PRIVACY INTERNATIONAL

The Right to Privacy (Article 8) and the Digital Revolution: Data collection by private companies: a threat to human rights?

Privacy International's response
to the UK Parliament
Joint Committee on Human Rights

28 March 2019

1. About Privacy International

1.1. Privacy International (PI) is a leading charity advocating for strong national, regional, and international laws that protect the right to privacy around the world. Founded in 1990 and based in London, PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

1.2. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

1.3. PI employs technologists, investigators, policy experts, and lawyers, who work together to understand the technical underpinnings of emerging technology and to consider how existing legal definitions and frameworks map onto such technology.

1.4. PI is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Parliament of the United Kingdom, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

Contact: Ailidh Callander, Legal Officer - ailidh@privacyinternational.org

2. Executive Summary

2.1. Privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. For people to fully participate in democratic society, developments in law and technologies must strengthen and not undermine peoples' ability to freely enjoy these rights.

2.2. The collection, generation, use, and storage of personal data by private companies threaten peoples' right to private and family life (Article 8 European Convention of Human Rights ("ECHR")), as well as freedom of expression (Article 10 ECHR), freedom of association (Article 11 ECHR), and non-discrimination (Article 14 ECHR). These rights are incorporated into domestic UK law through the Human Rights Act 1998. The EU Charter of Fundamental Rights also enshrines many relevant rights, including the right to privacy and the right to the protection of personal data, in Articles 7 and 8 respectively. As more data are collected and generated every day in every aspect of our lives, it is important to consider the implications of the use by private companies of this data not just for civil and political rights but also social, economic and cultural rights.

2.3. To protect privacy and the other human rights it supports, it is essential to regulate the collection, generation, use, retention and disclosure of personal data by private companies through the human rights framework as well as other legal frameworks such as data protection and competition law. Privacy International therefore very much welcomes this timely and important inquiry by the Joint Committee of Human Rights.

2.4. This submission primarily focusses on two of the questions posed as part of the Inquiry, which is in itself wide in scope. Privacy International would welcome the opportunity to engage further with the Committee as it proceeds.

3. "Some uses of content and metadata by private companies is so intrusive that states would be failing in their duty to protect human rights if they did not intervene?"

3.1. The Committee poses the above question. When talking about data it is important to note that there are different ways of classifying and distinguishing, between types of data and different framings may be used in different contexts. As well as content and metadata[1], we also talk about the data that can be derived, inferred and predicted. All of this data can be highly intrusive and reveal a huge amount about an individual. All of this data can also be personal data, which is entitled to specific protections under human rights and data protection law. Even more so when it is sensitive personal data (or special category personal data).

[1] *Video: What is metadata?*, Privacy International https://privacyinternational.org/video/1621/video-what-metadata.

3.2. Private companies are generating, collecting, and using people's data in ways that are so intrusive that these uses violate peoples' human rights, including the right to private and family life (Article 8 ECHR). The collection, generation and use of this data risks interfering with the whole spectrum of civil and political as well as economic, social and cultural rights.

3.3. The United Nations High Commissioner for Human Rights has affirmed that states are obligated to exercise regulatory jurisdiction over private companies to ensure that human rights protections extend to people whose privacy is impacted by the companies generating, collecting, and using their personal data.[2] States are further obligated to "mitigate the impact on human rights from . . . power and information asymmetries" that exist between people and private companies in the use of peoples' personal data.[3]

3.4. Data companies, including platforms, data brokers, advertisers, marketers, web trackers, and more, facilitate a highly intrusive hidden data ecosystem that collects, generates and supplies peoples' data to other advertisers, social media sites, credit agencies, insurers, law enforcement, and more, who then use that data to profile people, without their full knowledge or consent.[4]

3.5. Companies are relying less on data people provide and more on data that companies can automatically observe, as well as the insights that they can derive, and infer from large amounts of data.[5] Companies collect data from peoples' behavior, which is transmitted directly and automatically from devices, frequently without peoples' knowledge or awareness. This happens online -- for instance through tracking technologies on platforms, websites and apps[6] -- and in offline spaces -- including through sensors like microphones, and cameras and other sensors that are embedded in connected devices.

