HOUSE OF LORDS

Select Committee on Communications

2nd Report of Session 2017–19

Regulating in a digital world

Ordered to be printed 26 February 2019 and published 9 March 2019

Published by the Authority of the House of Lords

HL Paper 299

Select Committee on Communications

The Select Committee on Communications is appointed by the House of Lords in each session "to look at a broad range of communications and broadcasting public policy issues and highlight areas of concern to Parliament and the public".

Membership

The Members of the Select Committee on Communications are:

Lord Allen of Kensington
Baroness Benjamin
Baroness Bertin
Baroness Bonham-Carter of Yarnbury
The Lord Bishop of Chelmsford
Baroness Chisholm of Owlpen
Viscount Colville of Culross
Lord Gilbert of Panteg (Chairman)
Lord Goodlad
Lord Gordon of Strathblane
Baroness Kidron
Baroness McIntosh of Hudnall
Baroness Quin

Declaration of interests

See Appendix 1.

A full list of Members' interests can be found in the Register of Lords' Interests:
http://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests

Publications

All publications of the Committee are available at:
http://www.parliament.uk/hlcommunications

Parliament Live

Live coverage of debates and public sessions of the Committee's meetings are available at:
http://www.parliamentlive.tv

Further information

Further information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is available at:
http://www.parliament.uk/business/lords

Committee staff

The staff who worked on this inquiry were Theodore Pembroke (Clerk), Theo Demolder (Policy Analyst) and Rita Cohen (Committee Assistant).

Contact details

All correspondence should be addressed to the Select Committee on Communications, Committee Office, House of Lords, London SW1A 0PW. Telephone 020 7219 6076. Email holcommunications@parliament.uk

CONTENTS

Evidence is published online at http://www.parliament.uk/internet-regulation and available for inspection at the Parliamentary Archives (020 7219 3074)

Q in footnotes refers to a question in oral evidence.

SUMMARY

The internet has brought huge opportunities, connecting the world as never before. The 'digital world'—an environment composed of digital services facilitated by the internet—plays an ever-increasing role in all aspects of life. However, regulation of the digital world has not kept pace with its role in our lives. Although it is not a lawless 'Wild West', a large volume of activity occurs online which would not normally be tolerated offline. Misuse of personal data, abuse and hateful speech make the case for further regulation compelling. The Government is expected, through its Internet Safety Strategy, to propose legislation intended to help make the UK "the safest place in the world to be online".

The need for regulation goes beyond online harms. The digital world has become dominated by a small number of very large companies. These companies enjoy a substantial advantage, operating with an unprecedented knowledge of users and other businesses. Without intervention the largest tech companies are likely to gain more control of technologies which disseminate media content, extract data from the home and individuals or make decisions affecting people's lives.

Over a dozen regulators have a remit covering the digital world. But there is no overall regulator. Regulation of the digital environment is fragmented with overlaps and gaps. Notably, there is no specific content regulator for the internet. We recommend the development of a comprehensive and holistic strategy for regulation.

The digital world does not merely require more regulation but a different approach to regulation. The key ideas that shape this report are that there should be:

(1) **an agreed set of 10 principles that shape and frame all regulation of the internet, and**

(2) **a new Digital Authority to oversee this regulation with access to the highest level of the Government to facilitate the urgent change that is needed.**

In this way the services that constitute the digital world can be held accountable to an agreed and enforceable set of principles.

We recommend 10 principles to guide the development of regulation online:

- Parity: the same level of protection must be provided online as offline
- Accountability: processes must be in place to ensure individuals and organisations are held to account for their actions and policies
- Transparency: powerful businesses and organisations operating in the digital world must be open to scrutiny
- Openness: the internet must remain open to innovation and competition
- Privacy: to protect the privacy of individuals
- Ethical design: services must act in the interests of users and society

- Recognition of childhood: to protect the most vulnerable users of the internet
- Respect for human rights and equality: to safeguard the freedoms of expression and information online
- Education and awareness-raising: to enable people to navigate the digital world safely
- Democratic accountability, proportionality and evidence-based approach.

Proper enforcement and resources will be necessary to implement these principles and promote their importance to all parts of the digital world.

Responses to growing public concern have been piecemeal, whereas they should be continually reviewed as part of a wider strategy. A new framework for regulatory action is needed. We recommend that a new body, which we call the Digital Authority, be established to instruct and coordinate regulators. The Digital Authority would have the remit to continually assess regulation in the digital world and make recommendations on where additional powers are necessary to fill gaps. The Digital Authority would also bring together non-statutory organisations with duties in this area.

Effective and timely policy-making and legislation relies on decision-makers being fully informed. However, the speed at which the digital world is developing poses a serious challenge. The Digital Authority should play a key role in providing the public, the Government and Parliament with the latest information. To ensure a strong role for Parliament in the regulation of the digital world, the Digital Authority should report to a joint committee of both Houses of Parliament whose remit is to consider all matters related to the digital world.

Principles should guide the development of online services at every stage. The design of online services affects what users see and how they behave. A prominent business model of the internet involves capturing users' attention to collect their data and advertise to them. We argue that there should be greater transparency when data are collected and greater choice to allow users to control which data are taken. There should also be greater transparency around data use, including the use of algorithms.

Digital markets pose challenges to competition law, including network effects which result in 'winner-takes-all', the power of intermediaries, and consumer welfare in the context of 'free of charge' services. The largest tech companies can buy start-up companies before they can become competitive. Responses based on competition law struggle to keep pace with digital markets and often take place only once irreversible damage is done. We recommend that the consumer welfare test needs to be broadened and a public interest test should be applied to data-driven mergers.

There are other consequences of market concentration. A small number of companies have great power in society and act as gatekeepers to the internet. Greater use of data portability might help, but this will require more interoperability.

In the EU illegal content is regulated by the operation of the general law and by the e-Commerce Directive, which exempts online platforms from liability unless they have specific knowledge of illegal content. At nearly 20 years old, it was developed before platforms began to curate content for users. Although liability already depends on the role a platform plays in delivering of content, the directive is no longer adequate for dealing with online harms.

Self-regulation by online platforms which host user-generated content, including social media platforms, is failing. Their moderation processes are unacceptably opaque and slow. We recommend that online services which host user-generated content should be subject to a statutory duty of care and that Ofcom should have responsibility for enforcing this duty of care, particularly in respect of children and the vulnerable in society. The duty of care should ensure that providers take account of safety in designing their services to prevent harm. This should include providing appropriate moderation processes to handle complaints about content.

Public opinion is growing increasingly intolerant of the abuses which big tech companies have failed to eliminate. We hope that the industry will welcome our 10 principles and their potential to help restore trust in the services they provide. It is in the industry's own long-term interest to work constructively with policy-makers. If they fail to do so, they run the risk of further action being taken.

Regulating in a digital world

CHAPTER 1: INTRODUCTION

> *"The changes we've managed to bring have created a better and more connected world. But for all the good we've achieved, the web has evolved into an engine of inequity and division; swayed by powerful forces who use it for their own agendas." Sir Tim Berners-Lee, Creator of the World Wide Web*[1]

> *"My position is not that there should be no regulation. I think the real question as the internet becomes more important in people's lives is 'What is the right regulation?'" Mark Zuckerberg, Chief Executive Officer and founder of Facebook*[2]

Background

1. We began our inquiry by asking whether further internet regulation was possible or desirable.[3] However, the focus of this report might be better described as the 'digital world': an environment composed of digital services—facilitated by the internet—which plays an ever-increasing role in all aspects of life. The digital world enables people to communicate and transact business with one another on a scale previously unimaginable.

2. The internet has transformed and disrupted economies thanks to rapid innovation enabled by light-touch regulation and a corporate culture which espoused the mantra "move fast and break things". The speed of technological change and its transnational character make the digital world hard to regulate.[4] There has been a widespread perception therefore that comprehensive internet regulation was not possible or that, if it were possible, it would not be advisable.

3. More recently, however, there has been a backlash against this attitude. A series of events have highlighted a litany of concerns, such as harmful online content, abusive and threatening behaviour, cybercrime, misuse of data, and political misinformation and polarisation. According to a survey for Ofcom and the Information Commissioner's Office (ICO), 45% of adult internet users in the UK have experienced some form of online harm.[5] However, individuals are unaware of rights they have or what they should expect from online service providers.[6] There is an emerging consensus that action is needed to address these concerns.

4. The internet started more than 40 years ago as a decentralised communications network which was open to be used by anyone, although it was largely

1 Sir Tim Berners-Lee, 'One Small Step for the Web…', *Medium* (29 September 2018): https://medium.com/@timberners_lee/one-small-step-for-the-web-87f92217d085 [accessed 29 January 2019]
2 'Marks Zuckerberg's testimony to Congress: Facebook boss admits company working with Mueller's Russia probe' *The Daily Telegraph* (11 April 2018): https://www.telegraph.co.uk/technology/2018/04/10/mark-zuckerbergs-testimony-congress-latest-news-facebook-hearing/ [accessed 23 November 2018]
3 See appendix 3 for our call for evidence.
4 Written evidence from The Children's Media Foundation (CMF) (IRN0033)
5 Ofcom and ICO, *Internet users' experience of harm online: summary of survey research* (September 2018): https://www.ofcom.org.uk/__data/assets/pdf_file/0018/120852/Internet-harm-research-2018-report.pdf [accessed 3 January 2018]
6 Q 161 (Caroline Normand)

used by the military and academics who had the necessary equipment and technical ability.[7] Since then a small number of companies have come to dominate the digital world. In the quotation above, Sir Tim Berners-Lee, the creator of the World Wide Web, expressed concern that this has led to a power imbalance, allowing these large companies to treat users unfairly and with little regard to negative consequences for society as a whole. Without intervention the largest tech companies are likely to gain ever more control of technologies which disseminate media content, extract data from the home and individuals or make decisions affecting people's lives. If governments fail to regulate the internet adequately, it will evolve in ways determined by, and in the interests of, these companies. Professor Christopher Marsden of the University of Sussex explained: "Our relationship with the internet, as society and as individuals, continues to develop, so the do-nothing option is not one in which nothing happens. A great deal happens, but without legislative impulse."[8]

5. Although the internet is subject to a variety of laws and regulation including copyright law, defamation law, the data protection framework, and the criminal law, a large volume of activity occurs online which would not normally be tolerated offline.

6. One example is the combined effect of personal data profiling and targeted political and commercial messaging including so-called 'fake news'. While some activities surrounding the Cambridge Analytica scandal have been found to be criminal, with the ICO stating its intention to fine Facebook the maximum £500,000 for two breaches of the Data Protection Act 1998, other forms of targeted messaging exist in a grey area. The Digital, Culture, Media and Sport Committee found that "Electoral law in this country is not fit for purpose for the digital age, and needs to be amended to reflect new technologies."[9]

7. This is but one recent area of concern. Jamie Bartlett, Director of the Centre for the Analysis of Social Media at Demos, told us that the digital world encourages poor behaviour at the personal level:

> "Simply the way we communicate with each other online is very sharp, quick, and dramatic. We tend to overstate our enemies' or opponents' importance and significance, and we attribute to them all sorts of terrible motives that they probably do not have, and they do likewise to us."[10]

8. Considerable media focus has been brought to bear upon political discourse in social media involving hateful forms of speech directed at female MPs. Amnesty International found that Diane Abbott MP received 8,121 abusive tweets in 150 days—an average of 54 per day.[11] There are widespread concerns

---

7 John Naughton 'The evolution of the Internet: from military experiment to General Purpose Technology' *Journal of Cyber Policy*, vol. 1, (12 February 2016): https://www.tandfonline.com/doi/full/10.1080/23738871.2016.1157619 [accessed 26 February 2019]

8 Q 1

9 Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Interim Report* (Fifth Report, Session 2017–19, HC 363)

10 Q 53

11 Amnesty International, 'Unsocial Media: Tracking Twitter abuse against women MPs' *Medium* (3 September 2017): https://medium.com/@AmnestyInsights/unsocial-media-tracking-twitter-abuse-against-women-mps-fc28aeca498a [accessed 16 January 2019]

about the role of social media in spreading hate and societal dissonance in spite of services' community standards forbidding hate speech.[12]

9. Although much of the discussion about internet regulation has focused on social media, Rachel Coldicutt, Chief Executive Officer of Doteveryone, cautioned that this is just "the tip of the iceberg. There are an enormous number of other potential harms."[13]

10. Action is needed to address these harms and to make the digital world work better for individuals and society.

The law on the internet

11. The internet is not an unregulated 'Wild West', as it has sometimes been characterised.[14] Criminal and civil law generally applies to activity on the internet in the same way as elsewhere. For example, section 1 of the Malicious Communications Act 1988 prohibits the sending of messages which are threatening or grossly offensive; it applies whether the message is through the post or through any form of electronic communication. There is also legislation which specifically targets online behaviour, such as the Computer Misuse Act 1990.

12. There are three models to enhance and enforce rules of law and other norms and standards online: regulation, co-regulation and self-regulation

13. Regulation is carried out by independent bodies with powers to monitor and enforce rules for conducting specified types of activity. Several regulators have responsibilities for activities which are particularly relevant to the online environment. Notably, Ofcom has responsibility for 'TV-like' content and telecommunications companies, which provide material access to the internet, and the Information Commissioner's Office regulates the use of data, which is essential to the digital economy.[15] But no regulator has a remit for the internet in general and there are aspects of the digital environment, such as user-generated content, for which no specific regulator is responsible.

14. Self-regulation is where internet businesses set rules themselves on a voluntary basis. These may include best practice and corporate social responsibility. In our report *Growing up with the internet*,[16] we found a strong preference among internet policy-makers for self-regulation online as it allowed businesses to apply rules in accordance with their own business interests.

15. Co-regulation is where a regulatory body delegates responsibility to enforce rules to an industry body. For example, the Communications Act 2003 gave Ofcom the duty to regulate broadcast advertising, but Ofcom delegated the day-to-day responsibility for this to the Advertising Standards Authority, an industry body which regulates advertising content.[17] In practice, there is a sliding scale of self-regulation and co-regulation depending on the degree to

12 There are many reports on this such as *CNN Business*, 'Big Tech made the social media mess. It has to fix it' (29 October 2018): https://edition.cnn.com/2018/10/29/tech/social-media-hate-speech/index.html [accessed 16 January 2019].

13 Q 28

14 Written evidence from Dr Paul Bernal (IRN0019)

15 See appendix 4 for a list of regulatory bodies which have such a remit.

16 Communications Committee, *Growing up with the internet* (2nd Report, Session 2016–17, HL Paper 130)

17 Advertising Standards Authority, 'Self-regulation and co-regulation': https://www.asa.org.uk/about-asa-and-cap/about-regulation/self-regulation-and-co-regulation.html [accessed 29 November 2018]

which rules are formalised and the Government, or other public bodies, put pressure on industry to regulate itself.[18]

16. The transnational nature of the internet poses problems in enforcing regulation, including conflicts of law, confusion about which jurisdiction applies and in seeking redress against foreign actors. But individual countries are not powerless in enforcing their own laws. Professor Derek McAuley and his colleagues at the Horizon Digital Economy Research Institute, University of Nottingham, explained how the General Data Protection Regulation (GDPR) identifies jurisdiction by focusing on where the impact of processing occurs, namely the location of the data subject: "So generally, it is the case that services targeted at specific jurisdictions through localisation, whether through language or tailored local content, and generating revenue from such localisation should be required to obey the regulation within that jurisdiction."[19]

17. Similarly, although it may be difficult to prevent online harms which originate outside the United Kingdom, the law can still be effective in protecting victims within this jurisdiction. For example, although salacious reports were published around the world about the private life of an anonymous celebrity, the Supreme Court granted an injunction against such reports being circulated in England and Wales where the celebrity's child might see them in future on social media.[20]

18. In the long-term regulatory fragmentation threatens the cohesiveness and interoperability of the internet, which has developed as a global and borderless medium. The Internet Society has called on national policy-makers to weigh the risks and benefits of any regulatory action, to collaborate with stakeholders, and to be mindful of the unique properties of the internet including interoperability and accessibility.[21] Global action also makes domestic measures more effective. The Government told us that the UK has played a leading role in addressing problems raised by the internet and notes that: "As the UK leaves the EU, international collaboration will be more important than ever."[22] The UN is currently undertaking a high-level inquiry on digital cooperation.[23]

Our inquiry

19. Building on our previous inquiries on children's use of the internet and the digital advertising market,[24] we set out to explore how regulation of the digital world could be improved. In doing so, we sought to inform the Government's 'Digital Charter', an ongoing programme of work aiming to make the UK "the safest place in the world to be online and the best place

18 Written evidence from Professor Christopher Marsden (IRN0080)
19 Written evidence from Horizon Digital Economy Research Institute, University of Nottingham (IRN0038)
20 *PJS v Newsgroup Newspapers* [2016] UKSC 26
21 Internet Society 'The Internet and Extra-Territorial Effects of Laws' (18 October 2018): https://www.internetsociety.org/resources/doc/2018/the-internet-and-extra-territorial-effects-of-laws/ [accessed 7 January 2019]
22 Written evidence from Her Majesty's Government (IRN0109)
23 UN Secretary-General's High Level Panel on Digital Cooperation, *Digital Cooperation Press Release* (12 July 2018) http://www.un.org/en/digital-cooperation-panel/ [accessed 26 February 2019]
24 Communications Committee, *Growing up with the internet* (2nd Report, Session 2016–17, HL Paper 130); Communications Committee, *UK advertising in a digital age* (1st Report, Session 2017–19, HL Paper 116)

to start and grow a digital business".[25] We support these objectives. In our view, good regulation is not only about restricting certain types of conduct; rather, it makes the digital world work better for everyone and engenders a more respectful and trustworthy culture.

20. Several witnesses highlighted that the internet is too broad a concept to speak meaningfully of regulating it—comprising different layers such as network infrastructure, protocols and standards, and user services built on top of these.[26] This report focuses on issues which are particularly relevant to the upper "user services" layer of the internet, in particular online platforms (see Box 1), but we believe that many of our key recommendations apply more broadly. Many witnesses argued that regulatory action should focus on the function of specific regulation (for example, data protection) rather than the technology being used,[27] and that "one-size-fits-all" regulation would not work. However, we believe that regulation can be guided by common principles even where implementation differs.

21. We were concerned that there are gaps in regulation and that it appears to be fragmented and poorly enforced online. Policy discussion in this area seems to be driven by public perceptions of specific harms. The Royal Academy of Engineering called for:

> "A strategic approach … alongside a more direct response to the current challenges. There is a risk that any response is tactical and piecemeal, responding to received wisdoms. Instead, a more fundamental rethink is required."[28]

We sought to understand the question of internet regulation holistically to see what general approach was required for the future.

Box 1: Online platforms

The European Commission defines an online platform as "an undertaking operating in two (or multi)-sided markets, which uses the internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups". There is some uncertainty about the scope of this definition as the uses of online platforms are extremely diverse and still evolving. Examples include search engines, marketplaces, social media platforms, gaming platforms and content-sharing platforms.

Online platforms share the following features: they use communication and information technologies to facilitate interactions between users, they collect and use data about these interactions; and they tend to benefit from network effects.

Source: European Commission (2015), 'Consultation on Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy', 24 September, p 5 https://ec.europa.eu/digital-single-market/en/online-platforms-digital-single-market

25 DCMS, *Digital Charter* (25 January 2018): https://www.gov.uk/government/publications/digital-charter [accessed 26 November 2018]
26 Written evidence from Cloudfare (IRN0064) and Internet Society UK Chapter (IRN0076)
27 Written evidence from Horizon Digital Economy Research Institute, University of Nottingham (IRN0038)
28 Written evidence from the Royal Academy of Engineering (IRN0078)

22. In the next chapter we consider a principles-based approach to regulation. Then we examine two overarching issues: the concentration of internet services into the hands of a small number of companies and the ethical principles of designing internet technology. Then we consider the role of online platforms in dealing with online harms; this is an area of focus as the Government develops its Internet Safety Strategy, a major strand of the Digital Charter.[29] Finally, we explore how to regulate for the future.

23. We received over 100 pieces of written evidence. Between July 2018 and January 2019 we took oral evidence from many witnesses including legal and social science academics, think tanks, charities, rights groups, broadcasters, journalists, industry bodies, and representatives of some of the world's largest tech companies, Google, Facebook, Microsoft and Amazon, as well as Twitter and Match Group. We also met representatives of criminal law enforcement, regulators and Margot James MP, Minister for Digital and the Creative Industries.

