House of Commons
House of Lords

Joint Committee on Human Rights

# The Right to Privacy (Article 8) and the Digital Revolution

## Third Report of Session 2019

*Report, together with formal minutes relating to the report*

*Ordered by the House of Commons to be printed 30 October 2019*

*Ordered by the House of Lords to be printed 30 October 2019*

**HC 122**
**HL Paper 14**
Published on 3 November 2019
by authority of the House of Commons
and House of Lords

## Joint Committee on Human Rights

The Joint Committee on Human Rights is appointed by the House of Lords and the House of Commons to consider matters relating to human rights in the United Kingdom (but excluding consideration of individual cases); proposals for remedial orders, draft remedial orders and remedial orders.

The Joint Committee has a maximum of six Members appointed by each House, of whom the quorum for any formal proceedings is two from each House.

#### Current membership

**House of Commons**

Ms Harriet Harman QC MP (*Labour, Camberwell and Peckham*) (Chair)

Fiona Bruce MP (*Conservative, Congleton*)

Ms Karen Buck MP (*Labour, Westminster North*)

Joanna Cherry QC MP (*Scottish National Party, Edinburgh South West*)

Jeremy Lefroy MP (*Conservative, Stafford*)

Scott Mann MP (*Conservative, North Cornwall*)

**House of Lords**

Lord Brabazon of Tara (*Conservative*)

Lord Dubs (*Labour*)

Baroness Ludford (*Liberal Democrat*)

Baroness Massey of Darwen (*Labour*)

Lord Singh of Wimbledon (*Crossbench*)

Lord Trimble (*Conservative*)

#### Powers

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chairman.

#### Publication

© Parliamentary Copyright House of Commons 2019. This publication may be reproduced under the terms of the Open Parliament Licence, which is published at www.parliament.uk/copyright.

Committee reports are published on the Committee's website at www.parliament.uk/jchr by Order of the two Houses.

#### Committee staff

The current staff of the Committee are Claire Coast-Smith (Lords Committee Assistant), Miguel Boo Fraga (Senior Committee Assistant), Samantha Granger (Deputy Counsel), Shabana Gulma (Specialist Assistant), Katherine Hill (Committee Specialist), Eleanor Hourigan (Counsel), Lucinda Maer (Commons Clerk), Alexandra McMillan (Lords Clerk) and Jessica Bridges Palmer (Media Officer). For this report they were assisted by Abdulbasit Abdulrahim (on secondment from the Bonavero Institute of Human Rights, University of Oxford).

### Contacts

All correspondence should be addressed to the Clerk of the Joint Committee on Human Rights, Committee Office, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 2467; the Committee's email address is jchr@parliament.uk

You can follow the Committee on Twitter using @HumanRightsCtte

# Contents

# Summary

Most of us use the internet every day. We use it for work, to learn, to shop, to socialise, to watch films and listen to music, and to access vital services like banking and welfare benefits. The internet has the potential to enhance our human rights. It can support freedom of expression, the right to education, freedom of association and participation in elections.

While we recognise the benefits we get from the internet, we are all too aware of the potential for harm. We recently published the report of our 'Democracy, freedom of expression and freedom of association' inquiry which looked, among other things, at the threats and abuse directed at MPs on social media.[1] The death of Molly Russell in 2017 highlighted the danger posed by the graphic content relating to suicide and self-harm that is available online. Parents are 'worried sick' over the relatively easy access their children have to online pornography. Online misinformation campaigns aimed at influencing elections are the subject of inquiries across the globe. We recognise all of these concerns, but for this inquiry have focused on one specific aspect of online harm that has received less attention: the risk to our right to privacy, and the risk of discrimination, which arises from how companies collect and use our data online.

Much of what we are able to use on the internet is free because, from social media platforms to search engines, a business model has evolved in which companies make money from selling advertising opportunities to other companies rather than charging individuals to use the service. This makes having access to our data an extremely valuable commodity. Because, unlike advertising in a newspaper or on a bus stop, internet content can be personalised (meaning different people using the same website can be shown different advertisements), companies want as much information about us as possible, so that they can effectively target their advertising and maximise their revenue.

Companies collect this information from the forms we fill in online when we sign up to a website or buy something online or even when we agree to cookies when visiting websites . But they also use our photos, our social media 'likes', our browsing history and a wide range of other sources to build up a profile of us, which they may then sell on to other companies. The legal basis companies use for doing this is, in most cases, 'consent': we click a box when we sign up for a service, to say we accept how our data will be used.

The evidence we heard during this inquiry, however, has convinced us that the consent model is broken. The information providing the details of what we are consenting to is too complicated for the vast majority of people to understand. Far too often, the use of a service or website is conditional on consent being given: the choice is between full consent or not being able to use the website or service. This raises questions over how meaningful this consent can ever really be.

Whilst most of us are probably unaware of who we have consented to share our information with and what we have agreed that they can do with it, this is undoubtedly

1 Joint Committee on Human Rights, First Report Session 2019–20, Democracy, freedom of expression and freedom of association: Threats to MPs, HC 37 / HL Paper 5

doubly true for children. The law allows children aged 13 and over to give their own consent. If adults struggle to understand complex consent agreements, how do we expect our children to give informed consent. Parents have no say over or knowledge of the data their children are sharing with whom. There is no effective mechanism for a company to determine the age of a person providing consent. In reality a child of any age can click a 'consent' button.

The bogus reliance on 'consent' is in clear conflict with our right to privacy. The consent model relies on us, as individuals, to understand, take decisions, and be responsible for how our data is used. But we heard that it is difficult, if not nearly impossible, for people to find out whom their data has been shared with, to stop it being shared or to delete inaccurate information about themselves. Even when consent is given, all too often the limit of that consent is not respected. We believe companies must make it much easier for us to understand how our data is used and shared. They must make it easier for us to 'opt out' of some or all of our data being used. More fundamentally, however, the onus should not be on us to ensure our data is used appropriately - the system should be designed so that we are protected without requiring us to understand and to police whether our freedoms are being protected.

As one witness to our inquiry said, when we enter a building we expect it to be safe. We are not expected to examine and understand all the paperwork and then tick a box that lets the companies involved 'off the hook'. It is the job of the law, the regulatory system and of regulators to ensure that the appropriate standards have been met to keep us from harm and ensure our safe passage. We do not believe the internet should be any different. The Government must ensure that there is robust regulation over how our data can be collected and used, and that regulation must be stringently enforced.

Internet companies argue that we benefit from our data being collected and shared. It means the content we see online - from recommended TV shows to product advertisements - is more likely to be relevant to us. But there is a darker side to 'personalisation'. The ability to target advertisements and other content at specific groups of people makes it possible to ensure that only people of a certain age or race, for example, see a particular job opportunity or housing advertisement. Unlike traditional print advertising, where such blatant discrimination would be obvious, personalisation of content means people have no way of knowing how what they see online compares to anyone else. Short of a whistle-blower within the company or work by an investigative journalist, there does not currently seem to be a mechanism for uncovering these cases and protecting people from discrimination.

We also heard how the 'data' being used (often by computer programmes rather than people) to make potentially life-changing decisions about the services and information available to us is not even necessarily accurate, but based on inferences made from the data they do hold. We were told of one case, for example, where eye-tracking software was being used to make assumptions about people's sexual orientation, whether they have a mental illness, are drunk or have taken drugs. These inferences may be entirely untrue, but the individual has no way of finding out what judgements have been made about them.

We were left with the impression that the internet, at times, is like the 'Wild West', when it comes to the lack of effective regulation and enforcement.

That is why we are deeply frustrated that the Government's recently published Online Harms White Paper explicitly excludes the protection of people's personal data. The Government is intending to create a new statutory duty of care to make internet companies take more responsibility for the safety of their users, and an independent regulator to enforce it. This could be an ideal vehicle for requiring companies to take people's right to privacy, and freedom from discrimination, more seriously and we would strongly urge the Government to reconsider its decision to exclude data protection from the scope of their new regulatory framework. In particular, we consider that the enforcement of data protection rules - including the risks of discrimination through the use of algorithms - should be within scope of this work.

The internet is increasingly prevalent in all of our lives. More and more of us use 'virtual assistants' like Siri and Alexa and 'wearable tech' that collect our health data as we exercise and monitors our sleep. More and more services are inaccessible other than through the internet. The Government should be regulating to keep us safe online in the same way as they do in the real world - not by expecting us to become technical experts who can judge whether our data is being used appropriately but by having strictly enforced standards that protect our right to privacy and freedom from discrimination.

The internet has great potential to bring people together, give marginalised people a voice and enable access to learning at a scale that would be impossible offline. But we have heard how it has also led to vast swathes of, sometimes very personal, data being held and shared without our knowledge, used to make assumptions about us and discriminate against us. In the latest of Sir Tim Berners-Lee's annual letters on the 'birthday' of the World Wide Web he invented, he wrote:

> "Against the backdrop of news stories about how the web is misused, it's understandable that many people feel afraid and unsure if the web really is a force for good. But given how much the web has changed in the past 30 years, it would be defeatist and unimaginative to assume that the web as we know it can't be changed for the better in the next 30. If we give up on building a better web now, then the web will not have failed us. We will have failed the web."[2]

We cannot afford to wait 30 years; internet companies, regulators and the Government must step up now.

2 '30 years on, what's next #ForTheWeb', World Wide Web Foundation, 12 March 2019

# 1 The UK regulatory landscape

## Overview of the regulatory framework for data protection

1. The Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) provide the data protection framework in the UK. Data protection rules, under the GDPR, apply to companies and organisations who offer goods and services, whether or not they are based in the EU, whenever they process the personal data of individuals in the EU .

2. Data protection laws apply to all types of personal data. It does not matter what format the data takes. Whether it is online on a computer system or on paper in a structured file, whenever information directly or indirectly identifying an individual is processed, data protection rights have to be respected. The data protection regulatory landscape for the UK is governed by:

a) the general data protection regime which applies to most UK and EU businesses (and includes the General Data Protection Regulation ("GDPR") tailored by the Data Protection Act 2018 ("DPA"));

b) the Privacy and Electronic Communications Regulations ("PECR") which provide guidance on the use of electronic marketing messages (by phone, fax, email or text), cookies, or electronic communication services to the public; and

c) the electronic identification and trust services ("eIDAS") which governs the provision of trust services such as electronic signatures, electronic time stamps and website authentication certificates.