3.6. Companies routinely derive data from other data, such as determining how often someone calls their mother to calculate their credit-worthiness.[7] As a result,

---

[2] United Nations Human Rights Council, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, 3 August 2018, A/HRC/39/29, *available* from https://undocs.org/A/HRC/39/29 (accessed March 27, 2019)

[3] *Id.* at 8.

[4] *How do companies get our data?*, Privacy International https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data.

[5] *A world of data exploitation*, Privacy International https://privacyinternational.org/recommendation-principle-or-safeguard/world-data-exploitation.

[6] *Guess what? Facebook still tracks you on Android even if you don't have a Facebook account*, Privacy International (March 27, 2019), https://privacyinternational.org/blog/2758/guess-what-facebook-still-tracks-you-android-apps-even-if-you-dont-have-facebook-account (PI investigation revealed that some of most widely used Google Play store apps sent personal data to Facebook as soon as the apps were launched, before people can decide whether they want to consent or not).

[7] *Fintech: Privacy and Identity in the New Data-Intensive Financial Sector,* Privacy International https://privacyinternational.org/report/998/fintech-privacy-and-identity-new-data-intensive-financial-sector

potentially sensitive data can be inferred from seemingly mundane data, such as future health risks.[8] Combined data can reveal peoples' political and religious views; socioeconomic status; finances; spending habits; physical and mental health; relationships status; sexual preferences; family planning; internet browsing activities; and more. Combining data may expose patterns of behaviour people themselves are not aware of and highly sensitive information that they did not knowingly provide.

3.7. Often, there is more data being collected and shared than is necessary for companies to provide a service, to ensure the functionality of a device, or accomplish a clearly stated business purpose.

3.8. Private companies can search, cross-reference, and mine the datasets constructed from other data to map, understand, and predict peoples' behaviour and relationships with others.[9] The companies can use these datasets to derive, infer and predict even more granular insights, all of which is data that can be shared as well, or used to target people with particular appeals, messages or advertisements. Political parties and other campaign groups can use these same techniques to micro-target voters.[10] These practices risk undermining peoples' agency and autonomy.

3.9. Targeted advertising risks excluding or discriminating against minority groups.[11] It can be based on conclusions drawn about large groups of people, where some groups are excluded because their data is not included in the sets, or the quality of their data is poorer. Targeted advertising can also be based on aberrant data amongst larger sets, leading to the use of big data to discriminate against specific groups and activities. Targeting advertisements may be used to seek to bypass anti-discrimination laws[12] and special protections afforded under data protection legislation by using micro-targeting to circumnavigate being explicit about race, ethnicity, gender, disability, familial status, religion, or other factors in ways that

[8] *A snapshot of Corporate Profiling* https://privacyinternational.org/feature/1721/snapshot-corporate-profiling

[9] *Video: What is big data?* Privacy International https://privacyinternational.org/explainer/1310/big-data.

[10] *See, e.g.,* Information Commissioner's Office, *Democracy Disrupted? Personal Information and Political Influence* (July 2018), available from https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf (raising concerns about ways political parties and campaign groups are using personal information and data analytic techniques to target voters, and how such techniques can undermine the integrity of elections).(Accessed March 27, 2019).

[11] *See, e.g.,* Privacy International, Thematic Consultation Submission: Comments to the Article 29 Working Party Guidelines on Automated Decision Making and Profiling 4 (November 2017), https://privacyinternational.org/sites/default/files/2017-12/Privacy International - submission on profiling guidance.pdf (explanation of ways targeted online advertising can inherently exclude and discriminate against individuals) and Case Study: Invisible Discrimination and Poverty https://privacyinternational.org/case-studies/737/case-study-invisible-discrimination-and-poverty

[12] *See, e.g., Online personalisation enables invisible - and illegal - discrimination,* (https://privacyinternational.org/examples/868/online-personalisation-enables-invisible-and-illegal-discrimination (Summary of reporting and litigation in the US by the ACLUS and others regarding the use of proxies for race to bypass anti-discrimination laws regarding housing and employment).

are prohibited. As a result of action by civil society, companies are beginning to make changes to their practices[13] but do they go far enough? The links between the use of data by private companies and discrimination merit consideration by the Committee.