24. Our inquiry was also informed by several reports which have been published just before or during the inquiry. They include the work of:

    - the Select Committee on Artificial Intelligence;
    - the Digital, Culture, Media and Sport Committee which has been conducting an inquiry disinformation and 'fake news';
    - the Government's Internet Safety Strategy which has produced a Green Paper and a consultation response;
    - the House of Commons Science and Technology Committee;
    - the Australian Competition and Consumer Commission;
    - the Law Commission's scoping report;
    - Ofcom, which produced a discussion paper on addressing harmful online content; and
    - the European Commission, which has produced communications on online platforms and tackling illegal content online;[30]

    There have also been numerous reports by civil society groups and academics, including: Doteveryone, a thinktank; Communications Chambers, a consultancy; Professor Lorna Woods and William Perrin for the Carnegie UK Trust; and the LSE Truth, Trust and Technology Commission. The volume and contents of these reports reinforced our view that action is necessary.

25. The question of internet regulation has taken on a new prominence in the media since we began work. In particular, the death of 14-year-old Molly Russell and her family's campaigning has given rise to a greater public awareness of the most extreme risks the internet can pose. There has also been a noticeable shift in the rhetoric of major platforms. In February 2019 Twitter's CEO, Jack Dorsey, admitted that he would grade the company at a

29 DCMS, 'Internet Safety Strategy green paper (11 October 2017): https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper [accessed 11 December 2018]

30 This was also the subject of the European Union Committee's report. Select Committee on European Union, *Online platforms and the Digital Single Market* (10th Report, Session 2015–16, HL Paper 129)

'C' for 'Tech Responsibility' and reflected that Twitter had "put most of the burden on the victims of abuse (that's a huge fail)".[31] We hope that our report can play a valuable part in this crucial and fast-moving debate on the future of regulation in a digital world.

26. We are grateful to all those who contributed to our inquiry. We also thank Professor Andrew Murray, Professor of Law at the London School of Economics and Political Science, who provided expert advice throughout our inquiry.

31 Casey Quackenbush, 'Twitter's CEO gives the company a "C" for "Tech Responsibility"' *Time* (13 February 2019) http://time.com/5528229/twitter-jack-dorsey-combatting-abuse/ [accessed 14 February 2019]

CHAPTER 2: PRINCIPLES FOR REGULATION

A principles-based approach

27. The rapid pace of technological development requires a principles-based approach that sets out standards and expectations of service providers. Many witnesses advocated legislation that is 'technology neutral'—that is, legislation which targets specific types of behaviour regardless of the medium.[32] The Children's Media Foundation thought that "Legislation needs to be flexible to accommodate new challenges"[33] and that "the industry needs to interpret the intention of guidance as well as the specifics". To this end, a principles-based approach to regulation could help to improve the effectiveness of self- and co-regulation and inform and shape specific rules.

28. Principles can be applied to regulation in two ways. First, legislation can require that principles, expressed in a relatively general way, must be complied with. This form of principles-based regulation is often contrasted with rules-based regulation: principles-based regulation focuses on outcomes, whereas rules-based regulation prescribes the format compliance must take. The data protection principles set out in the GDPR are an example of this form of principles-based regulation. Elizabeth Denham, the Information Commissioner, explained:

> "Principles-based regulation works for an area of law that is fast changing and fast moving. [It] allows for more detail to be developed through guidelines, codes of practice and certification that flow from the principles."[34]

29. Ms Denham acknowledged that there were drawbacks of this approach: many commercial entities prefer the legal certainty of a rules-based system; however, she found such an approach to be "rigid" and "not future-focused".

30. Secondly, principles can be used to inform the development of regulation. Witnesses stressed the importance of legislation being aimed at specific 'sectors' of the internet[35] and enforced by the different regulators with expertise in their own area.[36] A principles-based approach can help to establish a common understanting for addressing issues which cut across sectors and can provide a common framework for regulators, executive bodies, policy-makers and lawmakers to work within to develop effective regulation.

31. The Government has used principles to inform work on its Digital Charter.[37] It argues that its principles are "mutually supportive", allowing for "a free and open internet while keeping people safe online". While we support these so far as they go, we believe that they are insufficient. In this chapter we

32 Written evidence from McEvedys Solicitors & Attorneys (IRN0065)
33 Written evidence from CMF (IRN0033)
34 Q 115
35 Written evidence from Airbnb (IRN0091). Airbnb lists e-commerce, media, search engines, communications, payment systems, labour provision, operating systems, transport, advertising, distribution of cultural content and social networks.
36 See appendix 4.
37 These are: the internet should be free, open and accessible; people should understand the rules that apply to them when they are online; personal data should be respected and used appropriately; protections should be in place to help keep people safe online, especially children; the same rights that people have offline must be protected online, and the social and economic benefits brought by new technologies should be fairly shared.

identify 10 principles which have emerged from our evidence and which should underpin regulation of the digital world:

- Parity
- Accountability
- Transparency
- Openness
- Ethical design
- Privacy
- Recognition of childhood
- Respect for human rights and equality rights
- Education and awareness-raising
- Democratic accountability, proportionality and evidence-based approach

32. No form of regulation will be effective unless it is enforced. Enforcement mechanisms must have sufficient resources and be rigorously applied.

Parity

33. We define the 'principle of parity' to mean that regulation should seek to achieve equivalent outcomes online and offline.

34. McEvedy's Solicitors and Attorneys wrote: "Good laws are technology and actor neutral and focus on behaviours and not actors, so the first question should remain what happens offline?"[38] None of our witnesses disputed the principle that what is illegal offline should also be illegal online. Though some felt that it had not always proved helpful in addressing policy issues.[39]

35. The London Internet Exchange (LINX), a membership association for network operators, warned that too often those who promote the principle exclusively want "restrictions and prohibitions" to be enforced online by private companies with no corresponding eagerness to ensure the administration of justice which balances competing interests in the independent court system offline.[40]

36. Myles Jackman, Legal Director of the Open Rights Group, told us that the underlying principles of regulation should apply both online and offline, but cautioned that care was needed to understand how technology will shape their implementation: "It is equally wrong to demand that something that works offline works exactly the same online—because it will not—as it is to say that the online world should create completely new rules."[41]

37. Recent developments on age verification provide an example of an attempt to transpose child protection rules into the digital environment. In the offline

38 Written evidence from McEvedys Solicitors and Attorneys (IRN0065)
39 Written evidence from Microsoft UK (IRN0085)
40 Written evidence from LINX (IRN0055)
41 Q 21. See also written evidence from British and Irish Legal Education Technology Association (BILETA) (IRN0029).

environment it would be illegal for a shopkeeper to supply a pornographic film to a child; this is regulated both by the classification framework operated by the British Board of Film Classification (BBFC) and the Video Recordings Act 1984. In the online environment, where the supplier of adult film content does not have face-to-face contact with the consumer and may not be directly subject to the UK regulatory framework, children are able to access material they would not normally be able to access offline. The Digital Economy Act 2017 requires commercial online pornography providers to check the age of users. These provisions will not be implemented until spring 2019 and gaps will persist. For example, social media companies will not immediately be in the scope of the most robust age verification standards.[42] The parity principle would bring them into scope.

Accountability

38. Accountability means that there are processes in place to ensure that individuals and organisations are held to account for their actions and policies. Such processes should involve establishing clear expectations and compliance with rules. If individuals or organisations are found to have not complied, they should be subject to sanctions or required to make amends. This principle applies to all organisations including third sector, businesses, public and regulatory bodies, and users.

39. There was widespread concern among our witnesses about the lack of accountability in the online environment. Many called for an 'enforcement approach', pointing out that often online the problem is not a lack of law or regulation but rather under-enforcement. Microsoft for example argued that "the challenges posed by the internet typically require enforcement of existing laws and regulations" rather than new legislation.[43]

40. Too often internet companies have been allowed "to mark their own homework" and can fail to uphold even the standards they themselves set in codes of practice.[44] Doteveryone told us that their research of public attitudes had found that people "feel disempowered in the face of technologies and have a strong appetite for greater accountability from technology companies and government".[45] This inequality suggests that independent oversight is required.

41. The Northumbria Internet & Society Research Interest Group suggested that users should also be made responsible for following rules, but added: "Long, unfair, and opaque privacy policies and usage guidelines are not a good way to achieve this."[46]

42. Given the power imbalances between users and tech companies, accountability mechanisms need to be quick, accessible and easy to use. Professor Lilian Edwards noted the value of "low cost or free [alternative dispute resolution] system for users, of the sort companies like eBay have provided in the past" though she remarked also on the need for public oversight or audit.[47] The

42 They may be classed as 'ancillary service providers', which would allow the BBFC to publicise their failure to comply with regulations but not to impose financial penalties.
43 Written evidence from Microsoft UK (IRN0085)
44 Written evidence from Sky (IRN0060)
45 Written evidence from Doteveryone (IRN0028)
46 Written evidence from NINSO (IRN0035)
47 Written evidence from Lilian Edwards, Professor of eGovernance (IRN0069)

evidence suggests that all parties, including internet platforms, regulators and governments, are failing to ensure access to redress.

Transparency

43. Transparency is key to ensuring accountability. It also has a role in enabling policy-makers to see how the online environment is functioning to identify problems, in promoting a common understanding of rules, and in enabling users to understand how their rights are affected. Transparency is particularly important online because of the balance of power between platforms and their users and because of the significant role platforms play in managing communications between individuals.

44. The issue of transparency grown in significance because of the adoption of automated decision-making systems in both the online and offline environment. For example, with a large volume of decisions surrounding content moderation now being fully or partly automated there is a risk that decision-making takes place within what Professor Frank Pasquale calls 'the black box', a system whose workings are mysterious; only inputs and outputs can be observed, but not the process in between.[48] Clare Sumner of the BBC said: "Everything around algorithms needs to be more transparent and people need to be more honest about whether they are using algorithms and what they are doing."[49]

45. This issue was raised in evidence on a number of occasions. Professor Lilian Edwards noted:

> "More transparency, as recently seen in the form of the publication of [Facebook's] content moderation rules and YouTube's take down "flags" is helpful and emerging driven by recent [public relations] scandals … But it is still unclear what action could be taken if the processes revealed seemed socially unacceptable either by governments or users, bar long and precarious challenges on human rights grounds."[50]

46. Very often it is not helpful to disclose a large volume of technical information, which can in fact lead to a lack of transparency as pertinent information is obscured. In such cases what is really needed is a clear explanation. Absolute transparency may also impinge on legitimate business interests. Subforum, a tech developer, noted that platforms were opaque because "transparent systems are easier to manipulate".[51] Recent scandals on data misuse, and concerns reported surrounding the policies applied by social media and other content moderation platforms, extending even to concerns raised in evidence by McEvedys around the highly respected system for regulation of child exploitation content, point to a "transparency gap".[52] It may be necessary to have different levels of transparency for different purposes. For example, the Information Commissioner's Office suggested that "Informing the users at a non-technical level must be paired with a deeper requirement to explain and account to the regulator."[53]

---

48 Professor Frank Pasquale, *The Black Box Society* (Harvard University Press 2015), p 3
49 Q 150
50 Written evidence from Lilian Edwards, Professor of eGovernance (IRN0069)
51 Written evidence from Subforum (IRN0013)
52 Written evidence from McEvedys Solicitors & Attorneys Ltd (IRN0065)
53 Written evidence from the Information Commissioner's Office (ICO) (IRN0087)

Openness

47. Openness has been a fundamental attribute of the internet since its inception. Professor John Naughton, Senior Research Fellow at the University of Cambridge, explained that the internet was designed with two fundamental axioms: "One was that there should be no central ownership or control of what they designed; the second was that they should design a network that was not optimised for anything they knew about at the time".[54] This has enabled creativity and "permissionless innovation".

48. Openness could be interpreted as a "carte-blanche for 'anything goes'".[55] Some innovation has been harmful. Jenny Afia, a partner at Schillings, told us that her biggest concern was that "children's best interests have been ignored probably because of the utopian vision that all internet users would be treated equally".[56] It therefore needs to be balanced against other principles, particularly ethical design and recognition of childhood, which are discussed below.

49. Others, such as Google, argue that the internet has enabled "the free flow of information online and given consumers, citizens, institutions and businesses more choice, power and opportunity".[57] As the internet plays a greater role in private and public life, human rights, including the rights of freedom of expression and freedom of information, need to be protected online.[58] One aspect of this is net neutrality: "the principle that internet service providers should enable access to all content and applications regardless of the source, and without favouring or blocking particular products or websites".[59] While net neutrality is traditionally associated with the infrastructure of the internet, analogous principles apply to certain internet services that run on top of the infrastructure level. Some witnesses expressed concern that the significant power of a small number of global companies is limiting choice and innovation: confining users within "walled gardens" and in so doing threatening the openness of the internet.[60] We consider this further in chapter 4.

Privacy

50. Privacy and data protection are already the subject of a significant body of law regulated by the Information Commissioner's Office. However, there is still much to be achieved in bringing about meaningful control of data privacy and data protection. The Northumbria Internet & Society Research Interest Group argued that "the recent issues with Facebook and Cambridge Analytica suggest there is scope for greater regulation of the use of individuals' personal data".[61]

51. Our evidence showed that there is a gap between what the data protection framework provides and what users expect. The Information Commissioner's

---

54 Q 83
55 Written evidence from CARE (IRN0024)
56 Q 59
57 Written evidence from Google (IRN0088). See also written evidence from the Royal Academy of Engineering (IRN0078).
58 Written evidence from BILETA (IRN0029). These two rights are enshrined in Article 10 of the European Convention on Human Rights.
59 Written evidence from the Advertising Association (IRN0039). In the US the Federal Communications Commission is seeking to repeal net neutrality rules in respect of Internet Service Providers.
60 Written evidence from Horizon Digital Economy Research Institute (IRN0038)
61 Written evidence from NINSO (IRN0035)

Office noted that despite the strength of the GDPR and related domestic legislation, "There is growing consumer unease about how online platforms are using personal data and potentially limiting consumer choice". It concluded: "it is fair to say that some aspects of the law have not kept pace with the rapid development of the internet".[62] As technological development increasingly results in connected homes, cars and cities, the balance between convenience and privacy will require debate and must be reflected in clear standards.

Ethical design

52. Many problems associated with the digital world originate in the way in which services are designed. Some internet technology is deliberately designed to take advantage of psychological insights to manipulate user behaviour. Laurie Laybourn-Langton, Senior Research Fellow, Institute for Public Policy Research, told us about how technology had used to learn more about user behaviour with a view to manipulating it.[63] He argued that there would have been a public backlash if the Government had undertaken similar research. This demonstrated a divergence between "the norms we have established in certain areas of society and those in this sector".

53. Ethical standards, such as safety and privacy, should be incorporated into the design of technology and delivered by default. Such standards should also ensure that individuals should not be manipulated but free to use the internet purposefully. Users should be treated on the basis of fair, transparent and consistent rules. Technology should act in the interests of users and the public. In particular, personal data should be used fairly. We consider this principle further in the next chapter.

Recognition of childhood

54. One third of internet users are under 18. In our report *Growing up with the internet*, we found that children are particularly vulnerable to online harms and that, although they are often early adopters of new technology, their welfare is very little considered by tech entrepreneurs.[64] We argued that this should change to make the internet work better for children.

55. Consideration of children should not just focus on protection. It is also necessary to consider how the internet can meet their needs and be accessible to them. Any principle-based approach to regulation must recognise children's rights, their legal status and the concept of childhood.

Respect for human rights and equality

56. The internet has become so ingrained in how individuals live that restricting internet access or usage threatens their ability to participate in essential personal, social, business and political activities. In particular, some witnesses stressed that the internet has become integral to participating in democratic life. It is therefore essential that regulation in the digital world respects human rights and equality rights. The Government told us that it was "firmly committed" to protecting these rights online: "These are essential qualities of any functioning democracy and promoting these

62 Written evidence from the ICO (IRN0087)
63 Q 53
64 Communications Committee, *Growing up with the internet* (2nd Report, Session 2016–17, HL Paper 130)

values is a key UK priority both at home and overseas. Any interference with these rights must be consistent with the principles of legality, necessity and proportionality."[65]

57. Dr Emily Laidlaw argued that the potential of the internet to promote and facilitate democratic activities was dependent on privately-owned companies which she called 'Internet Information Gatekeepers'. She explained that this referred to: "a gatekeeper which facilitates or hinders deliberation and participation in the forms of meaning making in democratic culture. Every time we use the internet we engage with IIGs. In order to find information, we use search engines. In order to sort through the clutter on the internet, we use portals. In order just to access the Internet, we need to use Internet service providers (ISP)."[66] The regulation and self-regulation of these gatekeepers must therefore take into account relevant human rights and equality legislation in the interests of users.

58. The Information Law and Policy Centre, Institute for Advanced Legal Studies suggested that the application of European Convention on Human Rights case law would help to avoid disproportionate censorship online.[67] Mark Stephens, a partner at Howard Kennedy, drew the committee's attention to the UN Guiding Principles on Business and Human Rights[68] ('Ruggie Principles'), which were designed to be used for businesses carrying out activities which affect human rights and could inform further internet regulation.[69] Any such regulation must observe due process, as outlined in Article 6 of the ECHR, both for gatekeepers being regulated and users seeking redress.

59. Consideration should also be given to protected characteristics, as set out in the Equality Act 2010. The internet can empower people from all backgrounds, providing a platform for those not heard elsewhere and a means of connecting with others. However, with these benefits come risks. Several witnesses discussed online abuse and harassment directed against specific groups according to gender, sexuality, race or religion. Addressing this can be challenging. The British Computer Society noted that removing racist content can take longer than content such as nudity which is easier to categorise[70]. Michael Veale, a researcher at University College London, described how automated content moderation systems can discriminate against ethnic minorities through a failure to understand non-mainstream uses of language.[71]

60. Margot James MP, Minister for Digital and the Creative Industries, was concerned that 20% of people with a registered disability have never been online. We share the Government's desire that the benefits of technology should "be shared across society, not for certain groups to benefit while other groups fall behind."[72] This includes the need to address the inequality

65 Written evidence from Her Majesty's Government (IRN0109)
66 Emily Laidlaw, *Internet Gatekeepers, Human Rights and Corporate Social Responsibilities*, PhD thesis (London School of Economics, 2012) p 3
67 Written evidence from the Information Law and Policy Centre, Institute for Advanced Legal Studies (IRN0063)
68 United Nations, *Guiding Principles on Business and Human Rights* (16 June 2011): https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf [accessed 26 February 2019]
69 Q 58
70 Written evidence from BCS, The Chartered Institute for IT (IRN0092)
71 Written evidence from Michael Veale, University College London (IRN0077)
72 Q 196

of experience among those who do use the internet. The UK Safer Internet Centre and Global Partners Digital both raised the difficulties people with low digital literacy or disabilities can have, such as in availing grievance redress mechanisms and understanding terms and conditions.[73] Which?, a consumer group, also reported that vulnerable adults can feel anxious about being 'micro-targeted' and possible harms resulting from the use of sensitive data.[74]

Education and awareness-raising

61. In our report *Growing up with the internet* we recommended that "digital literacy should be the fourth pillar of a child's education alongside reading, writing and mathematics". Digital literacy refers to "the skills to use, create and critique digital technologies" and the knowledge "to critically understand the structures and syntax of the digital world, and to be confident in managing new social norms".[75] The Children's Media Foundation found that digital literacy remains "poor in many audience groups—including children and parents."[76] Dr Paul Bernal of the University of East Anglia agreed that levels of understanding were low but noted that the internet would probably always be "a messy and sometimes confusing place".[77] He advocated that children should "become 'savvy' and encouraged to be sensible, rather than our suggesting that we can make the environment fundamentally safe". However, 5Rights Foundation argue that it is wrong to ask children to "be resilient to a system that does not respect or protect their safety and security".[78]

62. Parents play an important role in mediating children's use of the internet. However, many parents lack the knowledge or confidence to do so effectively. The government could do more to rationalise guidance to make it clearer and more easily accessible. Some of the largest companies support Internet Matters, a website of resources to help keep children safe online.[79] Tech companies which provide online services should take responsibility for providing educational tools and raising awareness, including raising awareness of how their services work and potential harms of using them. However, advice should not be limited to parents and children. Users of all ages can benefit from being better informed. The Northumbria Internet & Society Research Interest Group argued that: "Education and advice should become integrated as part of the online user experience."[80]

63. Many tech companies argued that the response to online harms should focus on improving digital literacy. But digital literacy cannot be the only solution to problems associated with the internet.[81] The most vulnerable people in society are particularly susceptible to online harms, but they are less likely to develop digital literacy.

