-off compliance box to tick. It requires consent to be actively obtained and gives users the option to withdraw at any moment. This is likely to cause at least some disruption to the business model of platforms where consent is the legal basis for data processing. It is necessary, though, to differentiate between those platforms that have a direct relationship with the data subject (e.g., Facebook and Google) and those that do not (e.g., data brokers like Acxiom and the adtech industry).

The GDPR expands and refines the notion by defining consent as an ongoing and actively-managed choice, rather than a one-off compliance box to tick

The tightening of consent rules by GDPR makes it more difficult for platforms that have a direct relationship with users to use the personal data they hold for advertising purposes without user permission. While they can process personal data necessary to provide services that their users request, using this data for any other purpose requires user permission. In practice, this means that users will have to opt-in to tracking (Ryan, 2017). Further, the application of the GDPR should mean that users will be aware of the uses of their data when consent is sought. The principle of purpose limitation – Article 5 (1) – means that personal data must only be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.' Third party data processing will therefore face disruption, which could have an impact on big platforms. Users will have to consent to the sharing of their data by the platform with any third party.

As a way out, platforms could pursue 'legitimate interests' as a legal ground for processing data. Recital 47 of the GDPR states: '[t]he processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.' However, the Article 29 Working Party recently indicated that this will not be possible without adequate user controls and proper safeguards.

Explicit consent is even harder to obtain for platforms with no direct relationship with the data subject, such as companies working in online behavioral advertising that track users across the net. As well as incorporating purpose limitation, consent must also be granular and must be sought for each specific purpose. This may mean that each data broker or adtech vendor will be required to obtain consent for each profile that is bought and sold. Some commentators in the adtech sector are predicting that the GDPR will severely weaken the third party data market, while others are calling for advertisers to stop relying on personal data and instead monetize 'non-personal data' (Ryan, 2018). Indeed, an unnamed big tech executive has claimed that 'personal data is quickly becoming a toxic asset' and that 'surreptitiously gathered personal data [is] the radon gas of business and a silent killer' (quoted in Rainie & Anderson, 2017). Third party data processors may have to rely on first party platforms (like Google and Facebook) for consent. Yet, the details of consent and legitimate interests for data brokers remain uncertain.

3.3 Processing of Sensitive Data

While the legal obligation to obtain explicit consent has the potential to disrupt aspects of platform business, the GDPR's rules against the processing of sensitive personal data -- laid out in Article 9 -- could add to this disruption by limiting the ability to profile data subjects. Article 9 states that 'Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or

data concerning a natural person's sex life or sexual orientation shall be prohibited.' Data brokers collect and trade this kind of sensitive personal data to partners like credit scoring and insurance companies and rely on it to select relevant ads for users, personalize services and products, and understand how categories of people browse the web. As the Spanish court in a case against Facebook noted in September 2017, '[Facebook] data on ideology, sex, religious beliefs, personal preferences or browsing activity are collected directly, through interaction with their services or from third party pages without clearly informing the user about how and for what purpose will use those data' (Cabanas et al, 2018, p. 4).

3.4 Definitions

Platforms are not defined consistently across different laws and regulations, or even within a policy framework. The IP Act, particularly, is underpinned by a number of inconsistent, broad and vague definitions. Platforms could fall under several definitions in the Act, depending on which particular surveillance power is evoked or, more problematically, depending on interpretation. These include: telecommunication operator, telecommunications service, communication service provider, internet service, and internet communications service. The Act significantly expands the category of organizations known as 'communication service providers' (CSPs) to include some platforms that are also Over the Top Communication Services like Facebook and Whatsapp. An 'internet service' here includes 'internet communication services, websites and applications', such as online travel booking or mapping services (Smith, 2015). 'Telecommunications operator' may include not only telcos, ISPs, etc., but also web e-mail, social media platforms, cloud hosts and Over the Top Communications providers (Smith, 2017).