3.10. Private companies can use the outputs they generate to make judgements about people that will disadvantage some relative to others and impact on their enjoyment of human rights. For example, credit agencies can lower credit ratings, insurance companies can raise premiums, financial companies can charge higher interest rates and employers can skip over job applications. These are data exploitation practices that do not need to be inevitable.[14]

3.11. Private companies, such as data brokers, may sell the data they exploit to other companies, advertisers, public authorities, and political parties, to profile people ever more precisely.[15] As a result, companies and groups people have never even heard of can have access to vast streams of information about them. For example, in 2017, data broker company Acxiom claimed to have data "on approximately 700 million consumers worldwide, and [Acxiom's] data products contain over 5,000 data elements from hundreds of sources."[16] Privacy International filed complaints with the UK, Irish and French data protection authorities to highlight how data practices by data brokers, credit references and ad tech companies fall below data protection standards.[17] These also should also be considered under the human rights lense.

3.12. The exploitable nature of peoples' datasets and the risks entailed are illustrated in the report by Privacy International and the International Committee of the Red Cross, which examined how the increasing reliance on digital and mobile technologies could have detrimental effects for people receiving humanitarian aid.[18]

---

[13] Doing more to protect against discrimination in housing, employment and credit advertising, Facebook Newsroom March 19, 2019 https://newsroom.fb.com/news/2019/03/protecting-against-discrimination-in-ads/ (accessed March 27, 2019)

[14] *Video: What is Data Exploitation?,* Privacy International https://privacyinternational.org/video/1626/video-what-data-exploitation.

[15] *Tell companies to stop exploiting your data!,* Privacy International https://privacyinternational.org/campaigns/tell-companies-stop-exploiting-your-data.

[16] *2017 Annual Report,* Acxiom (accessed March 27, 2019), https://s22.q4cdn.com/928934522/files/doc_financials/annual_reports/Annual-Report-2017-(Web-ready).pdf.

[17] *Privacy International complaints against Acxiom, Oracle, Equifax, Experian, Criteo, Tapad and Quantcast* (November 2018) https://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad

[18] *Practices of humanitarian sector are leaving aid recipients at risk, PI and ICRC find,* Privacy International https://privacyinternational.org/press-release/2510/practices-humanitarian-sector-are-leaving-aid-recipients-risk-pi-and-icrc-find.

3.13. Because the generation, collection, and use of data by private companies allows them to conduct surveillance on entire societies with a lack of transparency and accountability, such practices risk violating not just peoples' right to private and family life, but other rights too.

3.14. These technologies intrude into what should be private spaces, where people should be able to exercise their rights to private and family life, express themselves, and associate with others without fear of discrimination and without fear of being watched. When people fear how their data is being used and abused by private companies, they may self-censor their words, thoughts, and actions, which limits their ability to seek out new information, formulate ideas, express dissent, and organise to effect social change.

3.15. Increasingly, technologies developed and controlled by private companies are also relied upon by the public sector, including in healthcare, education, welfare, law enforcement and border control: these private-public arrangements raise further questions about whether the collection, generation, use, tracking, retention and disclosure of personal data by private companies allows states to obtain data they would otherwise be prohibited from obtaining and thereby circumnavigate legal constraints and oversight mechanisms that would otherwise apply.[19] Furthermore, people may not be aware of and would not consent to private companies sharing their personal information with state actors and vice versa. The responsibility of the state should also be considered in relation to the manufacture, sale, import and export of surveillance technologies. [20]

3.16. States have a positive obligation to ensure the enjoyment of human rights. First, as increasingly technologies developed and controlled by private companies are also relied upon by the public sector (as noted above) "facilitating" the execution of state obligations, states are directly implicated. Second, the obligation of states to protect human rights, includes the obligation to protect them from actions of private actors that impede the enjoyment of human rights. Finally, the UN Guiding Principles on Business and Human Rights (2011) recognised that private companies also play independent roles in either advancing or restricting human rights. Their specific obligations need to be further elaborated to ensure their enforcement. More must be done to translate these guiding principles into the lived realities people experience.