---

73 Written evidence from Global Partners Digital (IRN0099) and the UK Safer Internet Centre (IRN0061)
74 Written evidence from Which? (IRN0116)
75 5Rights, 'The right to digital literacy': https://5rightsfoundation.com/the-5-rights/the-right-to-digital-literacy.html [accessed 15 February 2019]
76 Written evidence from CMF (IRN0033)
77 Written evidence from Dr Paul Bernal (IRN0019)
78 5Rights, 'The right to digital literacy'
79 Q 104 (Daniel Butler)
80 Written evidence from NINSO (IRN0035)
81 Written evidence from CMF (IRN0033)

Democratic accountability, proportionality and evidenced-based approach

64. A report from Communications Chambers identified the risk of 'regulation by outrage' where in the absence of an effective regulatory framework "outrage, campaigning and lobbying" intensified by media coverage have stimulated *ad hoc* responses to online harms.[82] It is unclear how effective these responses are and they leave "consumers none the wiser about the true risks of online content nor what they have a right to expect from intermediaries". A more strategic approach is therefore necessary.

65. Many witnesses warned about the risks of unintended consequences when introducing regulation which might stifle competition, freedom of expression and information. Dr Paul Bernal advised that regulation needed to be "monitored very closely if a decision is made to regulate. Where regulation is not working or being counterproductive, it needs to be reversed."[83] Regulatory action should therefore be based on evidence. However, in some cases it can take a long time for harm to become apparent by which stage it is too late to react. In cases of high risk it may be appropriate to act to prevent harm before the evidence is conclusive.

66. On the other hand, witnesses criticised the current model self-regulation which encourages platforms to police online harms. Doteveryone said that this lacks "democratic legitimacy as there is little opportunity for the public, civil society and government to have their say on what constitutes a "harm", and where the damage caused by it outweighs the right to freedom of expression." In the final chapter of this report we consider how future regulatory responses should be developed.

Conclusion

67. ***The 10 principles set out in this report should guide the development and implementation of regulation online and be used to set expectations of digital services. These principles will help the industry, regulators, the Government and users work towards a common goal of making the internet a better, more respectful environment which is beneficial to all. They will help ensure that rights are protected online just as they are offline. If rights are infringed, those responsible should be held accountable in a fair and transparent way. With these principles the internet would remain open to innovation and creativity while a new culture of ethical behaviour would be embedded into the design of services.***

82 Mark Bunting 'Keeping consumers safe online: Legislating for platform accountability for online content' Communications Chambers (July 2018): http://static1.1.sqspcdn.com/static/f/1321365/27941308/1530714958163/Sky+Platform+Accountability+FINAL+020718+2200.pdf [accessed 16 January 2019]

83 Written evidence from Dr Paul Bernal (IRN0019)

CHAPTER 3: ETHICAL TECHNOLOGY

Introduction

68. Questions of design are at the heart of how the internet is experienced and regulated. The user experience of a website, search engine or social media platform is defined by the designers of that site. They can influence which posts or images users see, which sites users choose to visit, which news stories they read, and which videos or television programmes they watch. Design affects how privacy and security online are understood, how decisions are made about users by both humans and algorithms, and how users understand these decisions. In short, it affects how technology is used and perceived.

69. Thus, although public concern often focuses on inappropriate content or abusive behaviour, issues around the design of services may be more fundamental.[84] Professor Christopher Marsden said that the internet is "the largest single experiment in nudge regulation that exists".[85] He added:

> "If you want to achieve meaningful results, you have to deal with the way the companies regulate us and persuade them to regulate us differently, which means persuading them to change the way they engineer their software."[86]

70. In this chapter we explore issues arising from design and how they can be better accounted for in regulation. Different user groups may need specific design ethics applied to them. The internet should also cater for adults with specific needs, older people and children of different ages.

Data protection and privacy

71. Privacy and personal data are protected and regulated by an extensive body of law. In May 2018 data protection rights were significantly strengthened by the General Data Protection Regulation (GDPR). This introduced a number of new rights and obligations, as well as reaffirming existing law (see Box 2). The GDPR requires privacy and security to be incorporated in the design of services: "data protection by design and by default".[87] Dr Paul Bernal of the University of East Anglia said that the GDPR "has the potential to provide a good deal of support for individual privacy—but only if it is enforced with sufficient rigour and support."[88]

84 Q 31 (Rachel Coldicutt)
85 Q 1
86 Written evidence from Professor Christopher Marsden (IRN0080)
87 Regulation (EU) 2016/679 of the European Parliament and of the Council 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) (OJ L119/1, 27 April 2016), Article 25
88 Written evidence from Dr Paul Bernal (IRN0019)

Box 2: Selected list of rights under the General Data Protection Regulation

- The right to be informed: an individual must be given certain information about the collection and use of their personal data.
- The right of access: an individual can request to see the personal data held about them.
- The right to rectification: an individual can require incorrect or incomplete information to be amended.
- The right to erasure (also known as "the right to be forgotten"): an individual can request deletion of their personal data and the prevention of its processing in certain circumstances.
- The right to restrict processing: an individual may be entitled to restrict the way their data is processed.
- The right to data portability: an individual may obtain and reuse personal data they have provided to a controller for their own purposes across different services.
- The right to object: an individual can object to the processing of their personal data in certain circumstances.
- Rights in relation to automated decision making and profiling: including safeguards to prevent potentially damaging decisions being taken without human intervention.

72. As the GDPR came into force in May 2018, it is too early to judge how effective it will ultimately be. Many witnesses agreed that the GDPR was beneficial and that it would improve the visibility of data protection. However, the scale of concerns are considerable. The Children's Media Foundation told us that "The collection and exploitation of user data is an ongoing concern. The implications for children are even more significant, as they may not understand the long-term implications of sharing data or have the capacity to make informed decisions."[89]

73. The Data Protection Act 2018 requires the Information Commissioner's Office to develop an Age Appropriate Design Code to set out requirements for online services "likely to be accessed by children". This will create a specific provision in UK law which reflects recital 38 of the GDPR, which states that "children merit specific protection". This provision requires those processing children's data to respect children's rights as set out in the UN Convention on the Rights of the Child, and to take account of their age and development stage.

74. A draft of the Code is expected to be published soon and to include provisions requiring: high privacy by default, geolocation off by default, the upholding of published age-restrictions, content and behaviour rules by online services, preventing auto-recommendation of content detrimental to a child's health and wellbeing, and restrictions on addictive features, data-sharing, commercial targeting and other forms of profiling. The Code must be laid before Parliament before November 2019 and the enforcement penalties available to the regulator mirror those of the GDPR including fines of up to 4% of global turnover.

89 Written evidence from CMF (IRN0033)

Data and the digital economy

75. Personal data is vital to the business model which dominates the digital economy. Dr Jennifer Cobbe and Professor John Naughton described how Google developed this model, which came to be known as 'surveillance capitalism'. They explained that Google provided a search service which was free to use. In return it analysed phrases which a user entered into its search box (a) to make inferences to predict the user's wants and (b) to sell to other companies "the opportunity to target those users with advertising based on this prediction".[90] This business model has made Google one of the world's richest companies, first through targeted advertising and later "by surveilling user activities elsewhere so as to predict behaviour more generally and maximise opportunities for profit in many other contexts".

76. Conventional wisdom in the industry is that the more data that a business can gather from different sources the more accurate its analyses. This position forms the bedrock of the modern data science of big data analytics. As a result data is extremely valuable and companies strive to gather and trade in data. Some of these data are supplied directly by the user, but tech companies also gather data about user behaviour by monitoring users' online activities. For example, in the case of Facebook such 'behavioural data' include:

> "Data on which pages have been 'Liked' by a given user; on which posts have been viewed by a given user; on identifying other users with whom a given user has interacted (including how many times, when, and for how long); on which posts, images, or videos have been seen or watched by a given user (including how many times, when, and for how long); on which advertisers a given user has interacted with (including how many times, when, and for how long)."[91]

77. Internet businesses have accrued massive volumes of data, so called big data, which they cannot process efficiently using traditional digital applications. As a result, many are turning to machine learning to analyse these datasets. Machine learning is a form of artificial intelligence which learns from experience and through this process maximises its efficiency at any task. There are many applications for machine learning: it is already used to detect instances of credit card fraud and it will increasingly be used for healthcare.[92] Not all big data are generated online, but the internet is a major source, giving large tech companies a competitive advantage.

78. The Northumbria Internet & Society Research Interest Group (NINSO) told us that the Internet of Things posed additional risks: "As more and more devices become 'connected', and more and more businesses collect data, there is the potential for data protection standards to degrade as a result of hacks, mishaps or simple complacency."[93]

79. **As organisations, including financial and health services providers, increasingly perceive individuals as the aggregation of data gathered about them (sometimes called their 'data selves'), it is essential that data be accurate, up-to-date and processed fairly and lawfully, especially when processed by algorithm. While the GDPR and the Data Protection Act 2018 provide valuable safeguards, including**

90 Written evidence from Dr Jennifer Cobbe and Professor John Naughton (IRN0031)
91 *Ibid.*
92 Written evidence from the Royal Society (IRN0084)
93 Written evidence from CMF (IRN0033)

subject access rights to ensure that data are accurate and up to date and the right to opt out from purely automated processing, there are weaknesses in the regime. For example, a subject access request does not give subjects automatic access to behavioural data generated about them because it is deemed to be the property of the company that acquired it.

80. ***Users of internet services should have the right to receive a processing transparency report on request. In a model similar to a subject access report under the GDPR users should have the right to request a data transparency report from data controllers showing not only what data they hold on the data subject (which is the currently the case under the GDPR) but also what data they generate on them (behavioural data) and any behavioural data obtained from third parties, including details of when and how they are obtained.***

81. ***Data controllers and data processors should be required to publish an annual data transparency statement detailing which forms of behavioural data they generate or purchase from third parties, how they are stored and for how long, and how they are used and transferred.***

Capturing attention

82. The incentive to seek and retain users' attention—to gather more of their data and to target them with advertising—is a key attribute of the 'surveillance capitalism' business model. Professor John Naughton explained that companies deploy techniques which they have learned from applied psychology. The services are deliberately designed to be addictive. As a result:

> "Somebody goes on to Facebook to check a picture from a family member and an hour later they wonder why they are still there. They are still there, because it is beautiful software that is very cleverly designed."[94]

83. Subforum, a tech design and research organisation, described one psychological technique used, 'variable rewards', which plays off human responsiveness to "unpredictable rewards that are offered on a variable, non-fixed schedule", which increase the level of dopamine produced by the brain.[95] Subforum compared this technique to a slot machine:

> "You put in a coin. You pull the lever. Do the three shapes all match? Nope? OK, pull again. How about this time? That's the hook: the anticipation of getting a reward (whether or not we actually get one) increases the dopamine levels in our brains, which compels us to keep doing the thing that got us a reward before."

Table 1 provides examples of how platforms use this technique.

94 Q 86
95 Written evidence from Subforum (IRN0013)

Table 1: Variable rewards: examples

Behaviours the platform wants to reinforce	Variable reward offered
Scrolling Facebook's news feed or pull to refresh on Twitter	An interesting or amusing update
Posting, commenting or responding	Gratifying likes and other responses
Checking messages or notifications	Receipt of inbound communication

Source: Written evidence from Subforum (IRN0013)

84. Margrethe Vestager, the EU's Competition Commissioner, said these techniques "are designed to create a form of addiction".[96] Professor Chris Marsden, professor of internet law at the University of Sussex, said of Margrethe Vestager's remark, "She pointed out that we allow 13 year-olds to use these platforms perfectly legally in the UK—it differs in different European countries—in a way that we have decided not to do to for alcohol, tobacco or other types of addiction. Those are her words rather than mine. The world is built on addictive substances, from tea and sugar to everything else, but we should be aware that we are doing this."[97]

85. Professor Sonia Livingstone of the London School of Economics and Political Science suggested that human interaction with technology could be described as "a kind of compulsion and fascination, rather than addiction".[98] She argued that efforts should be made to intentional use, particularly among children: "It is all about the defaults and finding ways not to maximise eyeballs." Professor Livingstone predicted that we may be at the early of stage of a differentiation of business models. She suggested that businesses should be required to use "notifications, endless reminders and pop-up reminders to say, occasionally, 'Have you have been on too long?'"[99]

86. Tristan Harris, a former employee of Google, has championed a backlash to the surveillance capitalism model and has founded the Center for Humane Technology to raise awareness of the need for ethical design. He has warned: "With design as it is today, screens threaten our fundamental agency. Maybe we are 'choosing', but we are choosing from persuasive menus driven by companies who have different goals than ours."[100]

87. ***Digital service providers (such as hardware manufacturers, operators of digital platforms, including social media platforms and entertainment platforms, and games developers) should keep a record of time spent using their service which may be easily accessed and reviewed by users, with periodic reminders of prolonged or extended use through pop-up notices or similar. An industry standard on reasonable use should be developed to inform an understanding of what constitutes prolonged use. This standard***

96 'EU Commissioner Margrethe Vestager: Facebook is designed to create addiction—like tobacco and alcohol' *Berlingske* (7 April 2018): https://www.berlingske.dk/internationalt/eu-commissioner-margrethe-vestager-facebook-is-designed-to-create-addiction-like [accessed 5 December 2018]

97 Written evidence from Professor Christopher Marsden (IRN0080)

98 Q 75

99 Q 75 (Professor Sonia Livingstone)

100 Tristan Harris, 'Tech Companies Design Your Life, Here's Why You Should Care' (7 March 2016): http://www.tristanharris.com/essays/ [accessed 26 February 2019]

should guide design so that services mitigate the risk of encouraging compulsive behaviour.

Algorithmic curation

88. Online platforms have become the primary interface for internet users, helping them navigate vast volumes of content and sifting for what is most relevant. Dr Shehar Bano explained: "The human brain has limited capacity for processing information and the time span for which their interest is sustained; therefore the order and format in which information is presented to users is crucial."[101] Online platforms use algorithms (see Box 2) 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.

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: Andrew Smith, 'Franken-algorithms: the deadly consequences of unpredictable code' The Guardian (30 August 2018): https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger *[accessed 11 February 2019]*

89. Although personalisation is often said to optimise customer interaction, the Internet Society noted that it was not clear what was being optimised:

> "Is the content on the platform being shaped to provide content that will increase customer wellbeing, or is it shaped to maximise time spent on the platform and/or number of interactions with adverts even if this is to the detriment of the user?"[102]

90. Personalisation of content determines what people see online. Robert Colvile, Director of the Centre for Policy Studies, said that the algorithms tend to "intensify and radicalise your experience".[103] He gave the example an experience of "liking" content from UKIP on Facebook, which instantly returned content for the National Front and the BNP. Ultimately, these algorithms can create 'filter bubbles' where users see only information related to their preferences and 'echo chambers' where their beliefs are reinforced by like-minded or more extreme content. These have been linked to the spread of so-called 'fake news'. Dr Stephann Makri explained that "they can create 'distortions' in information flow (e.g. through misinformation, disinformation) that can undermine the fundamental British value of democracy".[104]

101 Written evidence from Dr Shehar Bano (IRN0114)
102 Written evidence from Internet Society UK Chapter (IRN0076)
103 Q 53
104 Written evidence from Dr Stephann Makri (IRN0113)

91. Personalisation may be based on profiling, whereby algorithms analyse a person's data to identify characteristics about the person such as their interests, personal preferences, health, reliability, behaviour and location.[105]

92. Platforms tend to keep the details of their algorithms secret on the grounds of commercial sensitivity and concern that people might seek to 'game' them. Our witnesses generally agreed that full transparency about the computer code containing algorithms would not help users to understand how they work.[106] Microsoft argued that even a detailed understanding of an algorithm would not be useful in understanding its outputs, which were derived from input data from other users.[107]

93. However, the lack of transparency has caused concern. Dr Bano described algorithms as "opaque" and was concerned that they may be "biased, and at times outright discriminatory".[108] Algorithmic bias may be caused by input data which is biased. This may be a particular problem with machine-learning algorithms which are programmed to spot patterns in large amounts of data. Professor John Naughton said, "Most datasets are not clean; they are coloured in one way or another with all kinds of unconscious and other biases."[109] He said that many people not involved with developing this technology were "dazzled" by it. This included members of the Government and industry who should be more sceptical.

94. The lack of transparency may conceal instances where algorithms are designed to act in ways which are contrary to the user's interests. For example, Margot James MP, the Minister for Digital and the Creative Industries, told us that some airlines' websites use an algorithm which identifies passengers with the same surname and deliberately allocates them seats apart from each other. The airlines can then charge passengers to change their seat to be with their family.[110]

95. Many witnesses called for greater transparency. The Children's Media Foundation proposed "the publication of the editorial guidelines and values that underpin them".[111] NINSO recommended that "Algorithms should also be auditable and audited frequently by an independent body."[112] It is not always possible to audit the technical content of algorithms, as they can rewrite themselves beyond the understanding of their creators. However, impact-based assessments are possible. These consider the decisions algorithms make rather than the processes by which they make them. The Information Commissioner's Office already carries out impact audits for Data Protection.

96. The Information Commissioner's Office told us that the Commissioner had started to work with the Turing Institute to produce a framework for explaining algorithmic processes and decisions. They stressed the need for transparent explanations of both data inputs and how data outputs are used and also the difficulties of engaging the average user with technical information.

---

105 Article 4 of the GDPR defines 'profiling'.
106 Written evidence from Dr Paul Bernal (IRN0019)
107 Written evidence from Microsoft (IRN0085)
108 Written evidence from Dr Shehar Bano (IRN0114)
109 Q 90
110 Q 188
111 Written evidence from CMF (IRN0033)
112 Written evidence from NINSO (IRN0035)

97. Katie Donovan, UK Public Policy Manager at Google, said: "We have developed our own AI principles to ensure that we use them ethically, that we have transparency about them and that we use them for social good."

98. The Government has set up the Centre for Data Ethics and Innovation to provide independent, expert advice on measures to ensure safe and ethical innovation in data-driven and AI-based technologies. Following a consultation on the role and objectives of the centre, the Government said that it will "agree and articulate best practice" for companies using data.[113]

99. ***The Information Commissioner's Office should set out rules for the use of algorithms based on the principles set out in chapter 2. The ICO should be empowered to conduct impact-based audits where risks associated with using algorithms are greatest and to require businesses to explain how they use personal data and what their algorithms do. Failure to comply with the rules should result in sanctions.***

100. ***The ICO should also publish a code of best practice informed by the work of the Centre for Data Ethics and Innovation around the use of algorithms. This code could form the basis of a gold-standard industry 'kitemark'.***

101. ***Data subjects should be given the right to request a statement from a data processor explaining how, if applicable, algorithms are used to profile them, deliver content or drive their behaviour.***

Terms of service and information

102. The GDPR prohibits personal data from being processed unless they are specifically permitted under one of six lawful bases.[114] Often online platforms rely on 'consent' as the legal basis for processing data. The GDPR has strengthened this legal basis by requiring that consent be freely given, specific, informed and unambiguous. Consent must be uncoupled from other written terms of service.

103. The GDPR requires organisations to explain how they use personal data, whether or not consent is the basis for processing. It includes the right to be informed.[115] The Information Commissioner's Office (ICO) told us:

> "Essentially, the GDPR 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 (this is not exhaustive)."[116]

104. The ICO has published guidance on how organisations can achieve this and encourages them "to be innovative in providing this information—embedding and layering the information as part of the design process, not just in one long notice."[117] It also argued that openness and transparency around data use were important not only for complying with the law but also "to engender trust and improve relationships with … customers".

113 Written evidence from Her Majesty's Government (IRN0109)
114 Article 6. The legal bases are consent, contract, legal obligation, vital interests, public task and legitimate interests.
115 This is mainly covered by articles 13 and 14 of GDPR.
116 Written evidence from ICO (IRN0087)
117 Written evidence from ICO (IRN0087)

105. Nearly all our witnesses said that there was a lack of understanding about how data were used. Information provided in terms of service did not help. The Children's Media Foundation said that terms of service and information about data use were not easy to find and were written in a way that is "impenetrable for most people—especially children".[118] Which? argued that businesses should "provide consumers with more transparency on the impacts of data use and the Government and others must work together to understand these impacts".

106. The Royal Society said that relying on information alone was problematic because of what it called the 'transparency paradox': consent requires information to make it meaningful but "anything too long or complex is unlikely to be broadly understood or read". On the other hand summarising information to make it more digestible "often discards the details that people care about".[119] The Royal Society concluded: "It is unreasonable to expect an individual to keep track of what data is collected about them and understand how it will be used, and therefore to give meaningful, informed consent."