**Box 1: What do we mean by 'processing' data?**

> Article 4 of the GDPR defines processing as: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Source: General Data Protection Regulation

3. The data protection rules, under the GDPR, describe different situations where a company or an organisation is allowed process personal data. There are six lawful bases:

a) Contract/explicit agreement: where you have expressly agreed to the collection and/or processing of your data in a contract. Examples would include a contract to supply goods or services when you buy something online, or an employee contract.

b) Legal obligation: when processing your data is a legal requirement. This includes, for example, when your employer gives information on your monthly salary to the relevant Government departments in order to determine National Insurance contributions, eligibility for welfare benefits etc.

c) Vital interest: such as when this might protect your life. This could apply in emergency medical care, for example, when it is necessary to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

d) Public interest: when processing is necessary to enable an organisation to carry out its public functions and powers, or specific tasks in the public interest, as enshrined in law. This could include processing necessary for the administration of justice; parliamentary functions; statutory functions, governmental functions or activities that support or promote democratic engagement.[3]

e) Legitimate interest: this could include your bank using your personal data to check whether you could be eligible for a savings account with a higher interest rate, for example.

f) Consent: consent should be a freely given, specific, informed and unambiguous indication of the individual's wishes. The company or organisation must keep records, so it can demonstrate that consent has been given by the relevant individual.

4. One of the key aims of the GDPR and the DPA is to empower individuals and give them control over their personal data. It preserves existing rights for individuals and adds additional rights such as the right to data portability and the right to be forgotten.

5. The data protection laws also contain specific protections for children. For the purposes of the GDPR, a child is someone below the age of 16, although Member States can reduce this age to 13, as the UK has done in the DPA. Therefore, consent can only be obtained from a child under 13 in relation to online services if the consent is authorised by a parent. In the UK, children who are 13 or older are expected to give consent in the same way as adults - with all of the associated risks. Other conditions under which the GDPR allows data to be processed can also be applied to children's data, although organisations may find the criteria for the 'legitimate interests' condition, in particular, difficult to meet in relation to children.

6. Specific protections for children in data protection laws include:

a) Simplicity: privacy policies must be very clear and simple if they are aimed at children.

b) Automated decisions: profiling and automated decision-making should not be applied to children.

c) The right to be forgotten: this applies very strongly to children.

7. Lastly, the data protection laws make provisions for special category data. Special category data is considered more sensitive, and so needs more protection. It includes information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, health, sex life and sexual orientation. Special category data is broadly similar to the concept of sensitive personal data under the Data Protection Act 1998. Organisations must have a lawful basis for processing special category data in exactly

3 Information Commissioner's Office, Lawful basis for processing: Public Task

the same way as for any other personal data. The difference is that they will also need to satisfy a specific condition under Article 9 (2) of the GDPR. There are 10 conditions listed in Article 9(2). One of these is that the data subject has given "explicit consent" to the processing.[4]

## The regulatory and governing bodies concerned with data protection

8. The primary enforcer of rules relating to data protection, including the GDPR and DPA, is the Information Commissioner and her office ("ICO"). The ICO is an independent body that provides information and guidance to individuals and businesses, as well as taking enforcement action when organisations fail to meet their legal obligations.

9. Since April 2010, the ICO has had the power to issue monetary penalty notices of up to £500,000 for serious breaches of the Data Protection Act 1998 (and now the DPA 2018), and since May 2011 this power has been extended to serious breaches of the PECR.[5] Under the DPA 2018, there is now a higher penalty for severe violations (€20 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher) which is intended to encourage compliance.[6]

10. The Government has also set up the Centre for Data Ethics and Innovation ("CDEI") to provide independent, impartial and expert advice on the ethical and innovative deployment of data and Artificial Intelligence ("AI"). They produce guidance, highlight best practice, and publish recommendations for Government (which the Government is bound to consider and respond to publicly). Of particular relevance to this inquiry, the CDEI's work programme for 2019–20 contains plans for key reviews of both algorithmic bias and online targeting, investigating how data is used to personalise and shape people's online environments.[7]

## Overview of the regulatory framework for equality and human rights

11. In addition to specific data protection laws, human rights and equality legislation can also offer protection in relation to how people's data is used.

12. The Human Rights Act 1998 ("HRA"), is based on, and "gives further effect" to, the rights and freedoms contained in the European Convention on Human Rights ("ECHR").[8] Of particular relevance are: (i) the right to respect for private and family life (Article 8 ECHR); and (ii) the prohibition of discrimination in the enjoyment of other ECHR rights (Article 14 ECHR). The right to respect for private and family life includes protections against unnecessary surveillance or intrusion into an individual's private life or correspondence. The prohibition of discrimination provides that no one should be discriminated against when applying the other rights in the Convention–because, for example, of their sex, race, disability, sexuality, religion or age.

13. In addition, Section 13 of the Equality Act 2010 prohibits direct discrimination, while Section 19 prohibits indirect discrimination (where a provision, criterion or practice puts

4 See Information Commissioner's Office, Special category data: At a glance, for all ten conditions.
5 Information Commissioner's Office, Our history
6 Data Protection Act 2018, Sections 155, 156 and 157
7 See Department for Digital, Culture, Media & Sport, Independent - The Centre for Data Ethics and Innovation (CDEI) 2019/ 20 Work Programme, 20 March 2019
8 Human Rights Act 1998, Preamble

people sharing a protected characteristic at a particular disadvantage, and this cannot be objectively justified). The characteristics that are protected by the Equality Act in relation to goods and services are: age (but only if an individual is 18 or over); disability; gender reassignment; pregnancy and maternity; race; religion or belief; sex; and sexual orientation.

# 2 Our inquiry

14. On 3 December 2018, we launched a call for evidence asking for views on how the processing of personal data by private companies impacted human rights. While we recognise that there are concerns around the use of personal data in the public sector, as highlighted in the recent report by the UN Special Rapporteur on extreme poverty on the digital welfare state,[9] we decided to focus our attention on the private sector given the current speed at which private companies are increasing their acquisition and use of data, and the consequent impact this has on individuals.

15. Through the course of the inquiry, we received 31 written submissions. We also took oral evidence from a range of witnesses including the Information Commissioner's Office, industry representatives, data brokers and Google, as well as specialist lawyers, academics, and journalists. We are grateful to everyone who gave written or oral evidence.

16. We invited six individuals from diverse backgrounds to observe our oral evidence sessions. These individuals were not experts in data, technology, or human rights matters, but instead were ordinary members of the public. The aim of inviting these people to the session was to hear their reflections on the oral evidence. In particular, we wanted to understand whether the data practices of private companies seemed acceptable to them or whether any of the evidence worried them. We are grateful for their input into our inquiry. A summary of some of their reflections is included in the Annex.

17. We note that there have been many other reports into the harms and risks that result from the advancement of internet-related technologies. These, among others, include the Department for Digital, Culture, Media and Sport's recently published *Online Harms White Paper*[10] and the House of Lords' Communications Committee's report: *Regulating in a Digital World*.[11] Our inquiry sought to add a new perspective to this debate by specifically focusing on how human rights may be violated by current practices in relation to the processing of data online and whether the current rules and regulations are sufficient to protect human rights.

9 United Nations Human Rights, Report of the Special Rapporteur on Extreme Poverty and Human Rights, 11 October 2019

10 Department for Digital, Culture, Media and Sport, and Home Office, Online Harms White Paper

11 House of Lords, Report of the Select Committee on Communications, 2nd Report of Session 2017–19, Regulating in a digital world, HL Paper 299

# Chapter 3: A focus on 'consent' and 'legitimate interests' as legal bases for processing personal data

18. As outlined in Chapter one, there are six lawful bases for processing personal data. In the context of the provision of internet-based services, the most common bases are consent and legitimate interests.

## Consent

19. Several witnesses expressed concern with the way that consent, as a legal basis for data processing, worked. Tamsin Allen, Partner at Bindmans LLP, emphasised what is at stake: "What we are dealing with is agreeing to the use of your data not just by one company; you are agreeing to your data being used, reused, combined, mathematically altered, and kept probably for ever in one form or another [ … ] keeping you as one digital archetype at one moment in time."[12]

20. A major concern was whether individuals are aware about what they are consenting to when using social media platforms or other web services. According to Liberty:

> "[ … ] 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."[13]

21. Doteveryone, a think tank that champions responsible technology, agreed. In a research project they conducted, 47% said felt they had no choice but to sign up to terms and conditions, even if they have concerns about them.[14]

22. Dr Orla Lynskey, Associate Professor of Law at the London School of Economics, told us:

> "To be valid from a legal perspective, consent has to be freely given, specific and informed, so you can already imagine how difficult it is to fulfil those conditions when you think of the way in which you are asked to provide consent in the digital environment. If you are consenting to something on your mobile phone, for instance, that information might be disaggregated across six or seven documents that you have to click through a number of times to get a complete picture of the way in which your personal information is being used. That makes it very difficult to have informed consent.