Platforms are not defined consistently across different laws and regulations, or even within a policy framework

The Act, moreover, introduces 21 different types of data which platforms may need to be informed about: communications data, relevant communications data, entity data, events data, internet connection record, postal data, private information, secondary data, systems data, related systems data, equipment data, overseas-related equipment data, identifying data, target data, authorization data, protected data, personal data, sensitive personal data, targeted data, content, and data. 'Relevant communications data', for example, may cover any type of communication on a network and internet connection. It includes communications without human intervention, where the sender and recipient are machines, such as background interactions that apps make automatically with their supplier servers. It goes beyond the data processed by a company in its normal course of business to create an additional obligation on providers to generate new types of data specifically for law enforcement purposes (techUK, 2015). Legal and academic communities as well as the tech industry have all pointed to a need for more clarity on definitions.

3.5 Extraterritorial Jurisdiction

The tendency of current legislation is to expand its jurisdiction. The GDPR applies not just to European citizens but to all citizens whose data is processed in the EU, and it covers data sharing arrangements with organizations outside the EU. The IP Act, similarly, has extra-territorial reach. The majority of powers that it covers (e.g., lawful interception, acquisition of communications data, equipment interference) assert UK jurisdiction overseas and thereby are in potential conflict with the laws of other countries. Platforms with a global reach have opposed this aspect of the Act as it means that overseas communication service providers will be affected by the legislation and legally obliged to hand over data to the UK, regardless of the legal framework of that country. Companies may be required to hand over data in one country and thereby directly contravene their legal obligations in another country. The view from industry, as stated by Apple, is that extraterritoriality 'will lead to major issues for businesses and could ultimately put UK users at greater risk' (Apple Inc., 2015). According to Liberty, a civil society

organization, 'an increasingly chaotic international legal system will leave companies in the impossible position of deciding whose laws to violate' (Liberty, 2015).

3.6 Mandatory Communications Data Retention

Despite the decision to revoke data retention rules that was confirmed by the UK Court of Appeal in 2018 (see above), mandatory retention of communications data remains part of the IP Act and its future is uncertain. The outcome of these legal battles will affect platforms significantly as data retention rules mandate the generation and collection of relevant communications data by 'telecommunications operators' for up to 12 months. As with Internet Connection Records (ICRs, see section below) this may well require platforms to produce data outside of their current business practices. Most civil society and tech organizations oppose mandatory data retention on the grounds that it is excessive and violates the right to privacy. The tech sector in particular has expressed concern that the IP Act's data retention and ICR provisions (see below) will significantly affect their business models. Whether and how exactly this will affect platforms is ambiguous due to the vague wording and broad and overlapping definitions in the Act.

3.7 Internet Connection Records

The IP Act introduces the requirement for internet service providers to capture Internet Connection Records (ICRs). Similar to the data retention rules, these affect platforms by forcing them to produce large volumes of new datasets and by imposing costs in the process. ICRs are an artificial construct with no concrete definition in the Act, and they are not a term recognized by the computing industry. It remains unclear whether ICRs can be matched to real categories of data processed by internet companies. As the ISPA says, 'ICRs are not currently retained or held by service providers for business purposes' and they lack 'a clear definition making it difficult to assess what data could fall under the definition and what impact the collection of this data may have on businesses and consumers.'

3.8 Age Verification: Platforms as Enforcers

The age verification rules of the DE Act, as noted above, require platforms to enforce age verification both on their own sites and on other third parties – known as ancillary service providers – to block infringing sites. The Electronic Frontier Foundation stated that 'the possible impact of the law extends beyond video hosting websites, but also extends to payment services providers, hosting providers, and advertisers on those websites, whether they are based in the United Kingdom or overseas' (Malcolm, 2016). Further, websites will be compelled to create databases of users' viewing habits along with their personal data – including credit card details – to be handed over to get past the verification (Open Rights Group, 2016b). It appears, therefore, that platforms will be affected by the DE Act by being forced into monitoring and censoring their users and content.

3.9 Data Sharing

As noted above, the DE Act also expands rules for data sharing between government departments and therefore contravenes the efforts made in the GDPR to limit the widespread distribution of data gathered through platforms. While the use of data by the government and commercial actors is regulated separately, the increasing use of commercial data aggregation tools (such as Mosaic) by the public sector blurs this line and points to a potential conflict between different legislation.