107. NINSO, on the other hand, argued that more could be done to ensure that terms of service and privacy policies were clear and easy to understand:

> "Videos and infographics are goods, ways to convey complex information such as this. The keywords should be in bold. The text should be readable, i.e. coefficient 8 Flesch-Kincaid [a reading standard] … Ultimately, the information should be delivered with a level of clarity that is sufficient to enable users to make an informed choice."[120]

108. ***Terms of service must be written in a form which is clearly accessible and understandable to internet users. Alongside terms of service statements a 'plain English' statement should be published which sets out clearly and concisely the most relevant provisions. These may make use of infographics or video statements where appropriate.***

109. ***Where children are permitted to access or use a service age-appropriate terms and conditions must be provided. These should be written in language clearly understandable to children of the minimum age allowed on the platform.***

110. Terms of service are often on an 'all or nothing' basis.[121] NINSO explained:

> "There is a substantial power imbalance between users and the operators of online platforms. Users frequently have no capacity to moderate terms but instead have the 'choice' of accepting all terms (which might include giving away significant amounts of personal data) or simply not using the service. This is not providing a real choice."[122]

As a result, according to Which?, many consumers "choose not to engage because it does not feel worthwhile".[123]

---

118 Written evidence from CMF (IRN0033)
119 Written evidence from the Royal Society (IRN0084)
120 Written evidence from NINSO (IRN0035)
121 Written evidence from the Internet Society UK Chapter (IRN0076)
122 Written evidence from NINSO (IRN0035)
123 Written evidence from Which? (IRN0116)

111. Dr Paul Bernal argued that what platforms do with data is more important than the question of what information they should provide:

> "People will generally simply scroll through whatever information is provided and click 'OK' at the end. Regulation of the use of personal data based on information and 'consent' is not sufficient: it is more important to set clear and strong rules about what is and is not allowed."[124]

112. Others argued that users should be given greater control. For example, NINSO suggested users should be given greater control of their data by having the option to pay for a premium service which does not collect data.

113. Jamie Bartlett said that the default setting of whether data are immediately shared or not probably has more effect than any other issue of design.[125]

114. ***Maximum privacy and safety settings should be included in services by default. The Information Commissioner's Office should provide guidance requiring platforms to provide greater choice to users to control how their data are collected and used.***

115. ***Regulators must ensure that terms of service are fair and must bring enforcement action against organisations which routinely breach their terms of service.***

Ethical by design

116. Ethical issues should be considered and addressed during the design process, reflecting concepts such as 'rights by design', 'privacy by design', 'security by design' and 'safety by design'. These problems are directly associated with design and so it is more effective to consider them early than to react to problems later on. Dr Stephann Makri told us: "This approach is far preferable to a box-ticking exercise where designers try to demonstrate meeting ethical design guidelines or regulations without considering ethical design from the outset."[126]

117. Doteveryone argued that developers should conduct "independent impact assessments at an early stage of a technology's lifecycle". It also argued that the 'precautionary principle' could be applied to internet technology:

> "This principle is applied in situations where there are reasonable grounds for concern that an activity is causing harm, but the scale and risk of these issues is unproven. The onus is then on organisations to prove that their practices are safe to a reasonable level."[127]

118. Dr Ewa Luger said that the culture of the tech industry needs to change. Currently "people do not set out to do harm, but they do not know what the alternative is. Responsible innovation is not embedded in the teaching of computer science, machine learning or AI."[128] Dr Luger recommended investment in higher education and embedding ethics into teaching.

119. ***Design principles and standards are a normal part of business life across all sectors. Establishing and enforcing standards***

---

124 Written evidence from Dr Paul Bernal (IRN0019)
125 Q 53
126 Written evidence from Dr Stephann Makri (IRN0113)
127 Written evidence from Doteveryone (IRN0028)
128 Q 99

that would meet the 10 principles would help to reduce harms to users and society. We recommend that regulation should follow the precautionary principle to ensure ethical design while also recognising the importance of innovation and entrepreneurship.

120. ***We recommend that the ethical approach outlined in our 10 principles should be embedded in the teaching of all levels of computer science. The Government should promote and support this. The Centre for Data Ethics and Innovation will also have a role in providing guidance which can be incorporated into teaching, as well as educating users on the ethics and risks of the internet.***

CHAPTER 4: MARKET CONCENTRATION

Introduction

121. Google, Amazon, Facebook and Apple (the 'GAFAs') are sometimes known as the 'Big Four' as they have grown at remarkable rates.[129] Microsoft is nearly 45 years old and remains a major presence online. Dr Shehar Bano said: "Over time the internet has evolved into an ecosystem dominated and controlled by a small number of large online platforms—resulting in centralisation and monopolies."[130] These platforms operate at an unprecedented scale. All five have a market value of over $400 billion. Facebook alone has 2.7 billion active monthly users across its services.[131] Google argued that the position of these five companies "does not reflect a lack of innovation in that space or a certainty over what will happen going forward. We thrive on innovation and feel we are operating in a very competitive environment."[132] Table 2 shows the major services that these companies provide across several different digital markets (bold indicates the biggest services in the market).

122. The Government told us that the Department for Business, Energy and Industrial Strategy is reviewing "the UK's competition tools in the context of digital markets to make sure the powers are effective in responding to the new digital challenges."[133] This is part of a wider competition law review. The review will consider "whether the current competition regime is sufficiently equipped to respond to the rapid changes taking place to business models in the digital economy. It is also seeking evidence on how it should address platforms, agglomeration, algorithms and the consolidation of competitors." On 2 August 2018 the Government appointed Professor Jason Furman to lead an expert panel for this review.[134]

123. Dr Damian Tambini told us that the public-policy debate around internet regulation had come about "because these info platforms now play a crucial infrastructure role in most of our lives. Therefore they are too important and powerful to ignore."[135]

Competition and digital markets

124. Competition law prohibits abuse of market dominance. While dominance by itself is not prohibited, dominant businesses have a responsibility to ensure that their conduct does not distort the market. Professor Pinar Akman did not think that "dominance and market power on their own are a cause for concern … What would be a cause for concern is if companies engage in conduct that is anticompetitive, distorts competition and ultimately harms consumers."[136] Size might be a "result of superior efficiency and being better than one's rivals".

129 Written evidence from BILETA (IRN0029)
130 Written evidence from Shehar Bano (IRN0114)
131 '"2.7 billion people can't be wrong": Here's what Wall Street is saying about Facebook earnings' *Markets Insider* (31 January 2019): https://markets.businessinsider.com/news/stocks/facebook-stock-price-earnings-revenuewall-street-2019-1-1027913555 [accessed 5 February 2019]
132 Q 177
133 Written evidence from Her Majesty's Government (IRN0109).
134 HM Treasury, 'Former Obama advisor to examine digital competition in the UK' (2 August 2018): https://www.gov.uk/government/news/former-obama-advisor-to-examine-digital-competition-in-the-uk [accessed 26 February 2019]
135 Written evidence from Dr Damian Tambini (IRN0101)
136 Q 84

Table 2: Digital markets

	Google	Facebook	Apple	Microsoft	Amazon
Search	**Google**			Bing	Own product search
Mail	**Gmail**		iCloud mail	**Outlook**	
Messaging	Hangouts	**Messenger WhatsApp**	iMessage	MSN Messenger, Yammer	
Maps	**Google Maps, Google Earth, Waze**		**Apple Maps**	Bing Maps, StreetSide	
Social networking	Google+	**Facebook, Instagram**		LinkedIn	Twitch/ Goodreads
Cloud	**Drive, Google Cloud Platform**		iCloud	Azure, OneDrive, SkyDrive	**AWS, Amazon Drive**
Autonomous vehicles	Waymo, Android Auto		AppleCar (software)	Software investment	
Voice-activated assistants	**Google Home**	Messenger Bots	**Siri**	Cortana, others	**Echo/Alexa**
Advertising	**AdWords, AdSense, DoubleClick, Tag Manager**	**In News Feed Audience Network**		Bing Ads	Amazon Advertising

Source: Diane Coyle, 'Practical competition policy implications of digital platforms' March 2018, p 9: https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Practical_competition_policy_tools_for_digital_platforms.pdf *[accessed 2 January 2019]*

125. Regulators generally assess abuse of market dominance on a case-by-case basis after undertaking a detailed analysis of the market concerned. First a specific market must be identified in which a company has a dominant position.[137] For the purposes of competition law, this can be a complex exercise taking account of demand-side and supply-side substitutes, so the question would always be whether the company concerned holds a dominant position in a relevant market. Javier Ruiz Diaz, Policy Director, Open Rights Group, said, "One of the fundamental problems with competition law is that we do not have a good definition of what the market is … There is no social media [or search engine] monopoly category".[138] Where there are several strong players it is more difficult to establish dominance of a single firm and collective dominance is difficult to establish.

126. Competition law focuses on maximising competition within markets to avoid economic detriment to consumers, using the 'consumer welfare standard'—an assessment of the individual benefits derived from consumption. Traditionally, in the case of mergers for example, the analysis would consider issues such as whether efficiencies gained by dominant or merging companies would be passed on to consumers in the form of lower prices, or whether it would still be possible for new entrants to break into the market.[139]

127. The Competition and Markets Authority (CMA), the UK regulator for competition and consumer law, told us that it did not intervene in markets unless the intervention:

    - Was proportionate and targeted specifically to address identified concerns
    - Did not inadvertently favour incumbents and large businesses by imposing undue compliance costs on small businesses or new entrants
    - Minimised competition distortions and did not impede innovation
    - Created a clear institutional mechanism to monitor and review the impact of regulations to ensure that such regulations remain effective and targeted.[140]

128. Witnesses were concerned that traditional analyses have not been effective in responding to digital platforms. The CMA conceded that the online economy posed challenges to the use of its powers, such as:

    - The cross-border nature of online markets
    - The presence of strong network effects which resulted in the rapid acquisition of significant market shares by a small number of dominant companies
    - The ability of businesses to use data and algorithms to differentiate between customers, which created efficiencies but also increased the

137 Diane Coyle, 'Practical competition policy implications of digital platforms' (March 2018): https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Practical_competition_policy_tools_for_digital_platforms.pdf [accessed 2 January 2019]

138 Q 26

139 Diane Coyle, 'Digital platforms force a rethink in competition theory', Financial Times (17 August 2017): https://www.ft.com/content/9dc80408–81e1-11e7-94e2-c5b903247afd [accessed 2 January 2019]

140 Written evidence from the Competition and Markets Authority (IRN0100)

risk of market abuse: the CMA had found that algorithms could have the same effect as price-fixing agreements

- The fast-moving nature of online markets meant that enforcement can come too late to address the harms of anti-competitive practices or restore competition.[141]

129. In our report *UK advertising in a digital age* we found that the digital advertising market was opaque and dominated by Google and Facebook. We called on the CMA to conduct a 'market study'—a broad 'health check' of a market—to see how it was operating and to ensure that it was working fairly for consumers and businesses.

Network effects and market share

130. Many witnesses noted that online platforms benefit from network effects. This is where the value of a service to users increases the more users it has. For example, telephones are useful only if other people have them; they are more useful as the number of other users increases. For online platforms this can lead to a 'winner takes all' outcome. Doteveryone warned: "Many tech companies are loss-making until they reach a critical mass of users. After this point network effects … often mean a platform can quickly become dominant in a short period of time."[142]

131. As noted in the previous chapter, large online platforms control large datasets, which give them a competitive advantage. Professor Lilian Edwards told us that can lead to a virtuous circle for incumbent platforms which can build proprietary data siloes.[143] The Open Data Institute were particularly concerned by the control that platforms have of large data assets and of "the attention of users who help to maintain and improve those data assets through their use of the online platform's services. This control limits how that data is used, reducing innovation and competition."[144]

132. As noted above, the largest online platforms operate across a range of markets. The British Computer Society told us that some companies sold products and services at a loss in one market to generate data that were valuable to them in other markets, as with the Amazon Echo device. It added: "The effects of combining data across different markets, and their influence on competition and consumer welfare, are not yet clear."[145]

133. Many witnesses from the tech industry argued that, notwithstanding the size of online platforms, digital markets remained dynamic and innovative. Facebook told us that it was an industry "where stakeholders have an enormous amount of choice and there are constant new opportunities. We are committed to seeing a healthy ecosystem which will continue to flourish."[146]

134. The Entrepreneurs Network and Adam Smith Institute argued consumer choice was not limited by the size of online platforms because they can "use multiple social networking services all at once (multi-homing) (e.g. Facebook, Snapchat, Instagram, Twitter, Tumblr, and Slack)".[147] The largest

141 Written evidence from the Competition and Markets Authority (IRN0100)
142 Written evidence from Doteveryone (IRN0028)
143 Written evidence from Lilian Edwards, Professor of eGovernance (IRN0069)
144 Written evidence from the Open Data Institute (IRN0073)
145 Written evidence from Doteveryone (IRN0028)
146 Written evidence from Facebook (IRN0098)
147 Written evidence from the Entrepreneurs Network and Adam Smith Institute (IRN0070)

online platforms offered intense competition to one another, given their pattern of venturing into markets outside their core business. For example, Google "handles 75% of global search requests but competes intensely in other markets such as the more lucrative product search markets (where Amazon has greater market share)."[148]

135. Witnesses said that online platforms could not take their current market shares for granted in the face of future competition. The Entrepreneurs Network and Adam Smith Institute noted that "MySpace was previously seen as an unassailable monopoly before Facebook eventually won out."[149] The British Computer Society said that, while there was a tendency for monopolies to develop online, it was not realistic at this early stage of its history to expect the internet to mature.[150]

136. The Entrepreneurs Network and Adam Smith Institute cited tech companies' heavy investment in research and development as evidence of this dynamic competition: "For instance, in 2014 Facebook spent $2.1bn on research and development representing 21% of its total revenue. By way of comparison, in the same year research-intensive pharma companies such as Roche, Novartis, or Pfizer did not spend more than 19% of total revenue on R&D."[151] However, it is unclear how far research and development has benefitted tech companies' customers.

137. The British and Irish Legal Education and Technology Association cautioned that "a case can be made that it is not the GAFAs … that one should be concerned about. China's internet giants Baidu, Alibaba and Tencent (the BATs) are now taking the lead, interacting with customers beyond China's boundaries and posing a risk to the global financial marketplace. In fact, the BATs seem to be much more active and dynamic than the GAFAs."[152]

138. However, Professor Patrick Barwise believed that the position of the GAFAs had probably become entrenched because "the economic properties of platform markets are such that normal processes of competitive creative destruction may not work: data driven dominance enables social media to become entrenched and see off competitive entrants."[153]

Cross-subsidisation and intermediation power

139. The two-sided nature of intermediaries allows them to shift costs from the demand to the supply side. Consumers may therefore benefit from free or discounted goods and services. Amazon told us this sort of discounting was "just retailing."[154] However, because of network effects both suppliers and consumers may be effectively locked-in to using the services of large intermediaries. Javier Ruiz Diaz of the Open Rights Group said: "Anyone who has dealt with public procurement on Oracle has horror stories about the vendor lock-in that Oracle imposes on people."[155]

148 Written evidence from the Entrepreneurs Network and Adam Smith Institute IRN0070)
149 Written evidence from the Entrepreneurs Network and Adam Smith Institute (IRN0070)
150 Written evidence from BCS, the Chartered Institute for IT (IRN0092)
151 Written evidence from the Entrepreneurs Network and Adam Smith Institute (IRN0070)
152 Written evidence from BILETA (IRN0029)
153 Written evidence from Dr Damian Tambini (IRN0101)
154 Q 203
155 Q 26

140. The British Computer Society provided another example of this 'lock-in' effect and the high costs associated with switching services. Amazon Web Services provides a computing service for app-developers which involves "software teams writing code to directly interface with the Amazon Service. To move that away from Amazon, would likely turn into a multi-year project of re-writing a significant amount of an application or service, while being at the mercy of Amazon changing things in the interim. Ultimately, there is a danger of companies being beholden to one supplier, as there is not an alternative platform that people could use."[156]

141. The Law Society of Scotland said that there was a danger where an operator of a marketplace platform was a goods seller:

> "This can manifest itself in a number of ways which centre around the ability to collect and manipulate data … a platform sells a particular category of consumer goods. It collects data on the preferences of those consumers which it can use to predict market trends. But it can also use that data to identify the best-selling products in that category at the current time … From a consumer perspective, this can lead to a reduction in the range of available products."[157]

142. Heike Schweitzer, a Professor of Law at Humboldt-Universität Berlin, has recommended that 'intermediation power' should be recognised as a source of dominance. He described this as:

> "the power of platform intermediaries when other firms depend on their services for access to sales and procurement markets. Whether such platforms enjoy market power should not depend on whether the platform's activity is qualified as 'providing intermediation services to suppliers' or 'demanding products or services on behalf of buy-side customers.' The platform's market power must be evaluated based on its concurrent roles for the different market sides that it brings together."[158]

Mergers and takeovers

143. Large tech companies have been active in acquiring smaller, innovative start-ups. For example, Google has acquired more than 200 start-ups, including DeepMind, since 2001. Antony Walker of techUK said that the founders of many businesses aspire for them to be bought, and in his view there was nothing wrong with that.[159] Some said that they were likely to take an ever larger share of the 'smart' economy and even banking.[160]

144. Some acquisitions can move these companies into unexpected new markets—most notably Amazon's purchase of Whole Foods Market. The British Computer Society said that "With many services and sectors yet to be fully digitalised, there are concerns that large tech companies will gain an unfair advantage in emerging online markets."[161] Professor Pinar Akman warned

156 Written evidence from BCS, the Chartered Institute for IT (IRN0092)
157 Written evidence from Law Society of Scotland (IRN0057)
158 Heike Schweitzer, 'Modernising the law on abuse of market power' (12 October 2018): https://www.law.ox.ac.uk/business-law-blog/blog/2018/10/modernising-law-abuse-market-power [accessed 26 February 2019]
159 Q 49
160 Written evidence from BILETA (IRN0029)
161 Written evidence from Doteveryone (IRN0028)

that anti-competitive mergers between companies which do not appear to be competitors can escape proper scrutiny.[162]

145. The nature of digital markets poses a problem in applying traditional competition law on mergers and takeovers. The CMA acknowledged a global debate as to whether "authorities' consideration of such mergers has had adequate regard to the advantage that incumbents enjoy or have been too optimistic about the prospect of new entrants disrupting the status quo."[163]

146. There was concern that leading tech companies could buy up potential competition before it could grow. Alex Hern of *The Guardian* told us Facebook's acquisition of Instagram was perhaps the biggest recent failure of regulation. Instagram was probably the greatest risk to Facebook's monopoly, although it was not providing exactly the same service: "It was slicing off a part of Facebook that people engage with very strongly, which was the photo-sharing part, and creating a social network that could quite healthily run parallel to Facebook."[164]

147. Dr Andrea Coscelli, Chief Executive of the Competition and Markets Authority, discussed the advantage of a public interest type test for digital mergers. He noted that there were three public interest categories for mergers: "One is media plurality, which was used in the context of the Fox-Sky review; the second is national security; and the third is financial stability. Parliament could add a fourth category, say, the creation of data monopolies."[165] He noted that there would be advantages and disadvantages to such a policy. On the one hand, it would create uncertainty around the acquisition of companies which might discourage foreign direct investment. On the other, it would give the CMA greater flexibility to make a judgement in the public interest. Whereas at present case law and the law on consumer welfare might prevent the CMA from intervening in an acquisition even if it were concerned about the accumulation of too much data by a platform.

148. A similar point was made by Dr Orla Lynskey "we should be considering whether or not to use tools that are parallel or complementary to competition tools, such as the public interest test in the context of mergers, to assess that type of transaction. That type of test is currently used primarily in the context of media mergers, but we might be able to make some sort of analogy with the data protection context and say that the economic outcome of the transaction is not the sole consideration."[166]

149. ***Mergers and acquisitions should not allow large companies to become data monopolies. We recommend that in its review of competition law in the context of digital markets the Government should consider implementing a public-interest test for data-driven mergers and acquisitions. The public-interest standard would be the management, in the public interest and through competition law, of the accumulation of data. If necessary, the Competition and Markets Authority (CMA) could therefore intervene as it currently does in cases relevant to media plurality or national security.***

162 Q 84
163 Written evidence from the Competition and Markets Authority (IRN0100)
164 Q 160 (Alex Hern)
165 Q 140
166 Q 85

Price and consumer welfare

150. The emergence of online platforms which do not charge for access to their services (while collecting user data) poses a challenge to traditional notions of the consumer welfare standard, which tends to focus on price.