12 Q20 [Tasmin Allen]
13 Liberty (RTP0018)
14 Doteveryone (RTP0007)

> There is [also] a widespread commercial practice of bundling consent—having very vaguely stated purposes for the use of your personal information, which militates against this idea that you should be consenting to something specific."[15]

23. Privacy International agreed that having unduly lengthy privacy policies made it difficult for individuals to make informed choices about handing over their personal data:

> "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. 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. Reading the privacy policies of the fifteen companies the BBC examined would take an average person almost nine hours to read."[16]

24. The 'consent model' also relies on individuals having the necessary expertise to understand the risks that may be involved in what they are consenting to. Tamsin Allen, a Partner at Bindmans LLP, made the point that we do not expect this from individuals when it comes to assessing risk in the 'real world':

> " If you enter a building, you do not sign away your rights to enter it safely. You do not sign a form with 14,000 pages that tells you how the building was built and that says you have to accept the risk. You rely on the fact that the architect, the engineer and the builder will be subject to regulation, and that there will be insurance and public liability requirements on the building because it is open to the public, and you will feel that you can then walk into that building safely.
>
> The companies that build data systems describe themselves as architects and engineers, so it is unfair on an individual to expect them to take responsibility for any risks, and there are serious risks of harm associated with using web-based services."[17]

25. **We consider that the vast majority of individuals would find it almost impossible to know what they are consenting to when using social media platforms or other web services. Individuals are highly unlikely to read or fully understand complex and lengthy terms and conditions or privacy notices. Moreover, these notices are non-negotiable and offered in a take it-or-leave-it manner. Facebook, Snapchat, YouTube and many other online services make joining a service conditional on agreeing wholesale to terms and conditions, which includes current privacy notices and future changes to terms. In practice, this means individuals often have no choice but to agree if they want to use a service, which raises questions about whether or not consent has really been given.**

15 Q2 [Dr Orla Lynskey]
16 Privacy International (RTP0025)
17 Q20 [Tamsin Allen]

26. **Our view, based on the evidence we heard, is that the consent model is broken. It puts too much onus on the individual to educate themselves on how the technology companies work rather than setting a high standard of protection by default.**

27. ***It is unreasonable to place the onus for knowing about the risks or harms associated with using web-based services on the consumer. Internet users should be able to trust that the infrastructure is secure and will protect them appropriately. Consent should no longer be used as a blanket basis for processing.***

28. ***Just as they do in the offline world, the Government must ensure robust regulatory standards are in place, and rigorously enforced, so internet users can be confident that any data that companies hold about them is being used in a reasonable manner.***

### *Children and the "consent" model*

29. There are also concerns about the way that children's consent is obtained online. As outlined in Chapter One, in the UK a child aged 13 years or older can consent to their personal data being processed; parental consent is required to collect and process the information of children aged 12 and under.

30. UNICEF UK argued that, in situations where parental consent is required for children to share their data, there is no guarantee that parents are better-positioned to make decisions that protect children's privacy.[18] UNICEF UK cite research by the LSE from May 2018 which looked at whether parents have the skills to translate concerns about privacy into practical action. They found that 58% of parents said they could change their own privacy settings online while 53% said they could decide which information they want to share, suggesting that nearly half would not know how to stop their children's data being shared.[19]

31. It is also not clear how websites and social media platforms can determine the age of the person consenting with any accuracy, suggesting the data of many children under the age of 13 may be being collected and processed without parental consent. We note that some respondents to the ICO's Age Appropriate Design Code Consultation, which closed in May 2019, highlighted obtaining and verifying parental consent for children under 13 was a problem.[20] We also note with considerable disappointment that Government plans to introduce an age verification of 18 for online pornography that were contained in Part 3 of the Digital Economy Act are not being commenced, although they are looking at other mechanisms to achieve similar aims.[21] We call on the Government to expedite finding an effective solution to this problem as part of its wider work on online harms. While not directly related to the focus of this inquiry, the debate on protecting children from adult content highlights the lack of mechanisms in place to determine the age of the user.

18 UNICEF UK (RTP0019)

19 London School of Economics, What do parents think, and do, about their children's online privacy? Parenting for a Digital Future: Survey Report 3, May 2018

20 Information Commissioner's Office ICO's call for evidence – Age appropriate design code: summary of responses, page 2

21 Rt Hon Nicky Morgan MP, Written Ministerial Statement, 16 October 2019, HCWS13

32. For those children deemed old enough to give consent (those aged 13 or over), 5Rights Foundation, an organisation which is dedicated to making the digital environment fit for children, stressed that the barriers to giving informed consent are even greater than for adults:

> "Technology companies often assert that children understand their privacy and rights online. Yet extensive independent research repeatedly finds not only that children don't fully understand their privacy or rights online, but also that they are actively discouraged from understanding them by the way the information is presented online.
>
> Children don't read terms and conditions or privacy notices and are either unable or discouraged to given their length and complexity"[22]

33. The Government has announced its intention to publish draft legislation aimed at tackling online harm, which includes protecting children from harmful content.[23] We believe this could also be a vehicle for protecting children (and adults) in relation to how their data is used, an issue we explore further in Chapter 6. We look forward to scrutinising the draft Bill, including to consider whether there are sufficient protections within it to protect children online, in line with the United Nations Convention on the Rights of the Child.[24]

34. **Children and vulnerable adults are likely to find it particularly difficult to give meaningful consent, given the complexity of documents they are being asked to read. In addition, peer pressure to join the same social networks as their friends may make the 'take it or leave it' approach to consent especially problematic for children.**

35. **We do not believe that it is reasonable to expect 13 year-olds to give informed consent to their personal data being processed.**

36. **We also believe there is a very strong likelihood of those under 13 regularly 'consenting' to their data being used, given that there is no meaningful way for a company to determine the age of the person consenting.**

37. ***The general rule under Article 8 of the GDPR is an age of digital consent of 16. Protections for children in the UN Convention on the Rights of the Child should apply to all children under the age of 18. While the 'consent model' for data processing in the GDPR remains, the Government should urgently act to protect children by raising the age of digital consent to 16, and putting in place adequate protection for all those under 18 who access services online. In any case, consent should not be used as a basis for processing the data of children under the age of 16.***

22 5Rights Foundation (RTP0017)

23 Prime Minister's Office, The Queen's Speech and associated background briefing, on the occasion of the opening of Parliament on Monday 14 October 2019

24 See for example the requirements of Articles 16, 17 and 19 UN Convention on the Rights of the Child, which apply to all children under the age of 18.

## Legitimate interests as a basis for processing data

38. Article 6(1)(f) of the GDPR allows processing of data where:

> "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[25]

39. Recital 47 of the GDPR broadly describes areas where legitimate interests could be relied upon, such as:

- "where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller;"
- When the processing of personal data is "necessary for the purposes of preventing fraud;" and
- When data is processed for direct marketing purposes, i.e. advertising or marketing material which is directed to a particular group of individuals.[26]

40. The ICO's guidance on legitimate interests states that a "wide range of interests may be legitimate interests. The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests."[27]

41. Richard Cumbley, from Linklaters LLP, told us that the use of legitimate interests now requires organisations to go through a legitimate interest assessment, evidencing to the regulator that appropriate steps have been taken to mitigate risks to individuals.[28] However, Ailidh Callander from Privacy International, expressed concern that:

> "[ … ] legitimate interest is being used as a way to justify any business interest. There is no demonstrable evidence of how the rights of individuals are being considered."[29]

The ICO has also found that companies "are unable to demonstrate that they have properly carried out the legitimate interests tests and implemented appropriate safeguards."[30]

42. **Article 6 of the GDPR states that there may be legitimate interest for the controller to process the data without consent where there is a relevant and appropriate relationship**

25 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)

26 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)

27 Information Commissioner's Office, Lawful basis for processing - Legitimate interests, 22 March 2018

28 Q21 [Richard Cumbley]

29 Q21 [Ailidh Callander]

30 Information Commissioner's Office, Update report into adtech and real time bidding, June 2019

**between the individual and controller. However, there is not sufficient clarity on how an organisation determines what is in its legitimate interest and how it overrides the individual's rights.**

43. ***Given that there is a lack of understanding among companies around the use and relevance of the legitimate interests basis, we consider that there should be clearer guidance to companies either issued from the ICO or the Government around when and how the legitimate interests basis can be used. We also consider that there should be a rigorous process to test whether companies are using legitimate interests appropriately.***

# Chapter 4: Risks to the right to privacy

44. The rapid development of technology, as well the growth of business models which allow companies to offer free services online in exchange for personal data, has meant that private companies are able to process personal data on a massive scale. A new industry has emerged, made up of companies known as 'data brokers', which collects and sells data on millions of individuals.

45. Most individuals have to use the internet in their everyday lives: according to the Office for National Statistics, 87% of all adults used the internet daily or almost every day in 2019.[31] As a consequence, individuals release significant amounts of data.

46. Private companies assert that they collect data for the purposes of targeted advertising or personalisation of content. Google told us that personalising advertising to users "provide[s] an experience where ads are more relevant, more likely to be useful and, for advertisers, more likely to be effective."[32] Acxiom used the following examples to illustrate how personalised advertising could be useful for individuals:

> If a car company thinks you are in the market to buy a car, it will look to show you, rather than someone who is not, its latest offer for its latest model. If you live in a high-rise building, people who sell garden equipment do not want to show you an advert, because not only is it a waste of your time but a waste of their resources. If they waste money on advertising, their costs go up, as does the price to the consumer. It is an incredibly complex equation.[33]

47. Some of our witnesses, however, argued that the scale and amount of data that is being collected is beyond what is needed to provide a service. Madhumita Murgia from the Financial Times told us that current data practices of private companies were excessive and posed significant risks to individuals' right to privacy:

> "There is a social contract between all of us and our use of the free internet. Yes, we get all these [ … ] services for free and, yes, we do not mind being advertised to, especially if that advertising is relevant and targeted. That is agreed, and people want to use the internet for free, so they are willing to give up some amount of data, but the problem here is that it is completely out of control."[34]

## The problem with consent

48. As discussed in detail in Chapter 3, because of the length and complexity of consent agreements, and people's desire or need to use the services on offer, it is likely that people are agreeing to their data being shared without realising what they have agreed to or feeling like they have a choice. Research by Doteveryone, a think tank that champions responsible technology, found that 62% of the people they spoke to were unaware that social media companies made money by selling data to third parties and 45% were unaware that information they enter on websites and social media can help target advertisements.[35]

31 Office for National Statistics, Internet access – households and individuals, Great Britain: 2019, 7 August 2020
32 Q35 [Lanah Kammourieh Donnelly]
33 Q10 [Jed Mole, Acxiom]
34 Q11 [Madhumita Murgia]
35 Doteveryone (RTP0007)

49. **Using the internet is an essential part of most people's day-to-day lives. But use of many websites and services is contingent on consenting to personal data being shared. This puts people's right to privacy at risk. It is likely that many people are unaware that they have agreed for their data to be shared, especially given the complexity of consent agreements.**

## Sharing data without the subject's knowledge

50. The ICO told us that businesses are increasingly buying and selling data through data brokers without the data subject's knowledge and despite the fact that the data subject only gave consent to the use of their data in return for a service from one business.[36] In 2018, for example, the ICO fined the owners of parenting advice website Emma's Diary £140,000 for illegally selling data belonging to more than one million people. The data included people's names, household addresses, the number of children they had and their childrens' dates of birth. Emma's Diary sold the information, obtained through their registration forms, to Experian Marketing Services. Experian, in turn, created a database for the Labour Party in order to profile new mums in the run up to the 2017 General Election.[37]

