LIBERTY'S WRITTEN EVIDENCE TO THE JOINT COMMITTEE ON HUMAN RIGHTS' INQUIRY ON THE RIGHT TO PRIVACY AND THE DIGITAL REVOLUTION

FEBRUARY 2019
ABOUT LIBERTY

Liberty is an independent membership organisation. We challenge injustice, defend freedom and campaign to make sure everyone in the UK is treated fairly. We are campaigners, lawyers and policy experts who work together to protect rights and hold the powerful to account.

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, inquiries and other policy fora, and undertake independent, funded research.

Liberty’s policy papers are available at libertyhumanrights.org.uk/policy.

CONTACT

HANNAH COUCHMAN
Policy and Campaigns Officer
020 7378 5255 | hannahc@libertyhumanrights.org.uk
INTRODUCTION

1. The Joint Committee on Human Rights (JCHR) has called for evidence on the threats posed to human rights by the collection, use and storage of personal data by private companies.

2. Liberty has long held the government to account over state use of data, including use by law enforcement, intelligence agencies, government departments and local authorities. Where individuals or bodies within the private sector engage in activities which give rise to human rights concerns, Liberty will put pressure on government to hold these individuals or bodies to account, and may also challenge those individuals or bodies directly.

3. Increasingly, the approaches to data collection and surveillance taken by government and private businesses merge and overlap, heightening the threat to our privacy (Article 8 of the European Convention on Human Rights, as protected in domestic law by the Human Rights Act 1998), freedom of expression (Article 10), freedom of association (Article 11) and freedom from discrimination (Article 14). This submission will address Liberty’s key concerns, focusing on:
   a. Data and online platforms
   b. Use of algorithms
   c. Use of biometric data
   d. Big data society and the web of surveillance.

DATA AND ONLINE PLATFORMS

4. The Facebook-Cambridge Analytica scandal saw the harvest of personal data from up to 87 million Facebook profiles for political purposes and without the data subject’s consent, using the data to target advertising and manipulate public opinion in one of Facebook’s biggest ever data breaches. The scandal demonstrated the shocking disregard with which our data is often treated by private companies and rightly generated significant public outrage. However, this scandal is part of a broader and alarming picture of the use of big data (extremely large data sets) and processes that collect, store and analyse data in a way that seeks to identify connections between this information and manipulate people on that basis.
5. Facebook’s business model, as with many online platforms, is predicated on advertisers being able to target customers with what seems to be a high degree of specificity. This is based not only on the data people “willingly” share with Facebook (although there remain significant questions around meaningful consent) but also the data which is inadvertently disclosed through usage of that platform, and others, including – for example – items purchased or search terms utilised.

6. It is clear that the vast numbers of people are not fully aware of how their data is being used, and do not have a meaningful level of choice to consent to this usage. Many users of social media platforms will feel trapped in the decision to either accept terms and conditions they are not comfortable with or find themselves unable to access the service which may form an integral part of their lives.

7. Research by the Norwegian Consumer Council\(^1\) shows how default settings on platforms such as Facebook, Google and Windows 10, along with the use of “dark patterns” and interface design, are used to manipulate users and encourage them towards more intrusive privacy options. The findings note the use of misleading wording, giving an “illusion of control”, hiding privacy-promoting options and presenting “take-it-or-leave-it” choices.\(^2\) These approaches ensure that the selection of privacy-friendly options is more onerous for users, in direct contravention of the principle of privacy by design and default.\(^3\)

8. These issues are replicated in other popular online platforms which are ostensibly available free of charge – be it the full range of Google services, social media platforms such as Facebook, Twitter and Instagram, and even some web clients. This problem is embedded deeply into our use of online services, presenting a significant threat to our privacy, with users kept in the dark about what data they are making available and how it will be used.