151. Doteveryone said that platforms selling products and services pose a challenge if they "deploy variable pricing and it can be hard to gauge where this practice is fair and where it's discriminatory. And on marketplace platforms, the price paid by a seller may differ from the amount received by a buyer and competition regulators also need to consider if all sides of this dynamic are treated fairly."[167]

152. Dr Damian Tambini said:

> "Consumer interests are often constructed in narrow terms and in particular in relation to price. Lina Khan points out in her excellent essay that Amazon's long-term strategy of achieving market dominance through low price, while sacrificing short and medium term profits has had the additional benefit to Amazon of providing a good deal of immunity from competition law as it appears to regulators that Amazon's low prices indicate the degree of consumer benefit."[168]

153. Amazon's Director of Public Policy, UK & Ireland, told us: "I do not think for a second that we have any interest in taking out competitors. That is not how it works."[169]

154. Price is not the only consideration in undertaking the consumer welfare test. After all, users pay for 'free' services with their attention which generates data and advertising revenue. The summary of the European Commission decision on the Google Search (Shopping) case, in which Google was fined €2.4 billion, states "The conclusion holds notwithstanding the fact that general search services are offered free of charge."[170] Professor Coyle, however, argued that "Although competition guidelines often pay lip service to quality and other characteristics as features of competition, in practice there is focus on price as it is definitionally crisp and easier to measure."[171] She noted that the Competition and Markets Authority Merger Assessment Guidelines refer almost entirely to price.

155. On consumer detriment unrelated to price, many witnesses were concerned about restriction of consumer choice and lack of motivation for improvement. Sky noted a European Commission review which found the following problems which might not exist if consumers could switch services more easily: "unexplained changes in terms and conditions without prior notice; lack of transparency related to the ranking of goods and services; unclear conditions for access to, and use of, data collected by providers; and a lack of transparency regarding favouring of providers' own competing services."[172]

---

167 Written evidence from Doteveryone (IRN0028)
168 Written evidence from Dr Damian Tambini (IRN0101)
169 Q 203
170 Summary of Commission decision of 27 June 2017 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement, (OJ C9/11, 12 January 2018)
171 Diane Coyle, 'Practical competition policy implications of digital platforms' March 2018: https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Practical_competition_policy_tools_for_digital_platforms.pdf [accessed 2 January 2019]
172 Written evidence from Sky (IRN0060)

The British Computer Society explained that there are difficulties with predicting this: "There have never previously been so few companies with such overarching control of global communication and data. The main concern is that some platforms now control such an amount of critical infrastructure and communication systems that it stops alternatives from ever being able to succeed."[173] Doteveryone suggested:

> "Taking a more holistic view of consumer welfare, considering issues such as consumer privacy, value of personal data and the ability of consumers to switch between services, can give regulators a better understanding of how consumers' interests are affected by digital technologies."[174]

156. However, Professor Pinar Akman, a competition law academic, thought that the consumer welfare standard should not expand to include non-economic concerns. She said:

> "[The consumer welfare standard] is far from perfect, but, of the other options we have, it is the most concrete … If we include other concerns that might be more political or might have to do with issues that the competition authority cannot really deal with in its assessment, we turn the business environment into a very uncertain one, which will put off businesses from investment and innovation."[175]

157. Professor Diane Coyle stated that many of the challenges presented by the dominance of platforms reflected a longstanding dilemma in competition assessments, which was how to weigh "static against dynamic efficiency".[176] Static efficiency was concerned with how well a market was currently functioning. Dynamic efficiency took account of the development of new products and services. Professor Coyle argued that, while the current focus of regulation was on problems associated with static competition, more attention to should be paid to "the scope for disruptive technological innovation and the dynamic consumer benefits of investment".

Competition law responses

158. Competition law interventions rely on meticulous and cautious assessments of complex situations. Antony Walker, Deputy Chief Executive of techUK, questioned whether competition law "can keep pace and keep up. Competition law is necessarily quite slow, but innovation and companies scale incredibly quickly. We have seen that over the last few years, and the question is whether [competition law] can keep pace."[177] Doteveryone said that "Focusing on profitability as the primary indicator of market power can often mean that a regulator only intervenes after companies gain market dominance, at which point effective regulation becomes harder."[178]

159. The result of this is that competition law interventions happen after problems become entrenched, rather than preventing them. Javier Ruiz Diaz of the Open Rights Group said that "the remedies for individuals can be either

173 Written evidence from British Computer Society (IRN0092)
174 Written evidence from Doteveryone (IRN0028)
175 Q 91
176 Diane Coyle, 'Practical competition policy implications of digital platforms' March 2018: https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Practical_competition_policy_tools_for_digital_platforms.pdf [accessed 2 January 2019]
177 Q 49 (Antony Walker)
178 Written evidence from Doteveryone (IRN0028)

non-existent or difficult. They have to go through several hoops to get a benefit at the end."[179] Professor Edwards said: "Legal solutions such as competition law actions are on historical evidence, likely to be long drawn out and less successful than technical solutions, which should at least be promoted alongside."[180] We discuss these technical solutions below.

160. **The modern internet is characterised by the concentration of market power in a small number of companies which operate online platforms. These services have been very popular and networks effects have helped them to become dominant. Yet the nature of digital markets challenges traditional competition law. The meticulous ex post analyses that competition regulators use struggle to keep pace with the digital economy. The ability of platforms to cross-subsidise their products and services across markets to deliver them free or discounted to users challenges traditional understanding of the consumer welfare standard.**

161. ***In reviewing the application of competition law to digital markets, the Government should recognise the inherent power of intermediaries and broaden the consumer welfare standard to ensure that it takes adequate account of long-term innovation. The Government should work with the CMA to make the process for imposing interim measures more effective.***

162. ***We take this opportunity to repeat the recommendation that we made in our report 'UK advertising in a digital world' that the CMA should undertake a market study of the digital advertising market. We would be grateful for an update from the Government and the CMA.***

Other consequences of concentration

163. Market dominance can cause other, non-economic, harms to society and individuals. Dr Orla Lynskey explained:

> "Competition law is relevant in so far as it is the primary legal instrument available to us to regulate and constrain private market power in any way. However, competition law is not designed with the intention of remedying human rights problems or other problems that fall outside the remit of the concept of consumer welfare."[181]

164. Jamie Bartlett raised concern about the future impact on society: "Mega-tech monopolies in the next 10 years will do incredible harm to democracy but not to consumer welfare. It would be brilliant for consumer welfare but not for the health of democracy."[182]

165. A number of witnesses said that online platforms had become 'gatekeepers', controlling access to the internet. The London Internet Exchange said:

> "Almost any action or behaviour is wholly reliant on one or more intermediaries: the internet access provider, the domain name registry, the website or social media platform, the search engine etc. In the offline

179 Q 26
180 Written evidence from Lilian Edwards, Professor of eGovernance (IRN0069)
181 Q 84
182 Q 55

> world, an actor can frequently act on their own, and are alone accountable for their action. In the online world, if a necessary intermediary chooses to intervene to suppress the action, the actor is sanctioned".[183]

166. Dr Shehar Bano said that this may have benefits: "For example, by providing users with a convenient way to publish and discover content without bothering about the intricate technical details. But the ability of a few large players to influence information flows of billions of users over the internet threatens users' right to free and fair access to information."[184] Dr Paul Bernal noted that the market dominance of online platforms gave them "immense power" which was coupled with power derived from the algorithms they use to "control what we see, read and hear".[185]

167. As discussed in chapter 2, openness should be an essential quality of the internet and we believe that it should be a fundamental principle for regulation (including self-regulation). This is vital as the internet enables users to engage with democratic debate and exercise their rights to freedom of expression and information. Dr Shehar Bano said that online platforms should have "the responsibility to fairly offer their services to users, without any discrimination".[186]

168. The role of gatekeeper has given platforms significant power over the media. The Internet Society said this had particular implications for younger people, who access much of their news from platforms. It continued:

> "Concerns about media empires with too much dominance in newspapers or TV coverage, should equally apply to online platforms where it is now common for a single provider to dominate a service sector (Facebook for social networks, Google for search). As shown by Facebook's own study (2012 US elections impact on likelihood to cast a vote), they have the power to influence voting behaviour."[187]

169. Which? suggested that users view large tech companies as utilities in the sense that people feel that they have little choice but to use them. [188] Professor Leighton Andrews, Cardiff Business School also suggested that online platforms may be considered as "performing a utility function".[189] He noted that Mark Zuckerberg has spoken of Facebook as "a social utility" or "social infrastructure". This had historically been a justification for regulation. While the situation of Facebook and Google was different, they had significant market power. At the very least, he said, "Their potential for exploitation by hostile state actors, as we have seen in both the US Presidential election and in the UK's EU referendum, means that they should be seen as critical social infrastructure."[190]

170. The concentration of platforms affects how they respond to online harms. The Northumbria Internet & Society Research Interest Group referred to

---

183 Written evidence from LINX (IRN0055)
184 Written evidence from Dr Shehar Bano (IRN0114)
185 Written evidence from Dr Paul Bernal (IRN0019)
186 Written evidence from Dr Shehar Bano (IRN0114)
187 Written evidence from Internet Society UK Chapter (IRN0076)
188 'Control, Alt or Delete? The Future of Consumer Data' *Which?* (4 June 2018) https://www.which.co.uk/policy/digitisation/2659/control-alt-or-delete-the-future-of-consumer-data-main-report [accessed 26 February 2019]
189 Written evidence from Professor Leighton Andrews (IRN0041)
190 Written evidence from Professor Leighton Andrews (IRN0041)

the significant power imbalance "where individuals are not able to negotiate the terms and there is in effect no real 'choice' at all."[191] All Rise Against Cyber-Abuse said, "The dominance of the online platforms and the scale of their userbase reduces the likelihood of consumers voting with their feet if they hear of, see or experience cyber abuse. With little competition, comes little motivation and little innovation in solving this problem."[192]

171. **Online communications platforms act as gatekeepers for the internet, controlling what users can access and how they behave. They can be compared to utilities in the sense that users feel they cannot do without them and so have limited choice but to accept their terms of service. Providers of these services currently have little incentive to address concerns about data misuse or online harms, including harms to society**

172. ***It is appropriate to put special obligations on these companies to ensure that they act fairly to users, other companies and in the interests of society. These obligations should be drawn up in accordance with the 10 principles we have set out earlier in this report and enforced by a regulator.***

Data rights, portability and interoperability

173. The internet was founded on principles of openness and interoperability. Professor Derek McAuley and his colleagues at Horizon told us that this environment was now being restricted by isolated "walled gardens" where dominant players control the software ecosystem.[193] This can result in 'lock-in' for suppliers and end users and result in high switching costs.

174. Some witnesses suggested that the new right to data portability under the GDPR, which gives individuals the right to request access to and move certain types of personal data between organisations, may improve this situation and make digital markets more competitive. The Government told us that it had commissioned research to understand "how greater portability could make a real difference to competition, and to engage with business to understand what actions are needed to deliver these benefits".[194]

175. Dr Damian Tambini told us that in practice the effectiveness of data portability will depend on a range of interpretations:

> "Will it in fact be possible for you to download your entire Facebook history, photos, friends, delete them from Facebook and transplant them into a competitor social network? That is the policy solution that would fuel real competition, but it is one that Facebook and co will fight tooth and nail to prevent."[195]

176. The right to data portability under the GDPR may be too limited as it applies only to data which users upload, rather than data which is inferred about them. Robert Colvile of the Centre for Policy Studies, for example,

191 Written evidence from NINSO (IRN0035)
192 Written evidence from All Rise Say No to Cyber Abuse (IRN0037)
193 Written evidence from Horizon Digital Economy Research Institute (IRN0038)
194 Written evidence from Her Majesty's Government (IRN0109)
195 Written evidence from Dr Damian Tambini (IRN0101)

suggested that it was restrictive in not allowing users to export their "social graph" (information about their network of contacts) to another site.[196]

177. Professor Lilian Edwards told us that the right of data portability would not be sufficient "to limit platform power and control over user data in contexts like social networking. Users will not leave platforms where all their friends are unless they think they can continue to interact with them. What they need is data interoperability for this." She warned that "Regulation to promote true interoperability is vital as the market alone will always reject it as a threat to proprietary advantage."[197] The Open Rights Group suggested that "platforms could be forced to maintain a greater degree of interoperability and permeability—for example, so that people outside of Facebook can contact people using Facebook."[198]

178. Professor Edwards suggested that personal data containers or "edge computing" might be a solution to the problem of privacy which could improve interoperability. Instead of users contributing their data to platforms, who then provide services like search or social networking, the user keeps their own data and applies processes to it.[199] Mark Bridge of *The Times* told us about an example of this being developed by Sir Tim Berners-Lee. He felt that it would be "fantastic" if it worked but cautioned that "The big incumbents, Facebook and Google, are so convenient. That is the thing: people will trade a lot for convenience."[200]

179. **It is too early to say how effective the right to data portability will be. It has the potential to help counteract the switching costs which lock users into services by giving them more autonomy over and control of their data. This will require greater interoperability. Portability would be more effective if the right applied to social graphs and other inferred data. The Centre for Data Ethics and Innovation should play a role developing best practice in this area. The Information Commissioner's Office should monitor the operation and effectiveness of this right and set out the basis on which it will be enforced.**

196 Supplementary written evidence from the Centre for Policy Studies (IRN0111)
197 Written evidence from Lilian Edwards, Professor of eGovernance (IRN0069)
198 Written evidence from Open Rights Group (IRN0090)
199 Written evidence from Lilian Edwards, Professor of eGovernance (IRN0069)
200 Q 160 (Mark Bridge)

CHAPTER 5: ONLINE PLATFORMS

180. Intermediaries, including online platforms, are the gatekeepers to the internet. In this chapter we consider their role in mediating content-based online harms, including: bullying, threats and abusive language (including hate speech), economic harms (including fraud and intellectual property infringement), harms to national security (including violent extremism) and harms to democracy.

181. Although online content is subject to civil and criminal law, including the law of defamation and public order offences, there is no systematic regulation of content analogous to that which applies to the use of data and market competition.[201] Mark Bunting, a partner at Communications Chambers, told us that content regulation represented the "the most obvious gap" in the regulatory landscape.[202] In particular he felt that there was a gap in "regulatory capacity to engage with platforms' role in managing access to … content". The Government agreed that the lack of enforcement in the online environment had allowed some forms of unacceptable behaviour to flourish online. The Government is developing an Internet Safety Strategy to address these gaps.[203]

182. It must be stressed that not all online harms are illegal. For example, instances of bullying, online abuse and disseminating extremist content or political misinformation may not cross the threshold of illegality. In this chapter we first consider the existing model for regulating illegal content and then how online harms in general can be better regulated. Table 3 sets out the different categories of online content and our approach to regulating them.

Illegal content

183. The European e-Commerce Directive provides that online intermediaries are not liable for illegal content found on their services unless they have specific knowledge of it.[204] If they become aware of such content, they must act expeditiously to remove it. This model is known as 'notice and takedown'. It enables platforms to intermediate large volumes of content from different sources without scrutinising its legality before publication. As set out in box 4, the liability exemption applies only to specific types of activity, not to the platforms themselves.

184. Article 15 of the directive provides that member states may not impose a general responsibility on service providers to monitor content (see box 5). In practice service providers frequently monitor content, often using specially designed software, and they work with designated organisations (called 'trusted flaggers') to identify illegal content. They also rely heavily on users to report content.

201 There are certain exceptions such as 'TV-like' content which is regulated by Ofcom.
202 Q 12
203 Written evidence from Her Majesty's Government (IRN0109)
204 *The e-Commerce Directive 2000/31/EC (OJ l87 17 July 2000)*

Table 3: Categories of online content

	Illegal	Harmful	Anti-Social
Examples	Terrorism-related, child sexual abuse material, threats of violence, infringement of intellectual property rights	Content which is not illegal but is inappropriate for children, content which promotes violence or self-harm and cyberbullying.	Indecent, disturbing or misleading content and swearing.
Current status	Governed by criminal and civil law and the e-Commerce Directive. The e-Commerce directive is evolving through case law.	Subject to Terms of Service.	Subject to Terms of Service.
Recommendations	The Directive is under review and will require further consideration after the UK leaves the European Union.	A duty of care should be imposed on platforms and regulated by Ofcom. Terms of service must be compatible with age policies.	Platforms should provide their terms of service in plain English and Ofcom should be empowered to ensure that they are upheld. Platforms should work with Ofcom to devise a classification framework
	Platforms should invest in their moderation systems to remove content which breaks the law or community standards more quickly and to provide a fair means of challenging moderation decisions.		

Box 4: The e-Commerce Directive: articles 12–14

The directive excludes liability for 'Information Society Service Providers' (which include internet service providers and most online platforms) where they are acting for the content in question as:

- **Access providers ("mere conduits")** which enable the transmission of information automatically and transiently, or provide access to a communication network. To qualify for this limitation, an intermediary must not (1) initiate the transmission, (2) select the receiver of information or the actual information in the transmission, or (3) modify it. The information transmitted must take place for the sole purpose of carrying out the transmission only, and not be stored for a period longer than reasonably necessary for the purposes of the transmission. Telecommunications operators such as mobile networks perform this function. (Article 12)
- **Cache providers** which store transmitted information automatically and temporarily "for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request". The intermediary must not modify the information. Internet service providers, such as BT, Sky Broadband and Virgin Media, perform this function. (Article 13)
- **Hosting providers** which store data specifically selected and uploaded by a user of the service, and intended to be stored ("hosted") for an unlimited amount of time. Hosting providers can benefit from the liability exemption only when they are "not aware of facts or circumstances from which the illegal activity or information is apparent" (when it concerns civil claims for damages) or when they "do not have actual knowledge of illegal activity or information." This can apply to some but not all activities of social media companies, search engines and other online platforms. (Article 14)

Source: Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') 2000/31/EC (OJ 187 17 July 2000). The directive refers to 'information society service providers'. It was transposed into UK law by The Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013)

185. EU member states have applied different standards in implementing this rule. For example, Germany's Network Enforcement Act (NetzDG) requires platforms with more than 2 million subscribers to remove "manifestly unlawful" content within 24 hours, with fines of up to €50 million for non-compliance. However, the law has been widely criticised for incentivising platforms to take down legal content.[205] On the first day of the law's coming into force, Twitter temporarily suspended the account of Beatrix von Storch, the deputy leader of Alternative für Deutschland (AfD), after she posted anti-Muslim tweets, and deleted tweets from other AfD politicians. It subsequently suspended for two days the account of *Titanic*, a German satirical magazine, for parodying von Storch. The German newspaper *Bild* said that the law made AfD "opinion martyrs" and called for it to be repealed.[206] techUK warned that the chilling effect of overly strict take-down obligations "could have untold consequences on the availability of legitimate content."[207]

205 Written evidence from Global Partners Digital (IRN0099)
206 Julian Reichelt, 'Bitte keine Meinugspolizei', *Bild* (3 January 2018): https://www.bild.de/politik/inland/gesetze/kommt-jetzt-die-meinungspolizei-54367844.bild.html [accessed 13 February 2019]
207 Written evidence from techUK (IRN0086)

Box 5: The e-Commerce Directive: article 15

Article 15 of the e-Commerce Directive prevents EU member states from imposing on intermediaries a general obligation to monitor information which they transmit or store, and provides that intermediaries cannot be generally obliged "actively to seek facts or circumstances indicating illegal activity". Article 15 does not prevent member states from setting up reporting mechanisms which require intermediaries to report illegal content once they are made aware of it. Graham Smith, a partner in Bird & Bird, has called article 15 "a strong candidate for the most significant piece of internet law in the UK and continental Europe".[208]

Whereas other provisions of the e-Commerce Directive were implemented by the Electronic Commerce (EC Directive) Regulations 2002, article 15 was not specifically implemented through UK domestic legislation. Under section 2 of the European Union (Withdrawal) Act 2018 directives are not in themselves "retained EU law", only the domestic legislation made to implement them. However, under section 4 of the Act any prior obligations or restrictions of EU law which are "recognised and available in domestic law" will continue after Brexit. As article 15 has been recognised by domestic courts, including the Supreme Court in *Cartier International AG and others v British Telecommunications Plc*,[209] it is likely to be considered retained law, but uncertainty may remain until the matter is tested by the courts.