51. The ICO also raised concerns about information acquired through business acquisitions. They told us that larger technology companies have been known to acquire vast amounts of data after buying smaller technology firms, even though consent for use of that data had been given by individuals at different times and to different entities.[38]

52. Dr Reuben Binns, a data scientist from the University of Oxford, told us about other ways in which people's data may be being shared without their consent. In his research study, which looked at nearly 1 million Android apps, he found that nine out of ten apps sent data back to Google; four out of ten apps sent data back to Facebook; and, in the case of Facebook, "many of them sent data automatically without the individual having the opportunity to say no to it."[39] Dr Binns told us that often even the developers of the apps are not necessarily fully aware of all the different parties that might receive that information:

> "You may think you have a relationship of trust between a user and an app developer, when in fact the app developer may not be fully in control of everything that is happening within the app they have developed. The same thing applies to many websites. A great deal of third-party code is included in these websites, which facilitates the harvesting of data for advertising technology purposes."[40]

53. **The evidence we heard suggests that people's data is routinely being shared and used without their consent, which clearly infringes on their right to privacy.**

54. ***It should be made much simpler for individuals to see what data has been shared about them, and with whom, and to prevent some or all of their data being shared.***

36 Information Commissioner's Office (RTP0027)
37 'Emma's Diary fined £140,000 for selling personal information for political campaigning', Information Commissioner's Office (9 August 2018)
38 Information Commissioner's Office (RTP0027)
39 Q10 [Dr Reuben Binns]
40 Q10 [Dr Reuben Binns]

55. ***The Government should explore the practicality and usefulness of creating a single online registry that would allow people to see, in real time, all the companies that hold personal data on them, and what data they hold.***

## Combining data from different sources

56. The ICO were one of a number of witnesses to raise concerns about data aggregation, or the practice of combining different data collected from different websites and online services, which can lead to very detailed profiles of individuals without the data subject's knowledge. The ICO state that "[a]s we enter the era of "the internet of things", larger aspects of people's lives will yield data including, for example, GPS systems in cars and on phones, online search histories, credit/debit card purchases, social media communications, and cookies on websites; combined they paint a sophisticated picture of an individual data subject."[41]

57. These profiles can be used, for example, to target online advertising, including through the real time bidding (RTB) process (see Box *2*) .

**Box 2: What is Real Time Bidding?**

RTB is a type of online advertising that enables advertisers to compete for digital advertising space, placing billions of online adverts on webpages and apps in the UK every day by automated means. It refers to the buying and selling of advertising inventory in real time through real-time auctions that occur in the time it takes a webpage to load.

Madhumita Murgia from the Financial Times explained how RTB can work in practice:

"There is an auction system in the way online advertising works. [ … ] If I am on one side, as a user of the internet going to visit a website, there are hundreds of companies that might want to advertise their product to a 30-year-old woman who lives in London, works in media and likes to buy clothes, for example [ … ] when you visit this website, a profile about who you are is sent out and people are asked to bid. Companies then decide if they want to place their ad in front of you and put out different bids. There is one winning bid, and that is the advert you see in front of you on your page [ … ]"[42]

58. The ICO's recent report into RTB explained:

> "[it] involves the creation and sharing of user profiles within an ecosystem comprising thousands of organisations. These profiles can also be 'enriched' by information gathered by other sources, e.g. concerning individuals' use of multiple devices and online services, as well as other 'data matching' services. The creation of these very detailed profiles, which are repeatedly augmented with information about actions that individuals take on the web, is disproportionate, intrusive and unfair in the context of the processing of personal data for the purposes of delivering targeted advertising."

41 Information Commissioner's Office (RTP0027

42 Q10 [Madhumita Murgia[

They go on to state that "in many cases data subjects are unaware that this processing is taking place."[43]

59. Financial Times journalist Madhumita Murgia explained the sort of data that could be being combined and shared in the RTB process:

> "It can be your IP address, which means your exact location; in some cases, your actual latitude and longitude are broadcast out. It can be where you live, where you work, what you like to buy, what health conditions you are interested in, where you are travelling to, everything you do in your daily life, what you have bought in the real world, political preferences or sexuality. The concern is that special category data that are protected, including race, sexuality and your health status, are being broadcast out to companies. We have no idea whom it is going to. We have no idea what they are doing with it. There is no transparency."[44]

60. The data broker Acxiom sought to reassure the Committee about the type of data that might be combined. They told us that they do provide a service which involves combining first-party data (i.e. that held by the client), with Acxiom's own data and/ or third-party data. However, they emphasised that they do not do this when it might result in insights that reveal special category data. Alex Hazell, the Head of Legal at Acxiom, gave an example:

> "[ … ] dry eye is a medical condition, so any data processed in relation to that condition would be special category data. [ … ] if we took Acxiom's dataset, combined it with people with dry eye and tried to spot some trends, in my view that would cross a red line, because the Acxiom data would become what, under data protection rules, is called special category data, which the legislation treats as a particularly sensitive form of data [ … ] That is one line we would never cross.[45]

### *Inferences*

61. Profiles that companies hold on individuals are likely to be partially based on data that the individual has submitted (either to that company or another company): perhaps as part of the sign-up process to join a social media network, or through a form filled in while buying something online. But profiles may also contain inferences that are made when that data is combined. Natasha Lomas from Tech Crunch explained:

> "Inferences can be made from personal data. You give your pieces of data and you think that is all you are giving, but using AI technologies all sorts of inferences can be drawn from this information. New companies might then calculate certain things about you that you do not necessarily know they are doing."[46]

43 Information Commissioner's Office, Update report into adtech and real time bidding, June 2019, page 6
44 Q10 [Madhumita Murgia]
45 Q13 [Alex Hazell, Acxiom]
46 Q8 [Natasha Lomas]

62. Natasha Lomas cited one example in which eye tracking software was being used to make assumptions about people's sexual orientation, whether they have mental illness, are drunk or have taken drugs. She said:

> "You are just using a piece of technology, and it might be making all these calculations about what it thinks you are, which might be wrong. If you do not even know it is happening, how could you address that inaccuracy? They might be telling someone else and sharing this inference that you are a drug taker, and it is not true."[47]

She went on to explain how difficult it would be to know if any inferences had been drawn about you:

> "[Facebook] has a button where you can download your data, but it will just give you the things you have literally uploaded. It will not give you all the inferences that Facebook has made from your data, everything it has learned by watching you continuously. It does not define all the surveillance and intelligence as your personal data."[48]

While the GDPR and the DPA give individuals the right to obtain a copy of their personal data (known as a 'subject access request'), this does not include the inferences that companies have made about a person based on that data as this is deemed to be the property of the company that acquired it. A House of Lords' Communications Committee report into digital regulation looked at this issue and recommended that users should be able to request, in a manner similar to a subject access request, any data that a company has generated about them.[49]

63. Professor Victoria Nash, from the Oxford Internet Institute at the University of Oxford, explained that these inferences could be used for a variety of purposes:

> "If their only effect is on what adverts I am served, I probably will not worry too much, but my understanding is that they may be used in many other areas, for example to affect the price of goods you are offered and the array of products that are served to you. They may be used in terms of transfers to health and insurance companies, and the technologies we use at work. The way in which inferences are drawn from this wide array of data is a trend that worries me."[50]

64. **Even where individuals have knowingly consented to sharing some of their personal data with one company, they may not be content with that data being combined to create a profile of themselves that they have no opportunity to see or edit.**

65. **It is deeply concerning that 'data' about an individual is being used and shared when it is based on inferences that may be untrue, and when the individual has no opportunity to correct any inaccuracies: indeed, there is no way of finding out what inferences may have been made about you.**

47 Q8 [Natasha Lomas]
48 Q8 [Natasha Lomas]
49 House of Lords, Report of the Select Committee on Communications, 2nd Report of Session 2017–19, Regulating in a digital world, HL Paper 299
50 Q10 [Professor Victoria Nash]

66. **This makes the need for people to be informed about what data is being collected and shared, and with whom, even more pressing.**

67. ***We agree with the recommendation of the House of Lords Communications Committee that, in a model similar to a subject access report under the GDPR, users should have the right to request data that a company has generated about them, so they are aware of any inferences that may have been made.***

## Risk of data breaches

68. The data storage practices of some businesses are another potential risk to privacy flagged to us by the ICO. They told us: "An obvious example is in the case of a data breach, where unauthorised entities gain access to data held by a data controller. This does not require a physical breach or loss, and with increasing amounts of data held in cloud storage remote hacking is becoming increasingly frequent."[51]

69. In July 2019, for example, the ICO issued a notice of its intention to fine the hotel chain Marriott International £99,200,396 for infringements to the GPDR. This related to a 'cyber incident' which exposed personal data from 339 million guest records.[52]

70. **Companies hold significant amounts of our personal data. They must take full responsibility for keeping it safe and secure.**

## User choice?

71. When Google gave evidence to our inquiry, they were keen to stress that "transparency, choice and control are fundamental tenets to us".[53] They described how users could "opt out of the personalisation of ads altogether" or use the "transparency and control tools [ … ] to revoke any consent to ads personalisation."[54] They explained how they had "embedded controls into the privacy policy so that when we describe a type of data collection and say, 'You have control over this', the control is right there" and that they offer 'privacy check-ups' to help people understand and alter their privacy settings, including what data they are content for Google to use.[55]

72. Research by Doteveryone, however, found that only 24% of people thought that digital services made it easy for people to change their privacy settings.