9. One of the key issues at the heart of the Cambridge Analytica scandal was the interconnectivity and use of data between apps and online platforms. Research undertaken by Privacy International illustrates the issues surrounding consent and


\(^2\) Ibid

\(^3\) The General Data Protection Regulation requires data controllers put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is known as “data protection by design and by default”, a key principle under both GDPR and the Data Protection Act 2018 (see section 57). See also section 57 of the Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/22/pdfs/ukpga_20180022_en.pdf
data sharing in this context. Their report shows that at least 61 per cent of the apps they tested automatically transferred data to Facebook the moment a user opened the app. This happens regardless of whether the user is logged into their Facebook account – and regardless of whether they even have a Facebook account. Ultimately this information allows advertisers to link data about user behaviour from different apps and web browsing into a comprehensive profile. An example outlined was the travel search and price comparison app "KAYAK", which sent detailed information about people’s flight searches to Facebook, including: departure city, departure airport, departure date, arrival city, arrival airport, arrival date, number of tickets (including number of children) and class of tickets. App developers share data with Facebook through the Facebook Software Development Kit (SDK), a set of software development tools. SDK’s default configuration is designed to automatically transmit data, so it is likely that some apps simply use the default. However, there were other issues identified by Privacy International around the use of a voluntary feature released in June 2018. This feature should have allowed developers to delay collecting automatically logged data until they acquired user consent, but didn’t work properly on older versions of the SDK.

10. Even more alarming is the fact that Facebook’s “Cookies Policy” describes two ways in which people who do not have a Facebook account can control the way Facebook uses cookies to show them ads. However, Privacy International tested both opt-outs and found that they had no discernible impact on the data sharing outlined in their report.7

11. That private companies exploit our data for commercial purposes is now a normalised part of our everyday existence. The data collected can reveal and manipulate our deepest and most sensitive thoughts and feelings – including our political views. This has far-reaching implications for democracy. It can also indicate our psychological wellness – for example, Facebook uses artificial

---

5 Ibid
6 Ibid
7 Ibid
intelligence to identify users they believe are at risk of suicide⁸, but has previously used data to manipulate users’ emotions and change their mood.⁹

12. The normalisation of these processes also threatens our freedom of expression and association by making it clear that we are being watched. Studies have shown that we are likely to censor what we post on social media or what we look up online when we are aware they are being surveilled.¹⁰

**USE OF ALGORITHMS**

13. Liberty notes the JCHR’s observation that algorithms can be discriminatory, and agrees that this is an area of enormous concern. Like any data collected in today’s social context, the data used to drive algorithms will be reflective of pre-existing patterns of discrimination. Filtering this decision-making process through complex software that few people understand lends unwarranted legitimacy to biased decision-making. The use of algorithms to make decisions in the private sector could lead to discrimination in areas such as hiring and employment, access to services and finance, differential pricing and more.

14. Even where sensitive data categories such as race are prohibited as a category of profiling data (in accordance with the General Data Protection Regulation¹¹), combinations of other categories of data can serve as a “proxy” for this information. For example, “if a certain geographic region has a high number of low income or minority residents, an algorithm that employs geographic data to determine loan eligibility is likely to produce results that are, in effect, informed by race and income.”¹² Liberty is concerned that the increasing use of algorithms in the private sector to make eligibility decisions, such as access to credit, may risk increasingly discriminatory outcomes.

---


⁹ Ensor (2014), How Facebook was able to manipulate your emotions, The Telegraph, 1 July, Available at: https://www.telegraph.co.uk/technology/facebook/10937214/How-Facebook-was-able-to-manipulate-your-emotions.html


¹¹ See Article 9(2)

¹² Goodman et al (2016), European Union regulations on algorithmic decision-making and a “right to explanation”, Available at: https://ora.ox.ac.uk/objects/uuid:59359ee-0457-4051-8357-e007064cf67c
15. Liberty is also concerned about the way algorithms can be used to customise pricing. It is vital that equality rights and data protection law are carefully observed, particularly by online retailers. The Government should prevent retailers from discriminating against consumers, and instead encourage transparency around their use of data and algorithms in order to monitor and challenge such discriminatory effects.

16. Liberty also notes that the increasing use of algorithms in decision-making may pressurise people into sacrificing their privacy in order to access goods or services. Sceptical or indifferent attitudes towards the right to privacy will be exacerbated as these processes are normalised and people are led to believe that they are simply a necessary step in securing this access.