186. Some witnesses argued that the directive, which is nearly 20 years old, is no longer adequate for today's internet. They argue that it was created when service providers did not have a role in curating content for users, as many do now. The Children's Media Foundation said: "Whether by accident or design, search engine algorithms are the de-facto curators for most people's access to content online. The platforms are using this curation to drive their revenues."[210] It disputed that online platforms had a passive role, arguing that they should be considered as publishers. All Rise agreed:

> "The e-Commerce Directive was introduced in what now feels like a bygone era … One of the biggest winners … has been the online platforms. They can provide services to millions of people worldwide, harvest their data and make millions in revenue, and yet have zero responsibility for what their customers see and experience and the harm they suffer whilst under their care. Yes, the platforms have to remove illegal content once they are notified, but they have no obligation proactively to stop that content from reaching our eyes and ears, even if they know their sites are full of it."[211]

187. The Northumbria Internet & Society Research Interest Group explained how the liability might be extended beyond 'notice and takedown':

> "A platform should be liable if it has knowledge of the unlawful content or it has the technical means and resources to ensure the legality of the activities carried out on the platform while striking a balance between the

208 Graham Smith, *Time to speak up for Article 15* (21 May 2017): https://www.cyberleagle.com/2017/05/time-to-speak-up-for-article-15.html [accessed 26 February 2019]

209 *Cartier International AG and others (Respondents) v British Telecommunications Plc and another (Appellants)* [2018] UKSC 28

210 Written evidence from CMF (IRN0033)

211 Written evidence from All Rise Say No to Cyber Abuse (IRN0037)

> different interests involved, including freedom of expression. Platforms which de facto or de jure monitor users cannot invoke immunity."[212]

188. By contrast Oath, a tech group, argued that the e-Commerce Directive framework was not "superannuated" but was "deliberately forward-looking and prescient by design".[213] According to Oath, it has several key strengths including that it is technology neutral and so can be adapted to "complex and fast-evolving business models".

189. The courts already take account of the fact that the platforms of today are very different from the providers that were around when the directive was introduced. In *L'Oréal v eBay* the court found that if the operator of a marketplace platform optimised the presentation of, or promoted, trademark-infringing goods listed for sale or promoted those offers, it could not rely on the exemption from liability under article 14. It could not be considered to have taken "a neutral position between the customer–seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale".[214] This judgment means that platforms which curate content may find that the safe harbour is not available to them.

190. Global Partners Digital cautioned against the introduction of "inappropriate legislation" which:

> "attaches liability to online platforms for content which is available on them, can lead to a 'chilling effect' in which platforms either become reluctant to host or otherwise make available content, or are overly zealous in removing content which might be harmful. It can also result in online platforms being forced to make decisions about the legality of content which they are ill-equipped to make, a problem exacerbated due to the minimal transparency that exists regarding online platforms' decision-making, and the absence of due process, safeguards for affected users, and oversight."[215]

191. The Internet Society warned that imposing specific legal liability might undermine competition, as "large platforms are more likely than smaller platforms to be able to invest in resources to (a) fight litigation, (b) develop tools and algorithms to police their platform and (c) actively employ people to police their platform".[216] The Internet Society also said that a change in the UK's rules would probably cause hosting providers to move their servers based in the UK to "more lenient regulation regimes."

192. Some have argued that the conditional exemption from liability should be abolished altogether. It has been suggested that using artificial intelligence to identify illegal content could allow companies to comply with strict liability. However, such technology is not capable of identifying illegal content accurately and can have a discriminatory effect. Imposing strict liability would therefore have a chilling effect on freedom of speech. These concerns would need to be addressed before the 'safe harbour' provisions of the e-Commerce Directive are repealed.

---

212 Written evidence from NINSO (IRN0035)
213 Written evidence from Oath (IRN0107)
214 See paragraph 116
215 Written evidence from Global Partners Digital (IRN0099)
216 Written evidence from the Internet Society (IRN0076)

193. **Online platforms have developed new services which were not envisaged when the e-Commerce Directive was introduced. They now play a key role in curating content for users, going beyond the role of a simple hosting platform. As such, they can facilitate the propagation of illegal content online. 'Notice and takedown' is not an adequate model for content regulation. Case law has already developed on situations where the conditional exemption from liability under the e-Commerce Directive should not apply. Nevertheless, the directive may need to be revised or replaced to reflect better its original purpose.**

Harmful and anti-social content

194. Online platforms, especially social media platforms, are under fire for enabling other online harms which may not cross the threshold of illegality, as well as for doing too little to prevent people, including children, from accessing inappropriate content. The case of 14-year-old Molly Russell, who took her own life in 2017 after being exposed to graphic self-harm images on Instagram, has prompted a wider debate about the safety of young people online.[217] Rebecca Stimson of Facebook told us that her company considered itself "responsible for the content of that platform to ensure that what people are seeing is not harmful, it is not hate speech, bullying and so forth, or containing fake adverts".[218]

195. Many witnesses were concerned that content regulation would be detrimental to freedom of speech and expression. Dr Paul Bernal said:

> "It is important to understand that it is a very slippery slope, and that there could easily be a chilling effect on freedom of speech if it is taken too far. A platform may be cautious about hosting, reducing the opportunities for people to find places to host their material, if it is in any way controversial."[219]

196. However, All Rise Say No to Cyber Abuse painted a picture of widespread abuse and linked social media to increasing rates of anxiety and depression.[220] It noted that, while freedom of speech was critical to modern society, it "is by no means freedom to abuse, nor does it mean freedom to harm—an inalienable right to say what you want with no constraint or accountability."[221] Cyber abuse was "killing free speech and itself bringing about the 'chilling effect' so often feared when we consider free speech. Voices are crushed and people stop speaking their truth, many too hurt and afraid even to be online." This position was supported in the review by the Committee on Standards in Public Life on *Intimidation in Public Life*, which found that technology had drastically increased the volume and frequency of abuse while the brevity of messages and lack of face-to-face contact made discussion more extreme.[222]

---

217 Richard Adams, 'Social media urged to take "moment to reflect" after girl's death', *The Guardian* (30 January 2019): https://www.theguardian.com/media/2019/jan/30/social-media-urged-to-take-moment-to-reflect-after-girls-death [accessed 13 February 2019]

218 Q 180

219 Written evidence from Dr Paul Bernal (IRN0019)

220 Written evidence from All Rise Say No to Cyber Abuse (IRN0037)

221 *Ibid.*

222 Committee on Standards in Public Life *Intimidation in Public Life*, Cm 9543, December 2017 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/666927/6.3637_CO_v6_061217_Web3.1__2_.pdf

Women and individuals from LGBT and black and minority ethnic groups received a disproportionate volume and degree of abuse.

197. The Government is seeking to address problems of online safety through its Internet Safety Strategy. In May 2018 it published a response to its consultation on this subject and it is expected to publish a white paper soon.[223] The main regulatory responses that it is considering are a code of practice for social media providers, required under the Digital Economy Act 2017, transparency reporting and a social media levy. The response included a draft of the code, which will be voluntary, and additional guidance.

A duty of care

198. Recital 48 of the e-Commerce Directive provides that the safe harbour provisions do not preclude member states from developing a duty of care. Professor Lorna Woods of the University of Essex and William Perrin of the Carnegie UK Trust have developed a detailed proposal to introduce a duty of care. Whereas debates around intermediary liability have been framed by the question of whether intermediaries should be treated as a publisher or a 'mere conduit', Professor Woods and Mr Perrin suggested that a better analogy would be to see them as a public space "like an office, bar or theme park".[224] Millions of users visit intermediary sites. In the offline world the owners of physical spaces owe a duty of care to visitors. In line with the parity principle which was considered in chapter 2, Professor Woods and Mr Perrin argue that owners of online services should also be required to "take reasonable measures to prevent harm". Professor Woods told us that this approach avoided "some of the questions about making platforms liable for the content of others".[225] In particular, action against online service providers "should only be in respect of systemic failures" rather than individual instances of speech.[226]

199. Professor Woods and Mr Perrin recommended that a regulator should be established to act against online service providers for breach of duty of care. They argued that this was necessary to redress the inherent inequality of arms between an individual user and a large social media company.[227] They envisaged that the regulator would promote a 'harm reduction cycle', whereby it would collaborate with the industry and with civil society to monitor harms and establish best practice. This would be an ongoing process that would be "transparent, proportionate, measurable and risk-based".

200. In chapter 2 we argued that principles-based regulation which is focused on achieving the right outcomes is desirable in the fast-changing digital world. Duties of care are also "expressed in terms of what they want to achieve—a desired outcome (i.e. the prevention of harm) rather than necessarily

223 DCMS, 'Government response to the Internet Safety Strategy Green Paper' (May 2018): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf [accessed 12 January 2019]

224 Written evidence from Professor Lorna Woods and William Perrin (IRN0047)

225 Q 1

226 Written evidence from Professor Lorna Woods and William Perrin (IRN0047)

227 Written evidence from Professor Lorna Woods and William Perrin (IRN0047). In their updated proposal, published in January 2019, they suggest that enforcement of the duty of care should be the sole preserve of the regulator and that it should not give rise to an individual right of action: Professor Lorna Woods and William Perrin, 'Internet Harms reduction: An updated proposal', p 12, *Carnegie UK Trust* (January 2019).

regulating the steps—the process—of how to get there".[228] This generality allows the approach to work across different types of services and would be largely future-proof.

201. The duty of care approach emphasises the design of services. Professor Woods and Mr Perrin cited the concept of privacy by design in the GDPR and safety by design in the Health and Safety at Work Act etc. 1974 as models for risk-based regulation which addresses all stages of product development. This approach draws on the "precautionary principle", which is:

> "applied in situations where there are reasonable grounds for concern that an activity is causing harm, but the scale and risk of these issues is unproven. The onus is then on organisations to prove that their practices are safe to a reasonable level."[229]

202. Professor Woods and Mr Perrin suggested that the duty of care should apply to social media services of all sizes and that it should apply to messaging services which permit large or public groups.[230] In doing so they noted that in another context food safety standards apply to all types of food producers, not just the largest. The issue of proportionality could be dealt with by a competent regulator. They left open the question of whether search engines, including YouTube, might also be covered.

203. There many different types of online platforms of different sizes: "for example websites operated by sporting groups or from community interest, which will also operate their own moderation policies". NINSO told us: "Given that such groups will rarely be able to benefit from the legal advice available to large corporations, a tailored approach to regulation or at least guidance for such groups would undoubtedly be helpful."[231]

204. In Australia an e-Safety Commissioner regulates social media platforms (see box 6). It operates a system which is voluntary for smaller platforms but mandatory for the largest, which are designated 'Tier 2' services through the exercise of ministerial powers.[232] The commissioner handles complaints if they are not dealt with by the companies themselves.

228 Written evidence from Professor Lorna Woods and William Perrin (IRN0047)
229 Written evidence from Doteveryone (IRN0028)
230 Professor Lorna Woods and William Perrin, 'Internet Harms reduction: An updated proposal', *Carnegie UK Trust* (January 2019): https://www.carnegieuktrust.org.uk/blog/internet-harm-reduction-a-proposal/ [accessed 26 February 2019]
231 Written evidence from NINSO (IRN0035)
232 Written evidence from the e-Safety Commissioner (IRN0016)

Box 6: Office of the e-Safety Commissioner of Australia

The Australian government established the Office of the e-Safety Commissioner in July 2015 to help keep children safe from online abuse. Two years later its remit was expanded to include the online safety of adults. The Office provides a mechanism through which Australians can report illegal or abusive content which social media companies have failed to remove within 48 hours. Companies can then be formally directed to remove content. In addition, the Office runs campaigns to educate citizens on the dangers of cyber abuse and to improve digital skills. One campaign, eSafetyWomen, helps women at risk of emotional abuse or violence to stay safe when using the internet. The Office also co-ordinates between organisations, including referring victims for counselling where appropriate.

The Office enjoys a range of discretionary powers, including power to impose civil penalties. It can impose fines of up to $21,000 a day for Tier 2 social media sites that do not comply with take-down notices. The Office notes that, while this may not be much for some of the big tech companies, the reputational impact on social media companies of being fined should not be underestimated. The Office has received full compliance from industry to date.

Source: Written evidence from the Office of the e-Safety Commissioner (IRN0016)

205. ***Technology companies provide venues for illegal content and other forms of online abuse, bullying and fake news. Although they acknowledge some responsibility, their responses are not commensurate with the scale of the problem. We recommend that a duty of care should be imposed on online services which host and curate content which can openly be uploaded and accessed by the public. This would aim to create a culture of risk management at all stages of the design and delivery of services.***

206. ***To be effective, a duty of care would have to be upheld by a regulator with a full set of enforcement powers. Given the urgency of the need to address online harms, we believe that in the first instance the remit of Ofcom should be expanded to include responsibility for enforcing the duty of care. Ofcom has experience of surveying digital literacy and consumption, and experience in assessing inappropriate content and balancing it against other rights, including freedom of expression. It may be that in time a new regulator is required.***

Moderation processes

207. The moderation of content is likely to be key to reducing online harm. This refers to the process of dealing with content which does not comply with 'community standards'. Katie O'Donovan of Google told us that the company has community standards which go further than merely ensuring that users abide by the law: "We enforce those and people will be removed from our platform if they break them. It is difficult, complicated and resource intensive but for us it preserves the free internet."[233]

208. Big Brother Watch told us platforms were "enforcing systems of governance that are constantly changing, unaccountable, and opaque".[234] Users cannot always easily find guidance about the policies online platforms use. Even

233 Q 180
234 Written evidence from Big Brother Watch (IRN0115)

when platforms provide an accessible policy it may not be helpful to the ordinary individual and may be considered misleading. As a result users may not know what they can expect and what is expected of them.[235]

209. Moderation mechanisms need to balance the interests of different parties. The Open Rights Group were clear that "all sides of a dispute need to have the ability to assert their rights".[236] However, McEvedys said that this was not the experience of many internet users. McEvedys concluded: "there are many issues with leaving the matter wholly to the private sector where they get to mark their own homework and/or are self-interested", suggesting "that the lack of [an effective] remedy is the real issue."[237]

210. There was a lack of transparency of those involved in moderation processes themselves. Matt Reynolds, a journalist with Wired UK, told us of his experience reporting far-right content to Facebook. At first Facebook took no action against content which Mr Reynolds believed violated community standards. He subsequently discovered that the content had been taken down after all. He found it "very hard to get an answer from Facebook" about its decision-making process.[238] He argued that there was no transparency in Facebook's moderation practices.

211. In December 2018 Facebook's moderation guidelines were leaked by an employee concerned that the company was acting inconsistently and without proper oversight.[239] The secrecy of the document highlighted the lack of transparency in Facebook's content policies. It also appears that the content of the guidelines was inadequate. The document revealed inconsistencies and errors in Facebook's approach, including factual errors on what was legal in different countries.

212. Jenny Afia, a partner at Schillings, agreed that moderation processes are not transparent: "You do not know if a human has made a decision on your complaint or it has just been determined by an algorithm."[240] She noted that: "Most platforms do not have dedicated 'legal' email addresses where complaints can be sent to or phone numbers to speak to people … The experience feels like dealing with a brick wall built by an algorithm."[241]

213. We heard that platforms have not dedicated sufficient resources to moderation. Alex Hern of *The Guardian* thought it "slightly unbelievable that any platform with users measured in the billions can count its human moderators in the thousands. That seems to be a scale error."[242] Facebook has over 2 billion users and Instagram has around 1 billion, yet there are only around 30,000 moderators between the two sites.[243] The volume of content each moderator must examine means that they often do not have sufficient understanding of particular contexts.

---

235 Written evidence from NINSO (IRN0035)
236 Written Evidence from the Open Rights Group (IRN0090)
237 Written Evidence from McEvedys Solicitors & Attorneys Ltd (IRN0065)
238 Q 156
239 Max Fisher, 'Inside Facebook's Secret Rulebook for Global Political Speech' *The New York Times* (27 December 2018) https://www.nytimes.com/2018/12/27/world/facebook-moderators.html [accessed 14 February 2019]
240 Q 61
241 Written evidence from Jenny Afia, Partner, Schillings (IRN0032)
242 Q 156
243 Mike Wright, 'Parental settings online failing to block violence, pornography and self-harm' *The Telegraph* (18 February 2019) https://www.telegraph.co.uk/news/2019/02/18/parental-settings-online-failing-block-violence-pornography/ [accessed 22 February 2019]

214. Facebook's public guidance on community standards states that they "try to consider the language, context and details in order to distinguish casual statements from content that constitutes a credible threat to public or personal safety."[244] However, *The Guardian* revealed that Facebook's internal guidance for moderators advised that 'casual statements' could include: "To snap a bitch's neck, make sure to apply all your pressure to the middle of her throat" and "fuck off and die".[245] Facebook suggested that saying these things could be permissible because they were not regarded as credible threats.

215. In December 2018 a report from two Israeli NGOs revealed WhatsApp's reliance on ineffective automated systems to police child sexual abuse material.[246] The study showed how third-party apps for discovering WhatsApp groups allowed for the trading of images of child exploitation. WhatsApp responded by stating that it had a zero-tolerance approach to images of child exploitation and that its systems had banned a further 130,000 accounts in a recent 10-day period for violating this policy.

216. Many legal experts felt that too much power had been delegated to private companies to act in effect as censors. NINSO told us that platforms do not use this power consistently and "are often over-effective when it comes to intellectual property infringement and non-effective when it comes to other forms of content, for example in relation to terrorism".[247]

217. In 2016 Facebook deleted a post by Norwegian writer Tom Egeland that featured 'The Terror of War', a Pulitzer prize-winning photograph by Nick Ut that showed children—including the naked nine-year-old Kim Phúc running away from a napalm attack during the Vietnam war. Egeland's post discussed "seven photographs that changed the history of warfare" a group to which the "napalm girl" image certainly seemed to belong. Facebook deleted the image for being in breach of its rules on nudity. The image was reinstated after Norway's largest newspaper published a front-page open letter to Mark Zuckerberg, the CEO of Facebook, criticising the company's decision to censor the historic photograph. While this may have been a sensible outcome, few individual users can rely on a national newspaper to challenge a decision which goes against them.

218. Platforms' role as gatekeepers to the internet can limit freedom of expression but is not accompanied by the safeguards for human rights which the UK is expected to observe.[248] Dr Nicolo Zingales, lecturer in Competition and Information Law at the University of Sussex, told us the UN special rapporteur on freedom of expression was concerned about the lack of transparency. While platforms were taking small steps, he felt that "it would

244 Facebook, 'Community Standards': https://m.facebook.com/communitystandards/violence_criminal_behavior/ [accessed 26 February 2019]

245 Nick Hopkins, 'Revealed: Facebook's internal rulebook on sex, terrorism and violence' *The Guardian* (21 May 2017) https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence [accessed 15 February 2019]

246 Priya Pathak, 'WhatsApp has a big child pornography problem, NGOs find many groups spreading it on chat app' *India Today* (21 December 2018) https://www.indiatoday.in/technology/news/story/whatsapp-has-a-big-child-pornography-problem-ngos-find-details-of-many-groups-spreading-it-on-chat-app-1414326–2018–12-21 [accessed 14 February 2019]

247 Written evidence from NINSO (IRN0035)

248 Q 83

be good if they had specific procedures in place to show that they have accountability by design".[249]

219. Mark Stephens, a partner at Howard Kennedy, suggested that the UN Guiding Principles on Business and Human Rights ('Ruggie principles') should be used to develop better moderation systems. These principles were designed to be used for businesses carrying out activities which affect human rights. Box 7 outlines principle 31, which applies to non-state actors operating a grievance mechanism.

Box 7: The Ruggie principles: principle 31

In order to ensure their effectiveness, non-judicial grievance mechanisms, both state-based and non-state-based, should be:

(a) Legitimate: enabling trust from the stakeholder groups for whose use they are intended, and being accountable for the fair conduct of grievance processes;

(b) Accessible: being known to all stakeholder groups for whose use they are intended, and providing adequate assistance for those who may face particular barriers to access;

(c) Predictable: providing a clear and known procedure with an indicative time frame for each stage, and clarity on the types of process and outcome available and means of monitoring implementation;

(d) Equitable: seeking to ensure that aggrieved parties have reasonable access to sources of information, advice and expertise necessary to engage in a grievance process on fair, informed and respectful terms;

(e) Transparent: keeping parties to a grievance informed about its progress, and providing sufficient information about the mechanism's performance to build confidence in its effectiveness and meet any public interest at stake;

(f) Rights-compatible: ensuring that outcomes and remedies accord with internationally recognised human rights;

(g) A source of continuous learning: drawing on relevant measures to identify lessons for improving the mechanism and preventing future grievances and harms.

Operational-level mechanisms should also be:

(h) based on engagement and dialogue: consulting the stakeholder groups for whose use they are intended on their design and performance, and focusing on dialogue as means to address and resolve grievances.