4. Conclusion

The rise of platforms and the extent of their data activities has generated an urgent need for a policy environment that addresses consumer protection, civic rights, innovation and security. However, reconciling these interests has been difficult, and recently developed legislation is contradictory regarding its rules and goals. While the IP Act and, to some extent, the DE Act mandate extensive data collection and sharing, the GDPR seeks to reduce these and

increase citizen control over their data. Platforms may face difficulty in complying with both sets of rules. For example, the data retention powers outlined in the IP Act contain secrecy provisions, or 'gag orders', that oblige ISPs and service providers to refrain from informing users about surveillance, which contradicts informed consent set out by the GDPR. There is also tension between data retention and ICRs on one hand, and the GDPR's principle of purpose limitation, laid out in Article 5, on the other. Platforms are facing equal uncertainty due to the tension between the DEA and the GDPR, with each law pulling data sharing in different directions.

The specific legal provisions are underpinned by contradictory underlying norms. While the GDPR is both informed and motivated by the need for updating and expanding consumer protection and citizen rights, the IP Act is strongly based on the interests of the security sector and the Home Office (the government department dealing with domestic security). Contributions to the development process of the IP law from civil society and industry were, hence, largely ignored (Hintz & Brown, 2017). Platforms thus have to respond to conflicting norms, and operate, as noted above, on the basis of unclear definitions and jurisdictions. Citizens' control over their data is an emerging principle that is recognized in documents such as the UK Digital Charter and advanced through the GDPR, but its specific implementation remains contradictory and limited. Even though provisions on data portability and user consent, for instance, have been strengthened, data collection and analysis, especially by public institutions, continues to expand.

Data-based forms of exclusion and discrimination are addressed by GDPR as it limits profiling and, particularly, the use of sensitive data. However, the practical application of GDPR will have to demonstrate how robust this framework is and what exemptions will be implemented. Many academic observers and digital rights groups believe that GDPR offers a starting-point for a citizen-oriented regulatory framework but that further thinking on data protection rules and concepts is necessary. The policy reform efforts mentioned here demonstrate the challenges of regulating the platform society and underline how new norms and approaches are required to address them.

References

A29WP. (2016). *Guidelines on the right to data portability. Adopted 13 December 2016*. Retrieved from: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Anderson, D.Q.C. (2015). A question of trust – Report of the Investigatory Powers Review. *Independent Reviewer of Terrorism Legislation*. Retrieved from: https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

Andrejevic, M. (2012). Exploitation in the data mine. In C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval (Eds.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. pp. 71–88. Abingdon: Routledge,

Apple Inc. (2015). Written Evidence (IPB0093). Retrieved from: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26341.pdf

Belli, L. & Zingales, N. (2017). *Platform Regulations*. Rio de Janeiro: FGV Direito Rio.

Cabanas, J.G., Cuevas, A., and Cuevas, R. (2018) *Facebook Use of Sensitive Data for Advertising in Europe*. Retrieved from: https://arxiv.org/abs/1802.05030

Council of Europe. (1950). *European Convention of Human Rights*. Retrieved from: https://www.echr.coe.int/Documents/Convention_ENG.pdf

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2017). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review* 34 (2), 193-203. Retrieved from: https://www.sciencedirect.com/science/article/pii/S0267364917303333#!

Edwards, L. & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke Law and Technology Review*, 16(1), 18–84.

Floridi, L. (2017). *The Fourth Revolution: How the infosphere is reshaping human reality*. Hay Festival, 30 May.

Graef, I., Valcke, P., & Verschakelen, J. (2013). Putting the right to data portability into a competition law perspective. *Law: The Journal of the Higher School of Economics*, Annual Review.