3.17. Companies should, by default and design, protect privacy and other human rights that privacy supports. People must have full access to appropriate judicial and non-judicial remedies in order to effectively protect their human rights.

---

[19] Statement on Visit to the United Kingdom, by Professor Philip Alston, United Nations Special Rapporteur on extreme poverty and human rights, London, 16 November 2018, https://www.ohchr.org/Documents/Issues/Poverty/EOM_GB_16Nov2018.pdf. (Accessed March 27, 2019)

[20] https://privacyinternational.org/blog/820/open-ngo-letter-eu-member-states-and-institutions-regarding-export-surveillance-equipment.

3.18. Therefore, it is timely for the Committee to examine how the data practices of private companies interfere individuals' human rights.

4. "Are consumers and individuals aware of how their data is being used, and do they have sufficient real choice to consent to this?"

4.1. The scale and nature of data collection and use means that the vast majority of people do not know or understand the unprecedented scale of detailed, encyclopaedic, personal information that private companies are generating, collecting, storing, sharing and exploiting, whether that data is accurate or up-to-date, or how people are being classified and targeted.[21]

4.2. People do not knowingly create or share the majority of the personal data generated about them. The devices people use contain sensors they cannot control, store data they cannot access, rely on operating systems they cannot monitor, and connect to services and platforms that access and share that data in environments where consent and peoples' rights can too often be rendered meaningless through the actions of companies.[22] For example, Privacy International found that some of the most popular apps on the Google Play Store automatically transfer personal data to Facebook the moment a user opens the app, before people are able to agree or consent, and this happens whether people have a Facebook account or not, or whether they are logged into Facebook or not.[23]

4.3. While this is the reality online, the Internet of Things (IoT) is slowly expanding a similar level of opaque data collection to public spaces, homes and cities. 'Smart cities,' for instance, use infrastructure and technology created and serviced by private companies, and build environments where people are no longer expected to consent to the collection and use of their data and there is no way for people to opt out.[24]

4.4. As highlighted by the UN High Commissioner for Human Rights, "[b]usiness enterprises and States continuously exchange and fuse personal data from various sources and databases, with data brokers assuming a key position. As a consequence, individuals find themselves in a position of powerlessness, as it seems

---

[21] *Video: How Companies Exploit Your Data,* Privacy International https://privacyinternational.org/video/1627/video-how-companies-exploit-your-data.

[22] *Invisible Manipulation: 10 ways our data is being used against us*, Privacy International https://privacyinternational.org/feature/1064/invisible-manipulation-10-ways-our-data-being-used-against-us.

[23] *Investigating Apps Interactions with Facebook on Android,* Privacy International https://privacyinternational.org/appdata

[24] *Case Study: Smart Cities and Our Brave New World*, Privacy International https://privacyinternational.org/case-studies/800/case-study-smart-cities-and-our-brave-new-world.

almost impossible to keep track of who holds what kind of information about them, let alone to control the many ways in which that information can be used."[25]

4.5. When data is generated without peoples' knowledge, it is impossible for people to know how their behaviour will allow inferences to be drawn or what sorts of predictions will be produce. For instance, a member of Privacy International's staff has used their data access rights to gain access to all the data that an online tracking company has collected about them. [26] The findings illustrate the challenge for people to understand why companies have classified and targeted them in specific ways, to reconstruct what data these classifications are based on, and to know when and how their data might be used against them.

4.6. Putting the burden on people to educate themselves and make informed choices about many of the ways private companies currently use their personal data is too often an impossible demand. Private companies create unduly lengthy privacy policies worded with confusing language. As a result, individuals often cannot provide meaningful, freely given, specific, informed, and unambiguous consent to, or effectively control or limit, the ways companies are using their information. For example, the average Internet user would have to spend seventy-six working days each year to simply read the privacy policies they would encounter in a given year.[27] An investigation by the BBC in June 2018 revealed that companies such as Amazon, Apple, Facebook, Google, Instagram, LinkedIn, Snapchat, Spotify, Tinder, Twitter, Whatsapp, and YouTube had privacy policies that were written at a university reading level and would be more complicated to read than Charles Dickens' *A Tale of Two Cities*.[28] Reading the privacy policies of the fifteen companies the BBC examined would take an average person almost nine hours to read.[29] Many of the companies examined by the BBC had sites and applications used by children aged thirteen.[30]

---

[25] Right to Privacy in a Digital Age, UN High Commissioner of Human Rights, August 3, 2018 A/HRC/39/29, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement (accessed March 27, 2019)

[26] *I asked an online tracking company for all my data and here's what I found,* Privacy International (March 27, 2019), https://privacyinternational.org/feature/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found.