73. Several witnesses[56] also referred to research by the Norwegian Consumer Council which found that Facebook, Google and Windows 10 all make it difficult for people to increase their privacy settings and restrict the amount of their personal data that is shared.[57] They found that, in the case of Facebook and Google, "users who want the privacy friendly option have to go through a significantly longer process". Their report states:

51 Information Commissioner's Office (RTP0027)
52 Information Commissioner's Office, Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, 9 July 2019
53 Q35 [Lanah Kammourieh Donnelly]
54 Q35 [Lanah Kammourieh Donnelly]
55 Q35 [Lanah Kammourieh Donnelly]
56 Liberty (RTP0018); Privacy International (RTP0025)
57 Forbrukerradet, Deceived by design, How tech companies use dark patterns to discourage us from exercising our rights to privacy, 2018

> "The popups from Facebook, Google and Windows 10 have design, symbols and wording that nudge users away from the privacy friendly choices. Choices are worded to compel users to make certain choices, while key information is omitted or downplayed. None of them lets the user freely postpone decisions. Also, Facebook and Google threaten users with loss of functionality or deletion of the user account if the user does not choose the privacy intrusive option. The GDPR settings from Facebook, Google and Windows 10 provide users with granular choices regarding the collection and use of personal data. At the same time, we find that the service providers employ numerous tactics in order to nudge or push consumers toward sharing as much data as possible."[58]

74. **Companies must respect people's right to privacy, and make it easier for people to limit or stop how their data is being shared.**

## Challenging or deleting personal data

75. Google's Public Policy Manager, Lanah Kammourieh Donnelly, told us that the company does offer "deletion settings" and that they "recently rolled out a feature called auto-delete that also allows users to set an automatic rolling deletion of data associated with their account."[59] Evidence from other witnesses, however, suggests that correcting or deleting personal data being held about you can be a near impossible task.

76. Dr Melanie Smallman is a lecturer at the Department of Science and Technology Studies at UCL. Despite her knowledge and expertise, however, she found herself unable to stop her personal data being shared or to have it deleted:

> "When I train in the gym and the machines gather any fitness or weight data, that data goes to an app that I never signed up to and have asked repeatedly to be unsigned from. I spent two days trying to get the bottom of where this data goes and who it can be shared with, which is not clear [ … ] What is clear is that there are three or four steps in the chain of where my personal health data, which I have repeatedly asked not to be stored, is going [ … ] I have [now] given up."[60]

77. Tamsin Allen told us about a client "about whom completely false and private information was published in newspapers."[61] He successfully won a libel case but the stories still appeared in internet searches and so he wanted Google to remove them. She told us:

> "Months and months later, after their refusing to delist the URLs, he had to instruct lawyers. Months and months after we wrote to them, at great expense on his part, they agreed to de-list just some. Finally, we had to issue proceedings here and apply to serve them out of the jurisdiction and serve them on a Google in America—at enormous cost, because they were not playing ball with their own delisting service. They instructed very expensive

58 Forbrukerradet, Deceived by design, How tech companies use dark patterns to discourage us from exercising our rights to privacy, 2018
59 Q35 [Lanah Kammourieh Donnelly]
60 Q38 [Dr Melanie Smallman]
61 Q25 [Tamsin Allen]

> lawyers in London, who had a row with us. Eventually they agreed: "Right, we'll delist". They delisted, but everything that previously did not appear on the Google listing because it was too far down the ranking suddenly popped up. We got to the conclusion of the proceedings, he spent a fortune, and suddenly there is a whole load more of the same pieces of information back on Google. So we had to write back and asked them to go through all this again. They said, "Okay. We'll get rid of it all again". The same thing happened [ … ] it took 18 months to get anywhere near an internet clean-up, which is exceptionally difficult and expensive to do."[62]

78. ***Given that many people will have consented to their personal data being shared without being in a position to understand what they were agreeing to, that people's data is being shared without their consent and that inferences are being drawn from people's data to create a profile of them that may be entirely incorrect, it is vital that companies make it easy for people to correct or remove data held about them. While the GDPR gives individuals the rights to have their personal data erased and rectified, the evidence we heard suggests that these are not always adequately enforced. Companies must respect people's right to privacy, and make it easier for people to limit or stop how their data is being shared. We consider that these rights could be more effectively enforced if specific sanctions were associated with non-compliance of these rights by companies, particularly when companies fail to respond promptly or adequately to individual's requests to rectify or delete their data.***

62 Q25 [Tamsin Allen]

# Chapter 5: Risks of discrimination

79. We also heard how the increasing sharing of personal data online and associated data processing could result in discrimination against certain groups or individuals in the way that their personal data was used. As outlined in chapter one, the Equality Act 2010 prohibits direct and indirect discrimination by private companies in the provision of goods and services. As such, private companies could be liable to breaching the prohibition on direct or indirect discrimination in relation to the way that they use technology - even if discrimination was not intended. The characteristics that are protected by the Equality Act in relation to goods and services are: age (but only if an individual is 18 or over); disability; gender reassignment; pregnancy and maternity; race; religion or belief; sex; and sexual orientation.

## Targeted advertising and algorithms

80. Several witnesses raised concerns that the way companies are using people's personal data to target advertisements to them is resulting in discrimination. "Online platforms use algorithms (see Box 3) to present content to users based on (depending on the nature of the platform) what they were searching for, data collected about them ('personalisation') and factors such as whether an advertiser has paid for content to be prioritised."[63]

**Box 3: Algorithms**

> "An algorithm is a set of rules to be used to make the necessary decisions to complete a given task. While algorithms have been used since antiquity, they have been critical to the development of computer science. In recent years, the word 'algorithm' is often taken to mean complex decision-making software. Algorithms are used in artificial intelligence. 'Reinforcement learning' allows algorithms to improve and rewrite themselves without further human input. Article 22 of the GDPR protects users from being subject to decisions made by algorithms which have "legal or significant effects", such as when applying for loans online."

Source: House of Lords, Report of the Select Committee on Communications, 2nd Report of Session 2017–19, HL Paper 299

81. Madhumita Murgia from the Financial Times provided several shocking examples of how targeted advertising had resulted in discriminatory outcomes. She told us that an investigation by fellow journalists into job advertisements on Facebook found that "lots of companies, including Amazon, Facebook itself and Goldman Sachs, were gating at what age people should see those ads, essentially discriminating by saying, "We only want young, hip people to work at our company, so only show this advert to people between 20 and 40".[64] They also found that Facebook were accepting housing advertisements discriminating by race, and advertisements aimed specifically at 'Jew haters'.[65] We invited Facebook to give evidence to us; they were unable to make anyone available on the dates requested.

82. It was equally concerning to hear that it was possible for companies to discriminate in less overt ways by using personal data to categorise people. In addition to targeting

63 House of Lords, Report of the Select Committee on Communications, 2nd Report of Session 2017–19, Regulating in a digital world, HL Paper 299
64 Q11 [Madhumita Murgia]
65 Q11 [Madhumita Murgia]

individuals based on their protected characteristics, companies can target preferences which are likely to be held by certain groups (i.e. using indirect discrimination). Dr Melanie Smallman explained that:

> "The point is that the algorithms do not act in a discriminatory way by saying, "We're going to exclude all women", for example. It is much subtler than that. If you want to identify a young person, you can find somebody who likes a particular band or people who holiday in a particular place. You can advertise jobs to people who like golf. We know what these things mean."[66]

83. When we asked Google how they were ensuring that their platform was not being used by companies to bypass anti-discrimination laws, their Public Policy Manager, Lanah Kammourieh Donnelly, told us:

> "First, we are bound by all the laws in place in this country, including legislation on equality and non-discrimination. That is simply our baseline. In addition to that, we do not allow the targeting of users based on sensitive data categories. Our policies, which we review regularly, make it clear that we do not allow discrimination; when we find a violation, we take action."[67]

84. Professor Victoria Nash explained to us how difficult it is to determine if discrimination is occurring, because the content that each individual sees online is personalised to them: "Without seeing the adverts that each and every one of us in the UK receives, it is impossible for me to look for trends, such as patterns of discrimination in the adverts that are displayed."[68] Dr Melanie Smallman argued that the lack of diversity in the workforce of many internet companies may account for some of the discrimination taking place. She pointed out that it was important to understand that algorithms were not "simply automatic" and that "when adverts are served in a sexist or racist way, somebody is, or has been behind that."[69] Dr Smallman said:

> "That takes us to a much broader question about how technology companies are staffed, what workforces look like and how such decisions are even turned into algorithms in the first place [ … ]
>
> "What are people wanting to advertise asking for? We have all heard stories like, "I'm less likely to be served an advert for a high-paid job than my male partner who has equal qualifications to mine". What are advertisers asking for? I do not want to defend Google—it is not my job—but some responsibility has to be with those asking for such adverts. If they say, "I want to get my job advert to the right people", questions need to be asked, such as, "How would you decide who the right people are? Are you going to advertise equally to women and men? Is there a risk of our company looking bad as a result of this?"[70]

66 Q42 [Dr Melanie Smallman]
67 Q38 [Lanah Kammourieh Donnelly]
68 Q16 [Professor Victoria Nash]
69 Q36 [Dr Melanie Smallman]
70 Q36 [Dr Melanie Smallman]

## Inferences made from personal data

85. Our written evidence also highlighted specific concerns about how algorithms could draw inferences from personal data, posing risks in terms of discrimination. Written evidence from Dr Matthew White cites research by Dr Sandra Wachter which looked at how inferences drawn from personal data can create opportunities for "discriminatory, biased and invasive decision-making." The research suggested that major internet platforms or social media companies like Facebook, are able to infer protected characteristics such as race and sexual orientation, which are then used for targeted advertising, and that third parties have used such data to infer the socioeconomic status of individuals to determine people's eligibility for loans. In their paper, *A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI*, Dr Sandra Wachter and Brent Mittelstadt argue that:

> "Big Data analytics and artificial intelligence (AI) draw non-intuitive and unverifiable inferences and predictions about the behaviors, preferences, and private lives of individuals. These inferences draw on highly diverse and feature-rich data of unpredictable value, and create new opportunities for discriminatory [ … ] decision-making … "
>
> "[ … ]a new data protection right, the "right to reasonable inferences," is needed to help close the accountability gap currently posed by "high risk inferences," [ … ] that damage privacy or reputation, or have low verifiability in the sense of being predictive or opinion based while being used in important decisions."[71]

86. ***We were shocked to hear that major companies have used the ability to target advertising in order to discriminate against certain groups of people. Those social media channels and websites on which the advertisements are being placed must accept responsibility and carry out sufficient checks on adverts to ensure that companies are not inadvertently or deliberately excluding people in a discriminatory way which disadvantages them in their access to opportunities in areas like employment, housing or finance.***