Greenfield, P. (2018). The Cambridge Analytica Files. *The Guardian.* Retrieved from: https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-_far

Watt, N. & Wintour, P. (2015, January 16). Facebook and Twitter have social responsibility to help fight terrorism, says Cameron. *The Guardian.* Retrieved from: http://www.theguardian.com/world/2015/jan/16/cameron-interrupt-terrorists-cybersecurity-cyberattack-threat

Hannigan, R. (2014, November 3). The Web is a terrorist's command-and-control network of choice. *Financial Times*. Retrieved from: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3TywRsOQ2

Hintz, A. & Brown, I. (2017). Enabling digital citizenship? The reshaping of surveillance policy after Snowden. *International Journal of Communication*, 11, 782–801.

Human Rights Council. (2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. Retrieved from: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx

Liberty. (2015). Written Evidence (IPB0143). Retrieved from: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26430.pdf

Lyon, D. (2015). *Surveillance after Snowden*. Cambridge: Polity.

Malcolm, J. New Censorship and Copyright Restrictions in UK Digital Economy Bill. *Electronic Frontier Foundation*, 2016, July 8. Retrieved from: https://www.eff.org/deeplinks/2016/07/new-censorship-and-copyright-restrictions-uk-digital-economy-bill

Open Rights Group (2016a). *Digital Economy Bill: Briefing to the House of Commons on Second Reading*. Retrieved from: https://www.openrightsgroup.org/ourwork/reports/digital-economy-bill-briefing-to-the-house-of-commons-on-second-reading

Open Rights Group (2016b). *A database of the UK's porn habits. What could possibly go wrong?* Retrieved from: https://www.openrightsgroup.org/blog/2016/a-database-of-the-uks-porn-habits-what-could-possibly-go-wrong

Rainie, L., & Anderson, J. (2017). The Fate of Online Trust in the Next Decade. *Pew Research Center*, August 10, 2017. Retrieved from: http://www.pewinternet.org/2017/08/10/the-fate-of-online-trust-in-the-next-decade/

RUSI. (2015). *A democratic licence to operate: Report of the Independent Surveillance Review*. Retrieved from: https://rusi.org/publication/whitehall-reports/democratic-licence-operate-report-independent-surveillance-review

Ryan, J. (2017). How the GDPR will disrupt Google and Facebook. *Pagefair,* August 30, 2017. Retrieved from: https://pagefair.com/blog/2017/gdpr_risk_to_the_duopoly/

Ryan, J. (2018). GDPR consent design: How granular must adtech opt-ins be? *Pagefair,* January 8, 2018. Retrieved from: https://pagefair.com/blog/2018/granular-gdpr-consent/

Smith, G. Never mind Internet Connection Records, what about Relevant Communications Data? *Cyberleagle*, 2015, November 29. Retrieved from: https://www.cyberleagle.com/search q=+internet+communication+records

Smith, G. Back doors, black boxes, and #IP Act technical capability regulations, *Cyberleagle.* 2017, May 8. Retrieved from: https://www.cyberleagle.com/2017/05/back-doors-black-boxes-and-ipact.html

Srnicek, N. (2016). *Platform Capitalism*. Cambridge: Polity.

techUK (2015). *Written Evidence* (IPB0088). Retrieved from: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26336.pdf

Temperton, J. No u-turn: David Cameron still wants to break encryption. *Wired*, 2015, July 15. Retrieved from: http://www.wired.co.uk/article/cameron-ban-encryption-u-turn

UN General Assembly. (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression*, Frank La Rue. Retrieved from: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Van Dijck, J. (2016). *The platform society*. Keynote at Association of Internet Researchers Conference, Berlin.

Vanberg, A.D., & Unver, M.B. (2017) The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? *European Journal of Law and Technology*, 8(1).

Wachter, S., Mittelstadt, B. & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99.

Wizner, B. (2017). What changed after Snowden? A US perspective. *International Journal of Communication*, 11, 897–901.

Zolynski, C. (2017). 'What legal framework for data ownership and access?' In Belli, L. and Zingales, N., eds., *Platform regulations: how platforms are regulated and how they regulate us*. Rio de Janeiro: FGV Direito Rio.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30, 75–89.