Source: Guiding Principles on Business and Human Rights

220. The Internet Watch Foundation believed that moderation decisions should be "quality assured through a rigorous internal process and externally audited. Ultimately, any challenge to the legality of content should be subject to judicial review."[250]

221. All Rise suggested establishing "an independent body to set the standard and ensure it is maintained, as well as to adjudicate on complex cases, undertake

249 Q 84
250 Written evidence from Internet Watch Foundation (IRN0034)

regular audits, preside over appeals and to provide transparency as to the state of play and progress".[251]

222. **Content moderation is often ineffective in removing content which is either illegal or breaks community standards. Major platforms have failed to invest in their moderation systems, leaving moderators overstretched and inadequately trained. There is little clarity about the expected standard of behaviour and little recourse for a user to seek to reverse a moderation decision against them. In cases where a user's content is blocked or removed this can impinge their right to freedom of expression.**

223. ***Community standards should be easily accessible to users and written in plain English. Ofcom should have power to investigate whether the standards are being upheld and to consider appeals against moderation decisions. Ofcom should be empowered to impose fines against a company if it finds that the company persistently breaches its terms of use.***

224. ***The sector should collaborate with Ofcom to devise a labelling scheme for social media websites and apps. A classification framework similar to that of the British Board of Film Classification would help users to identify more quickly the risks of using a platform. This would allow sites which wish to allow unfettered conversation or legal adult material to do so. Users could then more easily choose between platforms with stricter or more relaxed community standards.***

225. Community standards are not always consistent with platforms' age policies. For example, Twitter says that it "allows some forms of graphic violence and/or adult content in Tweets marked as containing sensitive media."[252] However, a user does not have to state that they are over 18 or enter a date of birth to view such content. Indeed, although Twitter has a nominal minimum age of 13, entering a date of birth is optional.

226. ***Community standards and classifications should be consistent with a platform's age policy.***

251 Written evidence from All Rise Say No to Cyber Abuse (IRN0037)

252 Twitter, 'Media Policy': https://help.twitter.com/en/rules-and-policies/media-policy [accessed 26 February 2019]

CHAPTER 6: THE DIGITAL AUTHORITY

Challenges

227. We began our inquiry by asking how internet regulation could be improved, but it became clear that the more salient question was how regulation should respond to changes brought about by the digital world. The digital world presents significant challenges to regulation, in particular: its transnational character, the pace of change, a lack of understanding among policy-makers about risks of emerging technologies and the fragmentation of regulatory action. In this chapter we consider how to ensure that regulation is implemented and developed consistently and effectively in the digital world.

228. As we noted in the introduction, a range of regulators have a stake in the digital world. Each has taken steps to understand the implications of this and to adapt. Caroline Normand, Director of Policy of Which?, said that this had created a confusing picture:

> "There are lots of initiatives, there are lots of regulators, there are underlaps and there are overlaps. We think that that needs to rapidly be sorted through, so that we have the appropriate level of regulation and the appropriate regulators as quickly as possible."[253]

229. Gaps have appeared in regulation which do not clearly fall within any one regulator's remit, or which would require a regulator's remit to be expanded. Matt Reynolds, a journalist at Wired UK, told us: "Consistently, existing bodies have not stepped up or seen that their remit extends to the online world".[254]

230. Policy makers have hesitated to address these gaps. When action does occur, there is a risk that it will be misdirected. Jamie Bartlett told us that "it will be very easy to pass very bad laws about how the internet works now, not thinking about how it might work in future."[255] He was concerned that such laws might be a reaction to public consternation about the internet, which itself was often driven by traditional news media organisations frustrated by the loss of advertising revenue to big tech companies, producing "remarkable headlines that are not particularly helpful".[256]

231. Dr Paul Bernal called for policy-makers, including parliamentarians, to develop "a better knowledge and understanding of the technology, of the environment, of the regulation and law that exists, and of the problems surrounding that regulation and law." He noted that there had been several recent examples of poor policy and practice, such as inappropriate prosecutions and ineffective legislation. He added: "Getting this right is critical before considering further regulation or legislation."[257]

232. However, inaction causes problems of its own. As we saw in chapter 4, competition law is slow and retroactive, and does not take account of non-economic problems associated with digital dominance. Once the damage is done, it is often too late to remedy. Preventative action is needed.

---

253 Q 161
254 Q 153
255 Q 52 (Jamie Bartlett)
256 Q 52 (Jamie Bartlett)
257 Written evidence from Dr Paul Bernal (IRN0019)

233. Regulation across different sectors needs to be strengthened and better coordinated to be capable of responding to the evolving digital world. Dr Damian Tambini said that before now regulatory measures had been implemented in "a fragmented way across different areas. The solution to the current impasse is not going to be a tweak here or there, but a policy response that is coordinated across multiple policy areas."[258] For example, competition policy should be considered alongside other forms of regulation and policy. In his view this was necessary for developing policies in the face of powerful international companies who might otherwise play different policy-makers off against each other.

Overarching regulation

234. Elizabeth Denham, the Information Commissioner, suggested establishing a body which would scan the horizon for emerging trends to help co-ordinate regulators. The aim of such a body would be to ensure that regulation across different sectors is equipped with the understanding to respond to the digital world. Yih-Choung Teh, Group Director for Strategy and Research at Ofcom, told us that Ofcom worked closely with other regulators and there were "a number of mechanisms in place to ensure effective collaboration and co-ordination".[259] Nonetheless, there were "real attractions" to an overarching body as it could help with digital capabilities and understanding.

235. Margot James MP, the Minister for Digital and the Creative Industries, recognised the importance of horizon scanning. Her department already had a team of highly qualified officials "tasked with assessing and staying across emerging technologies".[260]

236. Doteveryone proposed a new body, which it called the Office for Responsible Technology, whose responsibilities would be to empower regulators; to inform the public and policy-makers; and to support people to find redress.[261]

237. In this report we have recommended that the powers of the ICO, the CMA and Ofcom should be extended in various areas where there is a pressing need for regulation. However, the regulatory landscape and location of powers is in urgent need of review This might include consideration as to whether a new regulator for the internet is needed.

238. ***We recommend that a new body, which we call the Digital Authority, should be established to co-ordinate regulators in the digital world. We recommend that the Digital Authority should have the following functions:***

- ***to continually assess regulation in the digital world and make recommendations on where additional powers are necessary to fill gaps;***
- ***to establish an internal centre of expertise on digital trends which helps to scan the horizon for emerging risks and gaps in regulation;***

258 Written evidence from Dr Damian Tambini (IRN0101)
259 Q 129
260 Q 185
261 Catherine Miller, Jacob Ohrvik-Stott & Rachel Coldicutt, 'Regulating for Responsible Technology: Capacity, Evidence and Redress: a new system for a fairer future' (October 2018): https://doteveryone.org.uk/wp-content/uploads/2018/10/Doteveryone-Regulating-for-Responsible-Tech-Report.pdf [accessed 15 January 2019]

- ***to help regulators to implement the law effectively and in the public interest, in line with the 10 principles set out in this report;***
- ***to inform Parliament, the Government and public bodies of technological developments;***
- ***to provide a pool of expert investigators to be consulted by regulators for specific investigations;***
- ***to survey the public to identify how their attitudes to technology change over time, and to ensure that the concerns of the public are taken into account by regulators and policy-makers;***
- ***to raise awareness of issues connected to the digital world among the public;***
- ***to engage with the tech sector;***
- ***to ensure that human rights and children's rights are upheld in the digital world;***
- ***to liaise with European and international bodies responsible for internet regulation.***

239. ***Policy-makers across different sectors have not responded adequately to changes in the digital world. The Digital Authority should be empowered to instruct regulators to address specific problems or areas. In cases where this is not possible because problems are not within the remit of any regulator, the Digital Authority should advise the Government and Parliament that new or strengthened legal powers are needed.***

240. The Digital Authority must be properly funded to be effective and to carry out research. We recognise that this would give the Digital Authority significant powers. This is necessary because of the magnitude of urgent social and political problems caused by regulatory fragmentation in the digital world. These problems are likely to become more complex as technology develops. The Government's 'Digital Charter' work programme is a start, but a new body with the requisite resources and authority is needed to co-ordinate at the heart of the Government. The Digital Authority should therefore report to a Cabinet Office minister.

241. Given the European and international dimensions to these issues, it is important, after the UK leaves the EU, to have mechanisms in place which allow the UK to co-operate with European and international bodies with relevant responsibilities. For this reason it will be important not only for the UK Government to maintain links with European and international partners but for the Digital Authority to have responsibility for liaising with the appropriate European and international institutions.

242. The Digital Authority should be politically impartial and independent of the Government. Its board should consist of chief executives of relevant regulators with independent non-executives. It should be chaired by an independent non-executive. As the digital world develops, it will be important that democratic scrutiny is maintained of the regulators themselves. If regulation

needs to adapt, this may require the transfer of greater powers, as we have suggested in the case of Ofcom. Laurie Laybourn-Langton, Senior Research Fellow, Institute for Public Policy Research, said that addressing regulatory challenges should be "undertaken according to democratic principles, in the same way that we have provided regulation in other key areas of society and the economy through a democratic mechanism—Parliament and the people who represent us".[262]

243. ***The Digital Authority will co-ordinate regulators across different sectors and multiple Government department. We therefore recommend that it should report to the Cabinet Office and be overseen at the highest level.***

244. ***We recommend that a joint committee of both Houses of Parliament should be established to consider matters related to the digital environment. In addition to advising the Government the Digital Authority should report to Parliament on a quarterly basis and regularly give evidence to the new joint committee to discuss the adequacy of powers and resources in regulating the digital world. The combined force of the Digital Authority and the joint committee will bring a new consistency and urgency to regulation.***

262 Q 53

SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

Principles for regulation

1. The 10 principles set out in this report should guide the development and implementation of regulation online and be used to set expectations of digital services. These principles will help the industry, regulators, the Government and users work towards a common goal of making the internet a better, more respectful environment which is beneficial to all. They will help ensure that rights are protected online just as they are offline. If rights are infringed, those responsible should be held accountable in a fair and transparent way. With these principles the internet would remain open to innovation and creativity while a new culture of ethical behaviour would be embedded into the design of services. (Paragraph 68)

Ethical technology

2. As organisations, including financial and health services providers, increasingly perceive individuals as the aggregation of data gathered about them (sometimes called their 'data selves'), it is essential that data be accurate, up-to-date and processed fairly and lawfully, especially when processed by algorithm. While the GDPR and the Data Protection Act 2018 provide valuable safeguards, including subject access rights to ensure that data are accurate and up to date and the right to opt out from purely automated processing, there are weaknesses in the regime. For example, a subject access request does not give subjects automatic access to behavioural data generated about them because it is deemed to be the property of the company that acquired it. (Paragraph 80)

3. Users of internet services should have the right to receive a processing transparency report on request. In a model similar to a subject access report under the GDPR users should have the right to request a data transparency report from data controllers showing not only what data they hold on the data subject (which is the currently the case under the GDPR) but also what data they generate on them (behavioural data) and any behavioural data obtained from third parties, including details of when and how they are obtained. (Paragraph 81)

4. Data controllers and data processors should be required to publish an annual data transparency statement detailing which forms of behavioural data they generate or purchase from third parties, how they are stored and for how long, and how they are used and transferred. (Paragraph 82)

5. Digital service providers (such as hardware manufacturers, operators of digital platforms, including social media platforms and entertainment platforms, and games developers) should keep a record of time spent using their service which may be easily accessed and reviewed by users, with periodic reminders of prolonged or extended use through pop-up notices or similar. An industry standard on reasonable use should be developed to inform an understanding of what constitutes prolonged use. This standard should guide design so that services mitigate the risk of encouraging compulsive behaviour. (Paragraph 88)

6. The Information Commissioner's Office should set out rules for the use of algorithms based on the principles set out in chapter 2. The ICO should be empowered to conduct impact-based audits where risks associated with

using algorithms are greatest and to require businesses to explain how they use personal data and what their algorithms do. Failure to comply with the rules should result in sanctions. (Paragraph 100)

7. The ICO should also publish a code of best practice informed by the work of the Centre for Data Ethics and Innovation around the use of algorithms. This code could form the basis of a gold-standard industry 'kitemark'. (Paragraph 101)

8. Data subjects should be given the right to request a statement from a data processor explaining how, if applicable, algorithms are used to profile them, deliver content or drive their behaviour. (Paragraph 102)

9. Terms of service must be written in a form which is clearly accessible and understandable to internet users. Alongside terms of service statements a 'plain English' statement should be published which sets out clearly and concisely the most relevant provisions. These may make use of infographics or video statements where appropriate. (Paragraph 109)

10. Where children are permitted to access or use a service age-appropriate terms and conditions must be provided. These should be written in language clearly understandable to children of the minimum age allowed on the platform. (Paragraph 110)

11. Maximum privacy and safety settings should be included in services by default. The Information Commissioner's Office should provide guidance requiring platforms to provide greater choice to users to control how their data are collected and used. (Paragraph 115)

12. Regulators must ensure that terms of service are fair and must bring enforcement action against organisations which routinely breach their terms of service. (Paragraph 116)

13. Design principles and standards are a normal part of business life across all sectors. Establishing and enforcing standards that would meet the 10 principles would help to reduce harms to users and society. We recommend that regulation should follow the precautionary principle to ensure ethical design while also recognising the importance of innovation and entrepreneurship. (Paragraph 120)

14. We recommend that the ethical approach outlined in our 10 principles should be embedded in the teaching of all levels of computer science. The Government should promote and support this. The Centre for Data Ethics and Innovation will also have a role in providing guidance which can be incorporated into teaching, as well as educating users on the ethics and risks of the internet. (Paragraph 121)

Market concentration

15. Mergers and acquisitions should not allow large companies to become data monopolies. We recommend that in its review of competition law in the context of digital markets the Government should consider implementing a public-interest test for data-driven mergers and acquisitions. The public-interest standard would be the management, in the public interest and through competition law, of the accumulation of data. If necessary, the Competition and Markets Authority (CMA) could therefore intervene as

it currently does in cases relevant to media plurality or national security. (Paragraph 150)

16. The modern internet is characterised by the concentration of market power in a small number of companies which operate online platforms. These services have been very popular and networks effects have helped them to become dominant. Yet the nature of digital markets challenges traditional competition law. The meticulous ex post analyses that competition regulators use struggle to keep pace with the digital economy. The ability of platforms to cross-subsidise their products and services across markets to deliver them free or discounted to users challenges traditional understanding of the consumer welfare standard. (Paragraph 161)

17. In reviewing the application of competition law to digital markets, the Government should recognise the inherent power of intermediaries and broaden the consumer welfare standard to ensure that it takes adequate account of long-term innovation. The Government should work with the Competition and Markets Authority (CMA) to make the process for imposing interim measures more effective. (Paragraph 162)

18. We take this opportunity to repeat the recommendation that we made in our report 'UK advertising in a digital world' that the CMA should undertake a market study of the digital advertising market. We would be grateful for an update from the Government and the CMA. (Paragraph 163)

19. Online communications platforms act as gatekeepers for the internet, controlling what users can access and how they behave. They can be compared to utilities in the sense that users feel they cannot do without them and so have limited choice but to accept their terms of service. Providers of these services currently have little incentive to address concerns about data misuse or online harms, including harms to society (Paragraph 172)

20. It is appropriate to put special obligations on these companies to ensure that they act fairly to users, other companies and in the interests of society. These obligations should be drawn up in accordance with the 10 principles we have set out earlier in this report and enforced by a regulator. (Paragraph 173)

21. It is too early to say how effective the right to data portability will be. It has the potential to help counteract the switching costs which lock users into services by giving them more autonomy over and control of their data. This will require greater interoperability. Portability would be more effective if the right applied to social graphs and other inferred data. The Centre for Data Ethics and Innovation should play a role developing best practice in this area. The Information Commissioner's Office should monitor the operation and effectiveness of this right and set out the basis on which it will be enforced. (Paragraph 180)

Online platforms

22. Some have argued that the conditional exemption from liability should be abolished altogether. It has been suggested that using artificial intelligence to identify illegal content could allow companies to comply with strict liability. However, such technology is not capable of identifying illegal content accurately and can have a discriminatory effect. Imposing strict liability would therefore have a chilling effect on freedom of speech. These

concerns would need to be addressed before the 'safe harbour' provisions of the e-Commerce Directive are repealed. (Paragraph 194)

23. Online platforms have developed new services which were not envisaged when the e-Commerce Directive was introduced. They now play a key role in curating content for users, going beyond the role of a simple hosting platform. As such, they can facilitate the propagation of illegal content online. 'Notice and takedown' is not an adequate model for content regulation. Case law has already developed on situations where the conditional exemption from liability under the e-Commerce Directive should not apply. Nevertheless, the directive may need to be revised or replaced to reflect better its original purpose. (Paragraph 195)

24. Technology companies provide venues for illegal content and other forms of online abuse, bullying and fake news. Although they acknowledge some responsibility, their responses are not commensurate with the scale of the problem. We recommend that a duty of care should be imposed on online services which host and curate content which can openly be uploaded and accessed by the public. This would aim to create a culture of risk management at all stages of the design and delivery of services. (Paragraph 207)

25. To be effective, a duty of care would have to be upheld by a regulator with a full set of enforcement powers. Given the urgency of the need to address online harms, we believe that in the first instance the remit of Ofcom should be expanded to include responsibility for enforcing the duty of care. Ofcom has experience of surveying digital literacy and consumption, and experience in assessing inappropriate content and balancing it against other rights, including freedom of expression. It may be that in time a new regulator is required. (Paragraph 208)

26. Content moderation is often ineffective in removing content which is either illegal or breaks community standards. Major platforms have failed to invest in their moderation systems, leaving moderators overstretched and inadequately trained. There is little clarity about the expected standard of behaviour and little recourse for a user to seek to reverse a moderation decision against them. In cases where a user's content is blocked or removed this can impinge their right to freedom of expression. (Paragraph 224)

27. Community standards should be easily accessible to users and written in plain English. Ofcom should have power to investigate whether the standards are being upheld and to consider appeals against moderation decisions. Ofcom should be empowered to impose fines against a company if it finds that the company persistently breaches its terms of use. (Paragraph 225)

28. The sector should collaborate with Ofcom to devise a labelling scheme for social media websites and apps. A classification framework similar to that of the British Board of Film Classification would help users to identify more quickly the risks of using a platform. This would allow sites which wish to allow unfettered conversation or legal adult material to do so. Users could then more easily choose between platforms with stricter or more relaxed community standards. (Paragraph 226)

29. Community standards and classifications should be consistent with a platform's age policy. (Paragraph 228)

The Digital Authority

30. We recommend that a new body, which we call the Digital Authority, should be established to co-ordinate regulators in the digital world. We recommend that the Digital Authority should have the following functions: to continually assess regulation in the digital world and make recommendations on where additional powers are necessary to fill gaps;

    - to establish an internal centre of expertise on digital trends which helps to scan the horizon for emerging risks and gaps in regulation;
    - to help regulators to implement the law effectively and in the public interest, in line with the 10 principles set out in this report;
    - to inform Parliament, the Government and public bodies of technological developments;
    - to provide a pool of expert investigators to be consulted by regulators for specific investigations;
    - to survey the public to identify how their attitudes to technology change over time, and to ensure that the concerns of the public are taken into account by regulators and policy-makers;
    - to raise awareness of issues connected to the digital world among the public;
    - to engage with the tech sector;
    - to ensure that human rights and children's rights are upheld in the digital world;
    - to liaise with European and international bodies responsible for internet regulation. (Paragraph 240)

31. Policy-makers across different sectors have not responded adequately to changes in the digital world. The Digital Authority should be empowered to instruct regulators to address specific problems or areas. In cases where this is not possible because problems are not within the remit of any regulator, the Digital Authority should advise the Government and Parliament that new or strengthened legal powers are needed. (Paragraph 241)

32. The Digital Authority will co-ordinate regulators across different sectors and multiple Government department. We therefore recommend that it should report to the Cabinet Office and be overseen at the highest level. (Paragraph 245)

33. We recommend that a joint committee of both Houses of Parliament should be established to consider matters related to the digital environment. In addition to advising the Government the Digital Authority should report to Parliament on a quarterly basis and regularly give evidence to the new joint committee to discuss the adequacy of powers and resources in regulating the digital world. The combined force of the Digital Authority and the joint committee will bring a new consistency and urgency to regulation. (Paragraph 246)

APPENDIX 1: LIST OF MEMBERS AND DECLARATIONS OF INTEREST

Members

Lord Allen of Kensington
Baroness Benjamin
Baroness Bertin
Baroness Bonham-Carter of Yarnbury
The Lord Bishop of Chelmsford
Baroness Chisholm of Owlpen (from June 2018)
Viscount Colville of Culross
Lord Gilbert of Panteg (Chairman)
Lord Goodlad
Lord Gordon of Strathblane
Baroness Kidron
Baroness McIntosh of Hudnall
Baroness Quin

Declarations of interest

Lord Allen of Kensington

Chairman, Global Media & Entertainment (including Global Radio)

Chairman, Moelis & Company (an independent advisory bank which advises media companies)

Declarable shareholding, ITV plc

Baroness Benjamin

Actress and TV presenter who is often employed to do adverts/voiceovers for commercials and appear on TV

Member, BBC Diversity Panel

Vice President, Bernardo's

Champion, Internet Watch Foundation

Member, Children's Media Foundation

Baroness Bertin

Employee (part-time), BT

Baroness Bonham-Carter of Yarnbury

No relevant interests declared

Bishop of Chelmsford

No relevant interests declared

Baroness Chisholm of Owlpen

No relevant interests declared

Viscount Colville of Culross

Series Producer, ITN Productions, 6-month contract for Channel 5 commission

Lord Gilbert of Panteg (Chairman)

Commissioner, Electoral Commission

Director, Stephen Gilbert Consulting (Member's consultancy dealing in public-opinion research and communications strategy); current personal clients:

(i) The Conservative Party;

(ii) Finsbury, a public relations company owned by WPP

Lord Goodlad

Member, Advisory Board of GovNet Communications Ltd

Lord Gordon of Strathblane

Small shareholding in Johnston Press PLC

Baroness Kidron

Founder, 5Rights Foundation

Working on universal data standards with many international partners

Member, Broadband Commission on the Sustainable Development Goals

Member, Royal Foundation's Task Force on Cyberbullying

Member, Child Dignity Alliance Technical Working Group

Director, Freeformers (a digital transformation company)

Workshops with children to capture their thinking about the digital environment

Author of report on persuasive design 'Disrupted Childhood: The Cost of Persuasive Design'

Baroness McIntosh of Hudnall

No relevant interests declared

Baroness Quin

No relevant interests declared

A full list of Members' interests can be found in the Register of Lords' Interests: http://www.publications.parliament.uk/pa/ld/ldreg.htm

Specialist advisor

Professor Andrew Murray

Commissioner, LSE Truth, Trust and Technology Commission

APPENDIX 2: LIST OF WITNESSES

Evidence is published online at http://www.parliament.uk/internet-regulation and available for inspection at the Parliamentary Archives (020 7219 3074).