**USE OF BIOMETRIC DATA**

17. The use of biometric data by private companies presents unique concerns. Biometric data is even more sensitive than other important – but ultimately alterable – information like credit card numbers. Despite this, biometric data is regularly being gathered without any public information being made available as to how it is used and how it will be kept safe. The opacity of the use of this data only serves to compound the threat to our rights. For example, a 2015 survey of 150 retail executives by the IT services firm Computer Services Corporation suggested that a quarter of all British shops use facial recognition. Fashion retailers were particularly likely to adopt this technology – 59 per cent of those surveyed used some form of facial recognition, and it is likely that this number is now higher given developments in this field.

18. Facial recognition may be used for a variety of purposes in a retail context. These include identifying people who the business feels may engage in criminal behaviour, driving customer satisfaction (for example, advertising hoardings fitted with facial recognition software which present targeted advertising to passing individuals), checking identification documents and security.

19. Predictive analytics are used in a retail environment and can involve tying a piece of biometric data (i.e. your facial features) to your whereabouts, monitoring the

---

13. CSC technology (now DXC Technology) (2015), *Next Generation In-store Technology: Where do Shoppers and Retailers Stand*, Available at: https://turtl.dxc.technology/story/55ee63d88bb0d07f2d4e22eeg

way you move around a retail environment. For example, a supermarket could use facial recognition software to identify where customers focus their attention whilst shopping in the store. Retail companies may also use emotion recognition – a process which maps facial expressions to identify how a person is feeling using image processing software. The concept of sensors and cameras monitoring shoppers, seeking to interpret their emotions without their consent and even showing tailored advertising to suit their emotional state is a deeply intrusive one, as well as raising concerns around keeping this data secure. Furthermore, a technology which can identify and track people’s emotional state is ripe for misuse and may be purchased for state use in other more sinister settings. For example, a US-based manufacturer of emotion recognition technology, “Eyeris”, sold its software to law enforcement agencies for use in interrogations.\(^5\)

20. Oliver Philippou, an expert in video surveillance at IHS Markit, has raised concerns around the accuracy of emotion detection, stating: "When it comes simply to identifying faces, there are still decent margins of error - the best firms claim they can identify people with 90%-92% accuracy. When you try [to] assess emotions, too, the margin of error gets significantly bigger".\(^6\) Frederike Kaltheuner, Data Exploitation Programme Lead at Privacy International, has highlighted the rights impact of the use of this technology: “the privacy implications stemming from emotional surveillance, facial recognition and facial profiling are unprecedented”.\(^7\)

21. Recent reports suggest that use of facial recognition at self-service checkouts in UK supermarkets is also increasing, although in this context it is deployed to judge how old customers are at self-checkout machines, to identify them for controlled substances such as alcohol. The technology will be added into tills made by retail chains including Tesco, Sainsbury’s, Marks & Spencer, Boots, and WHSmith.\(^8\) Risks of these particular processes include identity theft, forced activation and data privacy (the ability for you to control what data is generated and shared about you – in this case, this includes deeply sensitive biometric information).

22. Private sector use of biometrics also includes verification for log-ins and the storing of biometric data for access to mobile phones, computers or games.

---


\(^6\) Thomas (2018), The cameras that know if you’re happy - or a threat BBC News, 17 July 2018. Available at: https://www.bbc.co.uk/news/business-44799239

\(^7\) Ibid

\(^8\) Archer (2018), Facial recognition to be used in British supermarkets for the first time, The Telegraph, 17 October. Available at: https://www.telegraph.co.uk/technology/2018/10/17/facial-recognition-used-british-supermarkets-first-time/
consoles. Databases containing biometric data also pose huge cybersecurity concerns because they are increasingly valuable for hackers.

23. Private companies such as Facewatch\(^9\) use facial recognition to send instant alerts when “subjects of interest” enter business premises. Facewatch claims that their system proactively deters crime and protects businesses. It also claims that it is the only shared national facial recognition watch-list – clearly a database which is open to the risks outlined above. We have previously met with Facewatch and expressed our concerns about their use of this technology.