[27] Keith Wagstaff, *You'd Need 76 Work Days to Read All Your Privacy Policies Each Year,* Time (March 27, 2019), http://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year/ (note that this story was published in 2012, and today the amount of time required would likely be much greater).

[28] Tom Calver and Joe Miller, *Social site terms tougher than Dickens*, BBC News (March 27, 2019), https://www.bbc.co.uk/news/business-44599968.

[29] *Id.* (The BBC also noted, "Spotify had the longest combined policies at 13,000 words, just shy of Shakespeare's shortest play *Comedy of Errors*. Their terms would take an average person 53 minutes to read without breaks.").

[30] *Id.*

4.7. Last year, a report from the Norwegian Consumer Council, last year highlighted the "dark patterns", default settings, features and techniques used by companies to nudge users towards privacy intrusive options. [31]

4.8. Privacy International has highlighted specific instances where private companies have failed to adequately inform people about how their data would be used and what the potential consequences would be, in a way that meant people could not give meaningful, informed, and specific consent to these companies. These problems are reflective of broader problems consumers and individuals face, and these problems are further compounded when companies share and sell peoples' information in ways people are not aware of or would not expect. For example, the collection of hundreds of data points about people from unknown sources by a company they have never heard of and do not have a direct relationship with, to profile them and then share these 'insights' with hundreds of other companies is not within individuals' reasonable expectations. Companies do not only collect and infer data about individuals but also others in an individuals' life, such as their partner/spouse and their children.[32]

4.9. Furthermore, because corporate power is so concentrated, people are unable to opt out of the corporate data exploitation model because no equivalent service exists.[33]

4.10. Finally, due to the lack of transparency and the often hidden complex nature of the way data is collected, generated and shared by private companies, sometimes in connection with the state, people are unable to effectively push back against corporate data exploitation or advocate for reform to ensure that laws and regulations adequately protect their rights.

4.11. For these reasons, independent scrutiny, such as that by the Committee is essential to reviewing the current state of play and considering what more should be done.

5. Conclusion

[31] Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy (27 June 2018) available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (March 27, 2019)

[32] Privacy International, *Submission to the Information Commission: Request for an Assessment Notice of Data Brokers, Acxiom & Oracle (the 'data brokers')* (November 2018), available from https://privacyinternational.org/sites/default/files/2018-11/08.11.18%20Final%20Complaint%20Acxiom%20%26%20Oracle.pdf; *See also Id.* at 15-16 and 25-27 for specific examples of privacy and consent policies that make it impossible for people to adequately understand and agree to companies' use of their data.

[33] *Competition and Data*, Privacy International (March 27, 2019), https://privacyinternational.org/topics/competition-and-data.

5.1. The issues raised in this submission are not exhaustive and meant to primarily highlight the nature of some of the problems that the Committee may wish to examine more deeply. The human rights framework should be used in tandem with other legal frameworks such as data protection and competition to reign in exploitative data practices, to boost transparency and accountability and ensure that the interference with human rights through the use of data by private companies is limited.

5.2. The human rights framework should support:

- Increasing individuals' control over their data to encourage the design of technologies that protect peoples' autonomy and privacy.
- Increasing security to result in more rights and protections for individuals and constraints applied to powerful entities.
- Creating further restraints on potential abuses arising from the vast accumulation of data.
- Further limiting how data is used to construct profiles and to make decisions about people, groups, and societies.
- Redress mechanisms for individuals, groups and civil society representing their interests.
- Joined up investigations and actions by National Human Rights Institutions together with other regulatory bodies, such as data protection and competition authorities.