87. ***There are challenging questions to be asked about the balance between providing 'personalised content' (i.e. showing someone the advertisements, news stories etc. that they are most likely to be interested in) and discriminating against people by deciding certain material should or should not be shown to them because of their particular demographics. This debate needs to be had, and we urge the Government to bring internet companies, regulators and users together to discuss this. These discussions should also explore how anti-discrimination laws can be better enforced in the online advertising world.***

88. ***Companies need to be aware of how targeting content at people based on certain hobbies, interests etc may indirectly be discriminating against certain groups of people. They should be actively looking for, and screening out, such practices and ensuring they have adequate tests in place to consider whether targeting certain aspects of users' profiles could be discriminatory.***

71 Dr Sandra Wachter and Brent Mittelstadt, A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI, Columbia Business Law Review, Volume 2019, Issue 2 (2018)

89. ***Important decisions–such as whether to refuse someone access to a service–should never be made based on inferences from people's data, and the Government should review whether the current legal framework is adequately robust in this regard.***

90. ***We consider that more transparency is needed in relation to how advertisements are targeted at individuals online, in order to prevent discrimination from occurring. This could potentially include introducing tools through which individuals can look up how companies are targeting adverts at them, or at others, online and which would enable regulators to effectively audit the criteria used by advertisers.***

91. We also note that there are concerns among some organisations working in this field that the DPA did not include a "collective redress" system, which would have allowed for one person or body to represent a group of individuals that have suffered the same harm.[72]

92. **We consider that mechanisms allowing for better collective redress could be particularly useful in relation to targeted advertisements online, given that an individual cannot compare what they see online with what is seen by others and would therefore be unaware that they were being discriminated against. In such situations, unlawful practices are more likely to be revealed by independent investigations, most often carried out by civil society organisations and charities; if these organisations could then pursue cases on behalf of the affected individuals, the companies undertaking these activities could more effectively be held to account.**

72 Privacy International, Privacy International's Response to the Open Consultation on the Online Harms White Paper, 1 July 2019

# 3 Chapter 6: Considering Alternative Enforcement Tools?

### *Implementing the UN Guiding Principles on Business and Human Rights*

93. The UN Guiding Principles on Business and Human Rights were endorsed by the UN Human Rights Council in 2011.[73] They are a set of guidelines for States and companies to prevent, address and remedy human rights abuses committed in business operations. A report by the UN High Commissioner for Human Rights, published in 2014, set out how these Principles apply to digital communication and the use of personal data.[74] The Commissioner states:

> "Enterprises that provide content or Internet services, or supply the technology and equipment that make digital communications possible, for example, should adopt an explicit policy statement outlining their commitment to respect human rights throughout the company's activities. They should also have in place appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact. Companies should assess whether and how their terms of service, or their policies for gathering and sharing customer data, may result in an adverse impact on the human rights of their users."[75]

94. The Commissioner also states:

> "In the context of information and communications technology companies, this [due diligence] also includes ensuring that users have meaningful transparency about how their data are being gathered, stored, used and potentially shared with others, so that they are able to raise concerns and make informed decisions. The Guiding Principles clarify that, where enterprises identify that they have caused or contributed to an adverse human rights impact, they have a responsibility to ensure remediation by providing [a] remedy directly or cooperating with legitimate remedy processes."[76]

95. The Northumbria Internet and Society Research Group explained how the Principles had the potential to help address privacy concerns in relation to how private companies use our data. They told us that adhering to the Principles "requires that a corporation knows the risks that big data and algorithmic decision making pose to privacy and is able to show that the collection, storage and processing of data is compliant with human rights."[77] But Dr Nora Ni Loidean and Dr Rachel Adams from the Information Law and Policy Centre at the Institute for Advanced Legal Studies told us that "the Principles have

73 United Nations Human Rights. Office of the High Commissioner, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, 2011

74 Human Rights Council, The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014

75 Human Rights Council, The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014

76 Human Rights Council, The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014

77 NINSO Northumbria Internet & Society Research Group (RTP0011)

not been widely implemented in practice."[78] They explained that the Principles "constitute a soft law mechanism in international law" and said that the Principles "are not binding on state parties or private companies."[79]

96. Horizon, a Research Institute at the University of Nottingham, suggested that the requirement for human rights impact assessments advocated by the Principles should be translated "into national requirements that are more specific and enforceable", including integrating them "into existing impact assessment schemes, such as the data protection impact assessment (DPIA), which are mandated by the GDPR."[80] The Northumbria Internet and Society Research Group were also keen to see "further initiatives for the promotion and the implementation of the Guiding Principles", along with an "effective enforcement mechanism."[81]

97. We looked at in detail at the Guiding Principles as part of our 2017 inquiry into human rights and business.[82] In our report, we noted that the UK was the first state to implement the Principles, by publishing a National Action Plan in 2013, but concluded that we shared "the disappointment of many of our witnesses over its [the National Action Plan's] modest scope and lack of new commitments."[83] We also recommended that the Government bring forward legislative proposals to make reporting on due diligence in relation to human rights compulsory for large businesses.[84]

98. **The UN Guiding Principles on Business and Human Rights, if fully implemented, would address many of the concerns raised in this report by requiring companies to both make users aware of how their data is used and proactively identify and mitigate any adverse impact their activities may have on people's human rights.**

99. ***The Government should consider how it could mandate internet companies to adhere to the Guiding Principles, and how it could effectively enforce such a requirement. We restate the recommendation from our 2017 report on business and human rights that reporting on due diligence in human rights should be compulsory for large businesses.***

100. ***The Government should also update its National Action Plan for implementing the Guiding Principles to include specific consideration of the impact of internet and social media companies on human rights.***

### *Stronger enforcement of legislation*

101. Some of our witnesses argued that the current risks arising from the mass processing of personal data by private companies were not due to the lack of protection within existing legislation but rather due to the lack of enforcement of the law. The Law Society of Scotland told us: "we consider that the existing legislation offers a good level of protection in principle but in practical terms, enforcement is the deciding factor as to whether it

78 Information Law and Policy Centre, Institute of Advanced Legal Studies (RTP0012)
79 Information Law and Policy Centre, Institute of Advanced Legal Studies (RTP0012)
80 Horizon Digital Economy Research, University of Nottingham (RTP0004)
81 NINSO Northumbria Internet & Society Research Group (RTP0011)
82 Joint Committee on Human Rights, Sixth Repot of Session 2016–17, Human Rights and Business 2017: Promoting responsibility and ensuring accountability, HC 443 / HL Paper 153
83 Joint Committee on Human Rights, Sixth Repot of Session 2016–17, Human Rights and Business 2017: Promoting responsibility and ensuring accountability, HC 443 / HL Paper 153
84 Joint Committee on Human Rights, Sixth Repot of Session 2016–17, Human Rights and Business 2017: Promoting responsibility and ensuring accountability, HC 443 / HL Paper 153

proves effective."[85] Similarly, Ailidh Callander from Privacy International said: "We really need implementation and enforcement. That is where the gap is at the moment and where the effort should be: on proactive implementation and enforcement where there is blatant noncompliance."[86]

102. The GDPR does, on paper, appear to offer many of the protections that this inquiry has found to be necessary. It "requires organisations to be clear about what they do with individuals' personal data, how they do it, on what basis they do it, what data they hold, how long they will hold it for and who they will share it with."[87] And yet the evidence to this inquiry strongly suggests that internet companies are not adequately complying with these requirements.

103. The Law Society of Scotland raised concerns about the remit and the resources of the ICO:

> "We understand that the ICO will investigate breaches or concerns but this does not mean it is actively policing the conduct of companies where no such concerns have been raised. Furthermore, enforcement may increasingly require the regulator to be able to develop their own technology and have teams able to understand technological developments if abuses are to be identified and effectively prosecuted."[88]

104. The resources of the ICO are dwarfed by the companies that they are expected to regulate. In 2018, the ICO had a budget of just over £40 million.[89] In comparison, Google UK's 2018 revenue totalled £1.4 billion.[90]

105. ***The GDPR should offer a substantial level of protection for people's personal data, but this does not seem to have materialised in practice. The Government should review whether there are adequate measures in place to enforce the GDPR and DPA in relation to how internet companies are using personal data, including consideration of whether the ICO has the resources necessary to act as an effective regulator.***

## New regulation

106. The Government's Online Harms White Paper, published in April 2019, outlined plans for a new system of oversight for internet companies, with a new regulatory framework and an independent regulator.[91] While the Government does not consider the protection of personal data to be in scope of the White Paper (indeed, they explicitly rule it out, stating that the UK "already enjoys high standards of data protection law"[92]), their proposals have the potential to help mitigate some of the concerns raised in this inquiry. The proposals include:

85 The Law Society of Scotland (RTP0016)
86 Q23 [Ailidh Callander]
87 Written evidence from the Information Commissioner's Office provided to the House of Lords' Select Committee on Communications (IRN0087)
88 The Law Society of Scotland (RTP0016)
89 Information Commissioner's Office, Finance Report, Financial Year 2018/19, September 2018
90 Google UK forks out £65m tax in 2018, a boost of 40% on previous year, The Register, 3 April 2019
91 Department for Digital, Culture, Media and Sport, and Home Office, Online Harms White Paper, Updated June 2019
92 Department for Digital, Culture, Media and Sport, and Home Office, Online Harms White Paper, Updated June 2019

- Establishing a statutory duty of care to make companies take more responsibility for the safety of their users, and a requirement for companies to show how they are meeting that duty;
- Enforcement of this duty of care by an independent regulator, who would be given a range of enforcement powers including the ability to issue substantial fines; and
- A requirement that companies terms and conditions are sufficiently clear and accessible, including to children and other vulnerable users.[93]

107. On 14 October, as part of the Queen's Speech, the Government announced its intention to analyse the responses it received to its consultation on the White Paper, and then publish draft legislation for pre-legislative scrutiny.[94]

108. ***While we welcome the publication of the Government's Online Harms White Paper, it was disappointing that violation of people's right to privacy and freedom from discrimination were not included in their list of online harmful activity that they consider to be in scope of the White Paper. We do not agree with the Government that the existing legal framework provides adequate protection against the misuse of people's data by internet companies and would urge them to reconsider the scope of their proposals.***