Evidence received by the Committee is listed below in chronological order of oral evidence session and in alphabetical order. Those witnesses marked with ** gave both oral evidence and written evidence. Those marked with * gave oral evidence and did not submit any written evidence. All other witnesses submitted written evidence only.

Oral evidence in chronological order

**	Professor Christopher Marsden, Professor of Internet Law, University of Sussex	QQ 1–11
*	Dr Victoria Nash, Deputy Director, Policy and Research Fellow, Oxford Internet Institute	
**	Professor Lorna Woods, Professor of Internet Law, University of Essex	
*	Mark Bunting, Partner, Communications Chambers	QQ 12–20
**	Dr Damian Tambini, Associate Professor, Department of Media and Communications, London School of Economics	
**	Myles Jackman, Legal Director; and Javier Ruiz Diaz, Policy Director, Open Rights Group	QQ 21–27
**	Rachel Coldicutt, CEO, Doteveryone	QQ 28–34
*	Julian Coles, independent digital media policy consultant	
**	Dr Konstantinos Komaitis, Director of Policy Development, Internet Society	
**	Susie Hargreaves OBE, Chief Executive Officer, Internet Watch Foundation	QQ 35–43
*	Chief Constable Stephen Kavanagh, National Police Chiefs' Council	
*	Will Kerr, Director of Vulnerabilities; and Donald Toon, Director of Prosperity, National Crime Agency	
*	Detective Superintendent Phil Tomlinson, Head of National Digital Exploitation Service, Metropolitan Police	
*	Dom Hallas, Executive Director, Coadec	QQ 44–51
**	Antony Walker, Deputy Chief Executive, techUK	
*	Jamie Bartlett, Director, Centre for the Analysis of Social Media at Demos	QQ 52–57

**	Robert Colvile, Director, Centre for Policy Studies	
*	Laurie Laybourn-Langton, Senior Research Fellow, Institute for Public Policy Research	
**	Jenny Afia, Partner, Schillings	QQ 58–70
*	Mark Stephens CBE, Partner, Howard Kennedy LLP	
*	Professor Sonia Livingstone OBE, Professor of Social Psychology, London School of Economics	QQ 71–82
**	Tony Stower, Head of Child Safety Online, NSPCC	
*	Professor Pinar Akman, Professor of Competition Law, University of Leeds	QQ 83–92
*	Dr Orla Lynskey, Assistant Professor of Law, London School of Economics and Political Science	
*	Dr Nicolo Zingales, Lecturer in Competition and Information Law, University of Sussex	
*	Dr Ewa Luger, Chancellor's Fellow, Digital Arts and Humanities, University of Edinburgh	QQ 93–102
**	Professor John Naughton, Senior Research Fellow, Centre for Research in the Arts, Social Sciences and Humanities, University of Cambridge	
*	Daniel Butler, Head of Public Affairs and Policy, Virgin Media	QQ 103–112
**	Adam Kinsley, Director of Policy, Sky	
**	Iain Wood, Director of Corporate Affairs and Regulation, TalkTalk Group	
**	Elizabeth Denham, Information Commissioner, Information Commissioner's Office	QQ 113–121
*	Nick Pickles, Senior Strategist, Public Policy, Twitter	QQ 122–127
*	Jared Sine, General Counsel & Secretary, Match Group	
*	Kevin Bakhurst, Group Director, Content and Media Policy; and Yih Choung Teh, Group Director, Strategy and Research. Ofcom	QQ 128–134
**	Dr Andrea Coscelli, Chief Executive Officer; and Simon Constantine, Director, Policy and International, Competition and Markets Authority	QQ 135–142

**	Dan Brooke, Chief Marketing and Communications Officer, Channel 4	QQ 143–151
**	Magnus Brooke, Director of Policy and Regulatory Affairs, ITV	
**	Clare Sumner CBE, Director, Policy, BBC	
**	Mark Bridge, Technology Correspondent, The Times	QQ 152–160
*	Alex Hern, Technology Reporter, the Guardian	
*	Matt Reynolds, Staff Writer, Wired UK	
**	Caroline Normand, Director of Policy, Which?	QQ 161–173
**	Hugh Milward, Director of Corporate, Legal and External Affairs, Microsoft	QQ 174–182
**	Katie O'Donovan, Public Policy Manager, Google UK	
**	Rebecca Stimson, Head of Public Policy, Facebook UK	
**	Margot James MP, Minister for Digital and the Creative Industries, Department for Digital, Culture, Media and Sport	QQ 183–196
*	Lesley Smith, Director Public Policy, UK & Ireland, Amazon	QQ 197–208

Alphabetical list of all witnesses

	The Adam Smith Institute	IRN0070
	Advertising Association	IRN0039
	Airbnb	IRN0091
*	Professor Pinar Akman (QQ 83–92)	
	All Rise Say No to Cyber Abuse	IRN0037
	Alliance for Intellectual Property	IRN0096
*	Amazon (QQ 197–208)	
	Professor Leighton Andrews, Cardiff Business School	IRN0041
	ARTICLE 19	IRN0095
	Association for Proper Internet Governance	IRN0001
	Association of School and College Leaders (ASCL)	IRN0005
	Dr Shehar Bano	IRN0114
	BASCA	IRN0027
**	BBC (QQ 143–151)	IRN0102
		IRN0119

	BBFC	IRN0068
	BCS, The Chartered Institute for IT	IRN0092
	Dr Paul Bernal, University of East Anglia Law School	IRN0019
	Big Brother Watch	IRN0115
	BPI	IRN0081
	Brass Horn Communications	IRN0044
	Bristol Safeguarding Children's Board E-Safety Working Group	IRN0009
	British and Irish Legal Education and Technology Association (BILETA)	IRN0029
*	Mark Bunting (QQ 12–20)	
	Dr Rosie Campbell OBE, University of Leicester	IRN0017
	CARE	IRN0024
	CBI	IRN0054
	Centre for Competition Policy, University of East Anglia	IRN0020
	Centre for International Governance Innovation	IRN0014
**	Centre for Policy Studies (QQ 52–57)	IRN0111
*	Centre for the Analysis of Social Media at Demos (QQ 52–57)	
	Centre for the Response to Radicalisation and Terrorism, The Henry Jackson Society	IRN0093
**	Channel 4 (QQ 143–151)	IRN0105 IRN0117
	Children's Charities' Coalition on Internet Safety	IRN0008
	The Children's Media Foundation	IRN0033
	The Children's Society	IRN0025
	Cloudflare	IRN0064
*	Coalition for a Digital Economy (Coadec) (QQ 44–51)	
	Jennifer Cobbe, Trustworthy Technologies Strategic Research Initiative, University of Cambridge	IRN0031
*	Julian Coles (QQ 28–34)	
**	Competition and Markets Authority (QQ 135–142)	IRN0100

	Cybersalon	IRN0030
	Digital UK	IRN0062
**	Doteveryone (QQ 28–34)	IRN0028
		IRN0103
	The Entrepreneurs Network	IRN0070
	Dr David Erdos	IRN0074
	eSafe Global Ltd	IRN0022
**	Facebook UK (QQ 174–182)	IRN0098
		IRN0126
	Full Fact	IRN0071
	Professor Christian Fuchs, Professor of Media and Communication Studies, University of Westminster	IRN0010
	The Global Network Initiative (GNI)	IRN0046
	Global Partners Digital	IRN0099
**	Google UK (QQ 174–182)	IRN0088
		IRN0121
	Clive Gringras	IRN0110
*	The Guardian (QQ 152–160)	
	Dr Yohko Hatada	IRN0082
**	Her Majesty's Government (QQ 183–196)	IRN0109
		IRN0124
	Horizon Digital Economy Research Institute, University of Nottingham	IRN0038
*	Mark Stephens CBE, Partner, Howard Kennedy LLP (QQ 58–70)	
	IAB UK	IRN0097
**	Information Commissioner's Office (QQ 113–121)	IRN0087
		IRN0120
	Information Law and Policy Centre, Institute for Advanced Legal Studies	IRN0063
	Institute of Practitioners in Advertising (IPA)	IRN0045
*	Institute for Public Policy Research (QQ 52–57)	
	Internet Commission	IRN0004
	Internet Service Providers' Association (ISPA UK)	IRN0108
**	Internet Society (QQ 28–34)	IRN0076
**	Internet Watch Foundation (QQ 35–43)	IRN0034

	ISBA	IRN0049
**	ITV plc (QQ 143–151)	IRN0122
	Law Society of Scotland	IRN0057
	Matthieu Le Berre	IRN0066
	LINX	IRN0055
*	Professor Sonia Livingstone (QQ 71–82)	
*	Dr Ewa Luger (QQ 93–102)	
*	Dr Orla Lynskey (QQ 83–92)	
	McEvedys Solicitors & Attorneys Ltd	IRN0065
	Bishoy Maher	IRN0015
	Dr Stephann Makri	IRN0113
**	Professor Christopher Marsden (QQ 1–11)	IRN0080
*	Match Group (QQ 122–127)	
	The Mayor of London	IRN0094
*	Metropolitan Police (QQ 35–43)	
**	Microsoft UK (QQ 174–182)	IRN0085
		IRN0125
	Motion Picture Association	IRN0089
*	Dr Victoria Nash (QQ 1–11)	
*	National Crime Agency (QQ 35–43)	
*	National Police Chief's Council (QQ 35–43)	
**	Professor John Naughton, Trustworthy Technologies Strategic Research Initiative, University of Cambridge (QQ 93–102)	IRN0031
	News Media Association	IRN0059
	NINSO (The Northumbria Internet & Society Research Interest Group)	IRN0035
	Nominet	IRN0053
	Emma Nottingham, University of Winchester	IRN0018
*	Tony Stower, Head of Child Safety Online, NSPCC (QQ 71–82)	
	Oath	IRN0107
	Dr Rachel O'Connell	IRN0075
*	Ofcom (QQ 128–134)	
	Office of the eSafety Commissioner, Australian Government	IRN0016
	Stephen Oliver	IRN0058
	Open Data Institute	IRN0073

**	Open Rights Group (QQ 21–27)	IRN0090
	Marion Oswald, University of Winchester	IRN0018
	Pact	IRN0003
	William Perrin	IRN0047
	Policy Exchange	IRN0072
	Procter & Gamble	IRN0104
	Lilian Edwards, Professor of eGovernance	IRN0069
	Radiocentre	IRN0048
	Jacob Rowbottom	IRN0026
	Royal Academy of Engineering	IRN0078
	The Royal Society	IRN0084
	Helen Ryan, University of Winchester	IRN0018
	Professor Teela Sanders, University of Leicester	IRN0017
**	Jenny Afia, Partner, Schillings (QQ 58–70)	IRN0032
	Professor Jane Scoular, University of Strathclyde	IRN0017
	The Self-Esteem Team (SET)	IRN0005
**	Sky (QQ 103–112)	IRN0060
	Stanford Law School Center for Internet and Society	IRN0052
	Subforum LLC	IRN0013
	Professor Richard Tait	IRN0042
	Rahim Talibzade	IRN0015
**	TalkTalk Group (QQ 103–112)	IRN0083
**	Dr Damian Tambini (QQ 12–20)	IRN0101
**	techUK (QQ 44–51)	IRN0086
		IRN0112
	Thinkbox	IRN0056
**	The Times (QQ 152–160)	IRN0118
	TripAdvisor	IRN0106
*	Twitter (QQ 122–127)	
	UK Computing Research Committee (UKCRC)	IRN0011
	UK Council for Child Internet Safety's Evidence Group	IRN0079
	UK Music	IRN0040
	UK Safer Internet Centre (UKSIC)	IRN0061
	Michael Veale, University College London	IRN0077

	Adrian Venditti	IRN0002
*	Virgin Media (QQ 103–112)	
	WebRoots Democracy	IRN0043
**	Which? (QQ 161–173)	IRN0116
		IRN0123
	Robert White	IRN0012
*	Wired UK (QQ 152–160)	
**	Professor Lorna Woods (QQ 1–11)	IRN0047
	Yoti	IRN0067
	YoungMinds	IRN0025
*	Dr Nicolo Zingales (QQ 83–92)	

APPENDIX 3: CALL FOR EVIDENCE

The House of Lords Select Committee on Communications, under the chairmanship of Lord Gilbert of Panteg, is to hold an inquiry into the how regulation of the internet should be improved. The Committee invites any interested organisation or individual to submit written evidence to the inquiry by Friday 11 May 2018.

The Committee expects to hear oral evidence from invited witnesses from April to September 2018 and intends to report towards the end of 2018. The Government has undertaken to respond in writing to reports from select committees.

Background

The internet has transformed how people around the world interact with one another, gather information and consume educational and entertaining content. It has 3.2 billion users.

The internet opens up new opportunities but also presents challenges. It is a platform for fake news, hate speech, abusive messages and extremist content. Democracy relies on a diversity of views but many news feeds use algorithms that direct users to content that echoes their own views.

In exchange for using services on the internet, users permit online platforms such as Google and Facebook to use their personal data to sell advertising. Users' relationship with online platforms raises questions over third-party access, transparency and accountability.

While there is no specific regulator for the internet in the UK, a number of statutory and non-governmental organisations regulate behaviour associated with the internet. For example, the Information Commissioner's Office has responsibility for data protection and privacy; Ofcom regulates TV-like content from on-demand programme services; and the Advertising Standards Authority is an industry body responsible for online advertising standards.

Online platforms have immunity under EU law from liability as a publisher for user-generated content on the ground that they do not exercise editorial control.[263] They are required, however, to remove illegal content as quickly as possible on obtaining knowledge of it. Many online platforms remove or otherwise 'moderate' content which does not comply with community standards. But some commentators have questioned whether such moderation is adequate to protect users and whether it is appropriate for private companies to exercise such power.[264]

In October 2017 the Government published its Internet Safety Strategy green paper. It is underpinned by the principle that "what is unacceptable offline should be unacceptable online".[265] In January 2018, the Government published its Digital Charter, which stated that that the Government will seek to establish norms and rules for the online world. This rolling programme of work might involve agreeing new standards, shifting expectations of behaviour and updating laws and

263 The E-Commerce Directive 2000/31/EC

264 'To censor or sanction extreme content? Either way, Facebook can't win', The Guardian (23 May 2017): https://www.theguardian.com/news/2017/may/22/facebook-moderator-guidelines-extreme-content-analysis [accessed 29 March 2018]

265 Department for Digital, Culture, Media and Sport, Internet Safety Strategy Green Paper, October 2017 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf [accessed 29 March 2018]

regulations. The Government will also consider "the legal liability that online platforms have for the content shared on their sites, including considering how we could get more effective action through better use of the existing legal frameworks and definitions".[266]

The Committee has previously investigated the functioning of the internet's advertising market and explored the relationship between children and the internet. In its report Growing up with the Internet the Committee found that responsibility for protecting children online was fragmented and recommended that the Government and businesses should develop a code of conduct for the internet.

Aim of the inquiry

Building on the work of previous inquiries, the Committee wishes to explore how the regulation of the internet should be improved, including through better self-regulation and governance, and whether a new regulatory framework for the internet is necessary or whether the general law of the UK is adequate. This inquiry will consider whether online platforms which mediate individuals' use of the internet have sufficient accountability and transparency, adequate governance and provide effective behavioural standards for users.

In launching this inquiry, the Committee notes that the Government's Digital Charter seeks to make the UK the safest place to be online and that the UK should lead the world in innovation-friendly regulation. The Government's stated aim is to increase public confidence and trust in new technologies and create the foundations for the UK digital economy to thrive.

The Committee seeks written evidence which addresses the following questions. Witnesses need not answer every question; experts in a particular area are encouraged to focus on that area. Witnesses may also address relevant issues that are not covered below provided that they explain the significance of the issues.

Questions

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

2. What should the legal liability of online platforms be for the content that they host?

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

6. What information should online platforms provide to users about the use of their personal data?

---

266 Department for Digital, Culture, Media and Sport, Digital Charter, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/676715/2018–01-25_Digital_Charter_final.pdf [accessed 29 March 2018]

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

29 March 2018

APPENDIX 4: EXISTING REGULATORS

This appendix lists of statutory and non-statutory bodies which have remits for online regulation. Of these bodies only the Internet Watch Foundation is exclusively concerned with the internet. The list is not exhaustive.

Advertising Standards Authority: remit includes advertisements on the internet, smartphone and tables, claims on companies' websites and commercial emails. It also regulates Online Behavioural Advertising (OBA). Regulation requires businesses to make clear when they are collecting and using information for OBA and to provide a tool so that individuals can choose not to receive it.

British Board of Film Classification (BBFC): provides the classification framework for mobile operators to restrict access to their commercial content that is unsuitable for customers under the age of 18. The BBFC is the designated regulator for the age verification of online pornography under Digital Economy Act 2017.

Competition and Markets Authority: responsible for strengthening business competition, and preventing and reducing anti-competitive activities, including by UK businesses which are active in the online economy. It investigates mergers and conducts market studies, including on internet-based businesses.

Direct Marketing Commission (DMC): an independent watchdog for the members of the Direct Marketing Association (DMA), a trade organisation which promotes direct marketing, including direct digital marketing. The DMC investigates and adjudicates reported breaches of the DMA's code. It aims to safeguard consumers' right to be contacted in the way they wish.

Financial Conduct Authority: regulates financial firms which provide services to consumers, including in the online economy. This includes reviewing financial firms' use of customer data, monitoring unauthorised internet banks, regulating firms which operate loan-based crowdfunding platforms and regulating the use of cryptocurrencies.

Gambling Commission: regulates online gambling activity by monitoring compliance with legislation, licence conditions and codes of practice. This includes ensuring internet gambling websites and apps meet existing regulatory requirements, including the right of consumers to access information on their gambling activity and net deposits, and to set financial limits on their accounts.

IMPRESS: is an independent regulator for press publications, including online editions. It was the first to be recognised by the Press Recognition Panel and is fully compliant with the recommendations of the Leveson Inquiry.

Independent Press Standards Organisation (IPSO): regulates the majority of UK local, regional and national publications. IPSO can investigate complaints that a publication has breached the Editors' Code and may ensure publications uphold factual standards. The organisation has launched a symbol to be used by publications regulated by the body to combat 'fake news'.

Information Commissioner's Office: enforces and oversees the Freedom of Information Act 2000, the Environmental Information Regulations, the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations.

Internet Watchdog Foundation: remit is to remove child sexual abuse content hosted anywhere in the world and non-photographic child sexual abuse images hosted in the UK.

Ofcom: regulates online services platforms, including BBC iPlayer and other catch-up services in line with its principles for broadcast media. It also regulates subscription services, although with more limited standards than live TV and catch-up services.

Phone-paid Services Authority: the regulator for content, goods and services charged to phone bills. This includes internet-based apps and services such as music subscriptions, in-app purchases, gaming and adult services.

Prudential Regulation Authority: responsible for the prudential regulation and supervision of banks, building societies, credit unions, insurers and major investment firms. This includes online activities undertaken by these firms.