House of Commons

Digital, Culture, Media and Sport Committee

Disinformation and 'fake news': Interim Report

Fifth Report of Session 2017–19

Report, together with formal minutes relating to the report

Ordered by the House of Commons
to be printed 24 July 2018

HC 363
Published on 29 July 2018
by authority of the House of Commons

The Digital, Culture, Media and Sport Committee

The Digital, Culture, Media and Sport Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Department for Digital, Culture, Media and Sport and its associated public bodies.

Current membership

Damian Collins MP (*Conservative, Folkestone and Hythe*) (Chair)

Clive Efford MP (*Labour, Eltham*)

Julie Elliott MP (*Labour, Sunderland Central*)

Paul Farrelly MP (*Labour, Newcastle-under-Lyme*)

Simon Hart MP (*Conservative, Carmarthen West and South Pembrokeshire*)

Julian Knight MP (*Conservative, Solihull*)

Ian C. Lucas MP (*Labour, Wrexham*)

Brendan O'Hara MP (*Scottish National Party, Argyll and Bute*)

Rebecca Pow MP (*Conservative, Taunton Deane*)

Jo Stevens MP (*Labour, Cardiff Central*)

Giles Watling MP (*Conservative, Clacton*)

The following Members were also members of the Committee during the inquiry

Christian Matheson MP (*Labour, City of Chester*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/dcmscom and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are Chloe Challender (Clerk), Joe Watt (Second Clerk), Lauren Boyer (Second Clerk), Josephine Willows (Senior Committee Specialist), Lois Jeary (Committee Specialist), Andy Boyd (Senior Committee Assistant), Keely Bishop (Committee Assistant), Lucy Dargahi (Media Officer) and Janet Coull Trisic (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Digital, Culture, Media and Sport Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 6188; the Committee's email address is cmscom@parliament.uk

Contents

Summary

There are many potential threats to our democracy and our values. One such threat arises from what has been coined 'fake news', created for profit or other gain, disseminated through state-sponsored programmes, or spread through the deliberate distortion of facts, by groups with a particular agenda, including the desire to affect political elections.

Such has been the impact of this agenda, the focus of our inquiry moved from understanding the phenomenon of 'fake news', distributed largely through social media, to issues concerning the very future of democracy. Arguably, more invasive than obviously false information is the relentless targeting of hyper-partisan views, which play to the fears and prejudices of people, in order to influence their voting plans and their behaviour. We are faced with a crisis concerning the use of data, the manipulation of our data, and the targeting of pernicious views. In particular, we heard evidence of Russian state-sponsored attempts to influence elections in the US and the UK through social media, of the efforts of private companies to do the same, and of law-breaking by certain Leave campaign groups in the UK's EU Referendum in their use of social media.

In this rapidly changing digital world, our existing legal framework is no longer fit for purpose. This is very much an interim Report, following an extensive inquiry. A further, substantive Report will follow in the autumn of 2018. We have highlighted significant concerns, following recent revelations regarding, in particular, political manipulation and set we out areas where urgent action needs to be taken by the Government and other regulatory agencies to build resilience against misinformation and disinformation into our democratic system. Our democracy is at risk, and now is the time to act, to protect our shared values and the integrity of our democratic institutions.

1 Introduction and background

1. In this inquiry, we have studied the spread of false, misleading, and persuasive content, and the ways in which malign players, whether automated or human, or both together, distort what is true in order to create influence, to intimidate, to make money, or to influence political elections.

2. People are increasingly finding out about what is happening in this country, in their local communities, and across the wider world, through social media, rather than through more traditional forms of communication, such as television, print media, or the radio.[1] Social media has become hugely influential in our lives.[2] Research by the Reuters Institute for the Study of Journalism has shown that not only are huge numbers of people accessing news and information worldwide through Facebook, in particular, but also through social messaging software such as WhatsApp. When such media are used to spread rumours and 'fake news', the consequences can be devastating.[3]

3. Tristan Harris, Co-founder and Executive Director, at the Center for Humane Technology—an organisation seeking to realign technology with the best interests of its users—told us about the many billions of people who interact with social media: "There are more than 2 billion people who use Facebook, which is about the number of conventional followers of Christianity. There are about 1.8 billion users of YouTube, which is about the number of conventional followers of Islam. People check their phones about 150 times a day in the developed world."[4] This equates to once every 6.4 minutes in a 16-hour day. This is a profound change in the way in which we access information and news, one which has occurred without conscious appreciation by most of us.