109. ***The Government's proposals to create a new statutory duty of care to make companies take more responsibility for the safety of their users, enforced by an independent regulator, could provide a valuable framework for ensuring that internet companies uphold people's human rights. We urge the Government to include in its proposed "duty of care" a requirement for companies to adhere to robust standards on how people's data is processed.***

110. ***The Government should also consider how the UN 's Guiding Principles on Business and Human Rights could be incorporated into their new regulatory regime.***

93 Department for Digital, Culture, Media and Sport, and Home Office, Online Harms White Paper, Updated June 2019

94 Prime Minister's Office, The Queen's Speech and associated background briefing, on the occasion of the opening of Parliament on Monday 14 October 2019

# Conclusions and recommendations

## Consent

1. We consider that the vast majority of individuals would find it almost impossible to know what they are consenting to when using social media platforms or other web services. Individuals are highly unlikely to read or fully understand complex and lengthy terms and conditions or privacy notices. Moreover, these notices are non-negotiable and offered in a take it-or-leave-it manner. Facebook, Snapchat, YouTube and many other online services make joining a service conditional on agreeing wholesale to terms and conditions, which includes current privacy notices and future changes to terms. In practice, this means individuals often have no choice but to agree if they want to use a service, which raises questions about whether or not consent has really been given. (Paragraph 25)

2. Our view, based on the evidence we heard, is that the consent model is broken. It puts too much onus on the individual to educate themselves on how the technology companies work rather than setting a high standard of protection by default. (Paragraph 26)

3. *It is unreasonable to place the onus for knowing about the risks or harms associated with using web-based services on the consumer. Internet users should be able to trust that the infrastructure is secure and will protect them appropriately. Consent should no longer be used as a blanket basis for processing.* (Paragraph 27)

4. *Just as they do in the offline world, the Government must ensure robust regulatory standards are in place, and rigorously enforced, so internet users can be confident that any data that companies hold about them is being used in a reasonable manner.* (Paragraph 28)

5. Children and vulnerable adults are likely to find it particularly difficult to give meaningful consent, given the complexity of documents they are being asked to read. In addition, peer pressure to join the same social networks as their friends may make the 'take it or leave it' approach to consent especially problematic for children. (Paragraph 34)

6. We do not believe that it is reasonable to expect 13 year-olds to give informed consent to their personal data being processed. (Paragraph 35)

7. We also believe there is a very strong likelihood of those under 13 regularly 'consenting' to their data being used, given that there is no meaningful way for a company to determine the age of the person consenting. (Paragraph 36)

8. *The general rule under Article 8 of the GDPR is an age of digital consent of 16. Protections for children in the UN Convention on the Rights of the Child should apply to all children under the age of 18. While the 'consent model' for data processing in the GDPR remains, the Government should urgently act to protect children by raising the age of digital consent to 16, and putting in place adequate protection for all those under 18 who access services online. In any case, consent should not be used as a basis for processing the data of children under the age of 16.* (Paragraph 37)

### Legitimate interests

9. Article 6 of the GDPR states that there may be legitimate interest for the controller to process the data without consent where there is a relevant and appropriate relationship between the individual and controller. However, there is not sufficient clarity on how an organisation determines what is in its legitimate interest and how it overrides the individual's rights. (Paragraph 42)

10. *Given that there is a lack of understanding among companies around the use and relevance of the legitimate interests basis, we consider that there should be clearer guidance to companies either issued from the ICO or the Government around when and how the legitimate interests basis can be used. We also consider that there should be a rigorous process to test whether companies are using legitimate interests appropriately.* (Paragraph 43)

### Risk to privacy

11. Using the internet is an essential part of most people's day-to-day lives. But use of many websites and services is contingent on consenting to personal data being shared. This puts people's right to privacy at risk. It is likely that many people are unaware that they have agreed for their data to be shared, especially given the complexity of consent agreements. (Paragraph 49)

### Sharing data without subject's knowledge

12. The evidence we heard suggests that people's data is routinely being shared and used without their consent, which clearly infringes on their right to privacy. (Paragraph 53)

13. *It should be made much simpler for individuals to see what data has been shared about them, and with whom, and to prevent some or all of their data being shared.* (Paragraph 54)

14. *The Government should explore the practicality and usefulness of creating a single online registry that would allow people to see, in real time, all the companies that hold personal data on them, and what data they hold.* (Paragraph 55)

### Combining data from different sources

15. Even where individuals have knowingly consented to sharing some of their personal data with one company, they may not be content with that data being combined to create a profile of themselves that they have no opportunity to see or edit. (Paragraph 64)

16. It is deeply concerning that 'data' about an individual is being used and shared when it is based on inferences that may be untrue, and when the individual has no opportunity to correct any inaccuracies: indeed, there is no way of finding out what inferences may have been made about you. (Paragraph 65)

17. This makes the need for people to be informed about what data is being collected and shared, and with whom, even more pressing. (Paragraph 66)

18. *We agree with the recommendation of the House of Lords Communications Committee that, in a model similar to a subject access report under the GDPR, users should have the right to request data that a company has generated about them, so they are aware of any inferences that may have been made.* (Paragraph 67)

### Risk of data breaches

19. Companies hold significant amounts of our personal data. They must take full responsibility for keeping it safe and secure. (Paragraph 70)

### User choice?

20. Companies must respect people's right to privacy, and make it easier for people to limit or stop how their data is being shared. (Paragraph 74)

### Challenging or deleting data

21. *Given that many people will have consented to their personal data being shared without being in a position to understand what they were agreeing to, that people's data is being shared without their consent and that inferences are being drawn from people's data to create a profile of them that may be entirely incorrect, it is vital that companies make it easy for people to correct or remove data held about them. While the GDPR gives individuals the rights to have their personal data erased and rectified, the evidence we heard suggests that these are not always adequately enforced. Companies must respect people's right to privacy, and make it easier for people to limit or stop how their data is being sha*red. We consider that these rights could be more effectively enforced if sp*ecific sanctions were associated with non-compliance of these rights by companies, particularly when companies fail to respond promptly or adequately to individual's requests to rectify or delete their data.* (Paragraph 78)

### The risk of discrimination

22. *We were shocked to hear that major companies have used the ability to target advertising in order to discriminate against certain groups of people. Those social media channels and websites on which the advertisements are being placed must accept responsibility and carry out sufficient checks on adverts to ensure that companies are not inadvertently or deliberately excluding people in a discriminatory way which disadvantages them in their access to opportunities in areas like employment, housing or finance.* (Paragraph 86)

23. *There are challenging questions to be asked about the balance between providing 'personalised content' (i.e. showing someone the advertisements, news stories etc. that they are most likely to be interested in) and discriminating against people by deciding certain material should or should not be shown to them because of their particular demographics. This debate needs to be had, and we urge the Government to bring*

*internet companies, regulators and users together to discuss this. These discussions should also explore how anti-discrimination laws can be better enforced in the online advertising world.* (Paragraph 87)

24. *Companies need to be aware of how targeting content at people based on certain hobbies, interests etc may indirectly be discriminating against certain groups of people. They should be actively looking for, and screening out, such practices and ensuring they have adequate tests in place to consider whether targeting certain aspects of users' profiles could be discriminatory.* (Paragraph 88)

25. *Important decisions–such as whether to refuse someone access to a service–should never be made based on inferences from people's data, and the Government should review whether the current legal framework is adequately robust in this regard.* (Paragraph 89)

26. *We consider that more transparency is needed in relation to how advertisements are targeted at individuals online, in order to prevent discrimination from occurring. This could potentially include introducing tools through which individuals can look up how companies are targeting adverts at them, or at others, online and which would enable regulators to effectively audit the criteria used by advertisers.* (Paragraph 90)

27. We consider that mechanisms allowing for better collective redress could be particularly useful in relation to targeted advertisements online, given that an individual cannot compare what they see online with what is seen by others and would therefore be unaware that they were being discriminated against. In such situations, unlawful practices are more likely to be revealed by independent investigations, most often carried out by civil society organisations and charities; if these organisations could then pursue cases on behalf of the affected individuals, the companies undertaking these activities could more effectively be held to account. (Paragraph 92)

## The UN Guiding Principles

28. The UN Guiding Principles on Business and Human Rights, if fully implemented, would address many of the concerns raised in this report by requiring companies to both make users aware of how their data is used and proactively identify and mitigate any adverse impact their activities may have on people's human rights. (Paragraph 98)

29. *The Government should consider how it could mandate internet companies to adhere to the Guiding Principles, and how it could effectively enforce such a requirement. We restate the recommendation from our 2017 report on business and human rights that reporting on due diligence in human rights should be compulsory for large businesses.* (Paragraph 99)

30. *The Government should also update its National Action Plan for implementing the Guiding Principles to include specific consideration of the impact of internet and social media companies on human rights.* (Paragraph 100)

## Stronger enforcement of regulation

31. *The GDPR should offer a substantial level of protection for people's personal data, but this does not seem to have materialised in practice. The Government should review whether there are adequate measures in place to enforce the GDPR and DPA in relation to how internet companies are using personal data, including consideration of whether the ICO has the resources necessary to act as an effective regulator* (Paragraph 105)

## New regulation

32. While we welcome the publication of the Government's Online Harms White Paper, it was disappo*inting that violation of people's right to privacy and freedom from discrimination were not included in their list of online harmful activity that they consider to be in scope of the White Paper. We do not agree with the Government that the existing legal framework provides adequate protection against the misuse of people's data by internet companies and would urge them to reconsider the scope of their proposals.* (Paragraph 108)

33. *The Government's proposals to create a new statutory duty of care to make companies take more responsibility for the safety of their users, enforced by an independent regulator, could provide a valuable framework for ensuring that internet companies uphold people's human rights. We urge the Government to include in its proposed "duty of care" a requirement for companies to adhere to robust standards on how people's data is processed.* (Paragraph 109)

34. *The Government should also consider how the UN 's Guiding Principles on Business and Human Rights could be incorporated into their new regulatory regime.* (Paragraph 110)