24. A particularly troubling use of biometrics in a retail context has been highlighted by news of long-term deployment of facial recognition in the Trafford Centre, Manchester. It has come to light\(^{20}\) that every visitor to the Trafford Centre in Manchester over a six-month period was monitored by facial recognition cameras, and Greater Manchester Police supplied approximately 30 images of missing persons as well as suspects.

25. What is of particular concern here is the use of Greater Manchester Police data in the context of a facial recognition deployment by a private company. A blog by the Surveillance Camera Commissioner\(^{21}\) highlights how the shopping centre decision makers were unaware of the responsibilities they would inherit when forming a partnership with the police force in question – including Freedom of Information Act obligations, accountability with the Crime and Disorder Act, and obligations under the Criminal Investigations and Procedure Act.

**BIG DATA SOCIETY AND THE WEB OF SURVEILLANCE**

26. Ever-expanding amounts of data are being collected in relation to each of us and then utilised in building up detailed and privacy-invading profiles. These profiles are opaque and insufficiently open to challenge. While they may be used to make erroneous or discriminatory decisions about how someone will think or behave, they also breach our fundamental right to privacy and increases the number of ways in which we are being monitored by the state.

---

\(^9\) See: [https://www.facewatch.co.uk/](https://www.facewatch.co.uk/)

\(^{20}\) Robson (2018), Greater Manchester Police monitored every visitor to Trafford Centre for SIX MONTHS using controversial technology until they were told to stop, Manchester Evening News, 15 October, Available at: [https://www.manchestereveningnews.co.uk/news/greater-manchester-news/gmp-trafford-centre-camera-monitored-15278943](https://www.manchestereveningnews.co.uk/news/greater-manchester-news/gmp-trafford-centre-camera-monitored-15278943)

27. This monitoring also impacts on our ability to express ourselves and discourages the expression of dissent or the alternative views necessary in a democratic society. Studies have shown that people censor what they post on social media or what they look up online when they are aware they are being surveilled by the state. This chilling effect won’t be felt evenly – for example, the same research showed that women and young people were more likely to self-censor as a result of surveillance.

28. Private companies play a significant role in amassing this data for their own purposes, but this also fuels state surveillance and the government will often rely on private companies to facilitate digital approaches in the public sector. This raises issues with the opacity of certain systems and the ability for data-based or automated decision-making processes to be open to challenge by those impacted by them.

29. Law enforcement bodies are rolling out a range of surveillance technologies with the capability to interact with data provided by private companies. This includes facial recognition, body worn video, mobile fingerprint scanners, IMSI catchers and mobile phone extraction kiosks. The ever-expanding amount of data collection in the private sector supports the use of these systems and will make mass surveillance easier to accomplish. For example, the ubiquity of surveillance cameras, which can easily be retrofitted with facial recognition software and fed into facial databases, means that there’s already an apparatus in place for large-scale monitoring, and the extensive repositories of photographs or the associated biometric data held by private companies could be requested by police for law enforcement purposes.

CONCLUSION


24 See, for example, the use of Experian’s “Mosaic” data by Durham Police in predicting offending behaviour: BBC News (2018), Durham police criticised over ‘crude’ profiling 9 April, Available at: https://www.bbc.co.uk/news/technology/43428265

25 For more information on the use of these technologies, see: https://www.libertyhumanrights.org.uk/human-rights/privacy/police-surveillance-technology
30. In Liberty’s view, and for the reasons outlined above, the collection, use and storage of data by private companies is sufficiently intrusive so as to require the Government to intervene in accordance with their duty to protect human rights. Alongside this, the Government itself must urgently address its own use of data, and the associated technologies and algorithms which feed off it, with a view to ensuring human rights compliance.

31. Encouraging advancements in the field of technology must never be used as a justification for the erosion of long-established, fundamental rights and freedoms. New, data-reliant technologies must have rights protections in-built by default and design, and it is from this basis that technological innovations can develop and thrive.

HANNAH COUCHMAN
Policy and Campaigns Officer