4. This kind of evidence led us to explore the use of data analytics and psychological profiling to target people on social media with political content, as its political impact has been profound, but largely unappreciated. The inquiry was launched in January 2017 in the previous Parliament, and then relaunched in the autumn, following the June 2017 election. The inquiry's Terms of Reference were as follows:

- What is 'fake news'? Where does biased but legitimate commentary shade into propaganda and lies?
- What impact has fake news on public understanding of the world, and also on the public response to traditional journalism? If all views are equally valid, does objectivity and balance lose all value?
- Is there any difference in the way people of different ages, social backgrounds, genders etc use and respond to fake news?
- Have changes in the selling and placing of advertising encouraged the growth of fake news, for example by making it profitable to use fake news to attract more hits to websites, and thus more income from advertisers?[5]

1 News consumption in the UK: 2016, Ofcom, 29 June 2017
2 Tristan Harris, Co-founder and Executive Director, Center for Humane Technology, Q3147
3 The seventh annual Digital News Report, by the Reuters Institute for the Study of Journalism, University of Oxford was based on a YouGov online survey of 74,000 people in 37 countries.
4 Tristan Harris, Q3147
5 Terms of reference, Fake News inquiry, DCMS Committee, 15 September 2017.

5. We will address the wider areas of our Terms of Reference, including the role of advertising, in our further Report this autumn. In recent months, however, our inquiry delved increasingly into the political use of social media, raising concerns that we wish to address immediately. We had asked representatives from Facebook, in February 2018, about Facebook developers and data harvesting.[6] Then, in March 2018, Carole Cadwalladr of *The Observer*,[7] together with Channel 4 News, and the *New York Times*, published allegations about Cambridge Analytica (and associated companies) and its work with Global Science Research (GSR), and the misuse of Facebook data.[8] Those allegations put into question the use of data during the EU Referendum in 2016, and the extent of foreign interference in UK politics. Our oral evidence sessions subsequently focussed on those specific revelations, and we invited several people involved to give evidence. The allegations highlighted both the amount of data that private companies and organisations hold on individuals, and the ability of technology to manipulate people.

6. This transatlantic media coverage brought our Committee into close contact with other parliaments around the world. The US Senate Select Committee on Intelligence, the US House of Representatives Permanent Select Committee on Intelligence, the European Parliament, and the Canadian Standing Committee on Access to Information, Privacy, and Ethics all carried out independent investigations. We shared information, sometimes live, during the hearings. Representatives from other countries, including Spain, France, Estonia, Latvia, Lithuania, Australia, Singapore, Canada, and Uzbekistan, have visited London, and we have shared our evidence and thoughts. We were also told about the work of SCL Elections—and other SCL associates, including Cambridge Analytica—set up by the businessman Alexander Nix; their role in manipulating foreign elections; and the financial benefits they gained through those activities. What became clear is that, without the knowledge of most politicians and election regulators across the world, not to mention the wider public, a small group of individuals and businesses had been influencing elections across different jurisdictions in recent years.

7. We invited many witnesses to give evidence. Some came to the Committee willingly, others less so. We were forced to summon two witnesses: Alexander Nix, former CEO of Cambridge Analytica; and Dominic Cummings, Campaign Director of Vote Leave, the designated Leave campaign group in the EU Referendum. While Mr. Nix subsequently agreed to appear before the Committee, Dominic Cummings still refused. We were then compelled to ask the House to support a motion ordering Mr Cummings to appear before the Committee.[9] At the time of writing he has still not complied with this Order, and the matter has been referred by the House to the Committee of Privileges. Mr Cummings' contemptuous behaviour is unprecedented in the history of this Committee's inquiries and underlines concerns about the difficulties of enforcing co-operation with Parliamentary scrutiny in the modern age. We will return to this issue in our Report in the autumn, and believe it to be an urgent matter for consideration by the Privileges Committee and by Parliament as a whole.

6 Monika Bickert, Q389

7 In June 2018, Carole Cadwalladr won the Orwell journalism prize, for her investigative work into Cambridge Analytica, which culminated in a series of articles from March 2018.