# Annex: Reflections from participants who attended evidence sessions

We invited six individuals from diverse backgrounds to our oral evidence sessions. These individuals were not experts in data, technology, or human rights matters, but instead were ordinary members of the public who used the internet as part of their day-to-day lives. The aim of inviting the participants to the session was to hear their reflections on the oral evidence and in particular to understand whether the data practices of private companies seemed acceptable to them or whether any of the evidence worried them. Some of their reflections are included below:

- "Algorithms are scripted by people and therefore are not free of biases. How can this be mitigated? How can this be made transparent? The implications of this are scary."
- "I didn't know that even if you pay for an app the app has most probably used third party code and if that is the case (which is mostly the case) then your data is not safe with the app as it goes beyond the control of the app."
- "Paying for a service also does not guarantee data protection. Data protection should not be something you should have to pay for."
- "It's very clear that Google chooses higher exposure standards because it's in their financial interest to do so."
- "the age of consent to access the internet is 13, it should be older"
- [was worried to hear that] "our cookies are being used as surveillance."
- [was worried to hear that] "paid apps are still sharing data with Facebook"

# Declaration of Interests

Interests declared by Members during the Inquiry and / or consideration):

**Lord Brabazon of Tara (joined JCHR on 3 July 2019)**

- No relevant interests to declare

**Lord Dubs (joined JCHR on 3 July 2019)**

- No relevant interests to declare

**Baroness Hamwee (left JCHR on 3 July 2019)**

- No relevant interests to declare

**Baroness Lawrence of Clarendon (left JCHR on 3 July 2019)**

- No relevant interests to declare

**Baroness Ludford (joined JCHR on 3 July 2019)**

- No Interests declared

**Baroness Massey of Darwen (joined JCHR on 3 July 2019)**

- No interests declared

**Baroness Nicholson of Winterbourne (left JCHR on 3 July 2019)**

- No relevant interests to declare

**Baroness Prosser (left JCHR on 3 July 2019)**

- No relevant interests to declare

**Lord Singh of Wimbledon (joined JCHR on 3 July 2019)**

- No Interests declared

**Lord Trimble**

- No relevant interests to declare

**Lord Woolf (left JCHR on 3 July 2019)**

- No interests declared

# Formal minutes

## Wednesday 30 October 2019

Members present:

Ms Harriet Harman MP, in the Chair

| | |
|---|---|
| Lord Brabazon of Tara | Baroness Massey of Darwen |
| Fiona Bruce MP | Lord Singh of Wimbledon |
| Jeremy Lefroy | Lord Trimble |

Draft Report (*The Right to Privacy (Article 8) and the Digital Revolution*), proposed by the Chair, brought up and read.

*Ordered*, That the Chair's draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 110 read and agreed to.

Summary read and agreed to.

Annex agreed to.

*Resolved*, That the Report be the Third Report of the Committee.

*Ordered*, That the Chair make the Report to the House of Commons and that the Report be made to the House of Lords.

*Ordered*, That embargoed copies of the report be made available in accordance with the provisions of Standing Order No. 134.

[The Committee adjourned

# Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

### Wednesday 19 June 2019

**Steve Wood**, Deputy Commissioner (Policy), Information Commissioner's Office, **Dr Orla Lynskey**, Associate Professor of Law, Department of Law, London School of Economics, **Natasha Lomas**, Editor, TechCrunch, and **Antony Walker**, Deputy Chief Executive Officer, techUK Q1–8

### Wednesday 3 July 2019

**Dr Reuben Binns**, Researcher, Department of Computer Science, **Professor Victoria Nash**, Deputy Director, Associate Professor, and Senior Policy Fellow, Oxford Internet Institute, University of Oxford, **Madhumita Murgia**, European Technology Correspondent, Financial Times, **Jed Mole**, Vice-President, Marketing, and **Alex Hazell**, Head of UK Legal, Acxiom Q9–18

### Wednesday 10 July 2019

**Ms Ailidh Callander**, Legal Officer, Privacy International, **Richard Cumbley**, Partner, Linklaters LLP, and **Tamsin Allen**, Partner, Bindmans LLP Q19–33

### Wednesday 17 July 2019

**Lanah Kammourieh Donnelly**, Public Policy Manager, Google, and **Dr Melanie Smallman**, University College London Q34–45

**Jonathan Westley**, Chief Data Officer, Experian Q46–49

# Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

RTP numbers are generated by the evidence processing system and so may not be complete.

1 5Rights Foundation (RTP0017)

2 Big Brother Watch (RTP0014)

3 Carnegie UK Trust (RTP0003)

4 Dativa (RTP0002)

5 defenddigitalme (RTP0031)

6 Doteveryone (RTP0007)

7 eyeo GmbH (RTP0015)

8 Facebook (RTP0013)

9 Google (RTP0032)

10 Hedley, Susan (RTP0008)

11 Horizon Digital Economy Research, University of Nottingham (RTP0004)

12 Hull, Robin (RTP0024)

13 Independent Living Strategy Group (RTP0006)

14 Information Commissioner's Office (RTP0027)

15 Information Law and Policy Centre, Institute of Advanced Legal Studies (RTP0012)

16 The Law Society of Scotland (RTP0016)

17 Liberty (RTP0018)

18 Mavis Machirori, Stephanie Mulrine and Madeleine Murtagh (RTP0022)

19 medConfidential (RTP0005)

20 NINSO Northumbria Internet & Society Research Group (RTP0011)

21 Ordnance Survey (RTP0020)

22 Privacy International (RTP0025)

23 Reiber, Bettina (RTP0023)

24 Royal Geographical Society (with IBG) (RTP0009)

25 The Sanctuary (RTP0029)

26 Thomson Reuters (RTP0010)

27 Unicef UK (RTP0019)

28 Welch, Clare (RTP0028)

29 White, Matthew (RTP0021)

# List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

### Session 2017–19

| | | |
|---|---|---|
| First Report | Legislative Scrutiny: The EU (Withdrawal) Bill: A Right by Right Analysis | HC 774<br>HL 70 |
| Second Report | Proposal for a Draft Human Fertilisation and Embryology Act 2008 (Remedial) Order 2018 | HC 645<br>HL 86 |
| Third Report | Legislative Scrutiny: The Sanctions and Anti-Money Laundering Bill | HC 568<br>HL 87 |
| Fourth Report | Freedom of Speech in Universities | HC 589<br>HL 111 |
| Fifth Report | Proposal for a draft British Nationality Act 1981 (Remedial) Order 2018 | HC 926<br>HL 146 |
| Sixth Report | Windrush generation detention | HC 1034<br>HL 160<br>(HC 1633) |
| Seventh Report | The Right to Freedom and Safety: Reform of the Deprivation of Liberty Safeguards | HC 890<br>HL 161 |
| Eighth Report | Freedom of Speech in Universities: Responses | HC 1279<br>HL 162 |
| Ninth Report | Legislative Scrutiny: Counter-Terrorism and Border Security Bill | HC 1208<br>HL 167<br>(HC 1578) |
| Tenth Report | Enforcing Human Rights | HC 669<br>HL 171 |
| Eleventh Report | Second Legislative Scrutiny Report: Counter-Terrorism and Border Security Bill | HC 1616<br>HL 195<br>(HC 1827) |
| Twelfth Report | Legislative Scrutiny: Mental Capacity (Amendment) Bill | HC 1662<br>HL 208 |
| Thirteenth Report | Proposal for a draft Jobseekers (Back to Work Schemes) Act 2013 (Remedial) Order 2018 | HC 1451<br>HL 209 |
| Fourteenth Report | Draft Human Fertilisation and Embryology Act 2008 (Remedial) Order 2018 | HC 1547<br>HL 227 |
| Fifteenth Report | Proposal for a draft Human Rights Act 1998 (Remedial) Order 2019 | HC 1457<br>HL 228 |
| Sixteenth Report | Immigration Detention | HC 1484<br>HL 279 |
| Seventeenth Report | Human Rights Protections in International Agreements | HC 1883<br>HL 310<br>(HC 2199) |

| | | |
|---|---|---|
| Eighteenth Report | Legislative Scrutiny: Immigration and Social Security Co-ordination (EU Withdrawal) Bill | HC 569<br>HL 324 |
| Nineteenth Report | Youth detention: solitary confinement and restraint | HC 994<br>HL 343 |
| Twentieth Report | Good Character Requirements: Draft British Nationality Act 1981 (Remedial) Order 2019 - Second Report | HC 1943<br>HL 397<br>(HC 120) |
| Twenty-first Report | Proposal for a draft Fatal Accidents Act 1976 (Remedial) Order 2019 | HC 2225<br>HL 405 |
| Twenty-second Report | The right to family life: children whose mothers are in prison | HC 1610<br>HL 411 |
| First Special Report | Human Rights and Business 2017: Promoting responsibility and ensuring accountability: Government Response to the Committee's Sixth Report of Session 2016–17 | HC 686 |
| Second Special Report | Mental Health and Deaths in Prison: Interim Report: Government Response to the Committee's Seventh Report of Session 2016–17 | HC 753 |
| Third Special Report | Legislative Scrutiny: Counter–Terrorism and Border Security Bill: Government Response to the Committee's Ninth Report of Session 2017–19 | HC 1578 |
| Fourth Special Report | Windrush generation detention: Government Response to the Committee's Sixth Report of Session 2017–19 | HC 1633 |
| Fifth Special Report | Second Legislative Scrutiny Report: Counter-Terrorism and Border Security Bill: Government Response to the Committee's Eleventh Report of Session 2017–19 | HC 1827 |
| Sixth Special Report | Human Rights Protections in International Agreements: Government Response to the Committee's Seventeenth Report of Session 2017–19 | HC 2199 |

## Session 2019–20

| | | |
|---|---|---|
| First Report | Democracy, freedom of expression and freedom of association: Threats to MPs | HC 37<br>HL 5 |
| Second Report | The detention of young people with learning disabilities and/or autism | HC 121<br>HL 10 |
| First Special Report | Good Character Requirements: Draft British Nationality Act 1981 (Remedial) Order 2019 - Second Report: Government Response to the Committee's Twentieth Report of Session 2017–19 | HC 120 |

| | | |
|---|---|---|
| Second Special Report | Immigration detention: Government Response to the Committee's Sixteenth Report of Session 2017–19: Second Special Report of Session 2019–20 | HC 216 |