8 Harry Davies had previously published the following article Ted Cruz using firm that harvested data on millions of unwitting Facebook users, in The Guardian, on 11 December 2015, which first revealed the harvesting of data from Facebook.

9 Following the motion being passed, Dominic Cummings did not appear before the Committee. The matter was then referred to the Privileges Committee on 28 June 2018.

8. In total, we held twenty oral evidence sessions, including two informal background sessions, and heard from 61 witnesses, asking over 3,500 questions at these hearings. We received over 150 written submissions, numerous pieces of background evidence, and undertook substantial exchanges of correspondence with organisations and individuals. We held one oral evidence session in Washington D.C. (the first time a Select Committee has held a public, live broadcast oral evidence session abroad) and also heard from experts in the tech field, journalists and politicians, in private meetings, in Washington and New York. Most of our witnesses took the Select Committee process seriously, and gave considered, thoughtful evidence, specific to the context of our inquiry. We thank witnesses, experts, politicians, and individuals (including whistle-blowers) whom we met in public and in private, in this country and abroad, and who have been generous with their expertise, knowledge, help and ideas.[10] We also thank Dr Lara Brown and her team at the Graduate School of Political Management at George Washington University, for hosting the Select Committee's oral evidence session in the US.

9. As noted above, this is our first Report on misinformation and disinformation. Another Report will be published in the autumn of 2018, which will include more substantive recommendations, and also detailed analysis of data obtained from the insecure AggregateIQ website, harvested and submitted to us by Chris Vickery, Director of Cyber Risk Research at UpGuard.[11] Aggregate IQ is one of the businesses involved most closely in influencing elections.

10. Since we commenced this inquiry, the Electoral Commission has reported on serious breaches by Vote Leave and other campaign groups during the 2016 EU Referendum; the Information Commissioner's Office has found serious data breaches by Facebook and Cambridge Analytica, amongst others; the Department for Digital, Culture, Media and Sport (DDCMS) has launched the Cairncross Review into press sustainability in the digital age; and, following a Green Paper in May, 2018, the Government has announced its intention to publish a White Paper later this year into making the internet and social media safer. This interim Report, therefore, focuses at this stage on seven of the areas covered in our inquiry:

- Definition of fake news, and how to spot it;
- Definition, role and legal liabilities of social media platforms;
- Data misuse and targeting, focussing on the Facebook/Cambridge Analytica/AIQ revelations;
- Political campaigning;
- Foreign players in UK elections and referenda;
- Co-ordination of Departments within Government;
- Digital literacy.

10 Our expert adviser for the inquiry was Dr Charles Kriel, Associate Fellow at the King's Centre for Strategic Communications (KCSC), King's College London. His Declaration of Interests are: Director, Kriel.Agency, a digital media and social data consulting agency; Countering Violent Extremism Programme Director, Corsham Institute, a civil society charity; and Cofounder and shareholder, Lightful, a social media tool for charities.

11 In the early autumn, we hope to invite Ofcom and the Advertising Standards Authority to give evidence, and to re-invite witnesses from the Information Commissioner's Office and the Electoral Commission, and this oral evidence will also inform our substantive Report.

Definition of 'fake news'

11. There is no agreed definition of the term 'fake news', which became widely used in 2016 (although it first appeared in the US in the latter part of the 19th century).[12] Claire Wardle, from First Draft, told us in our oral evidence session in Washington D.C. that "when we are talking about this huge spectrum, we cannot start thinking about regulation, and we cannot start talking about interventions, if we are not clear about what we mean".[13] It has been used by some, notably the current US President Donald Trump, to describe content published by established news providers that they dislike or disagree with, but is more widely applied to various types of false information, including:

- **Fabricated content**: completely false content;
- **Manipulated content**: distortion of genuine information or imagery, for example a headline that is made more sensationalist, often popularised by 'clickbait';
- **Imposter content**: impersonation of genuine sources, for example by using the branding of an established news agency;
- **Misleading content**: misleading use of information, for example by presenting comment as fact;
- **False context of connection**: factually accurate content that is shared with false contextual information, for example when a headline of an article does not reflect the content;
- **Satire and parody**: presenting humorous but false stores as if they are true. Although not usually categorised as fake news, this may unintentionally fool readers.[14]

12. In addition to the above is the relentless prevalence of 'micro-targeted messaging', which may distort people's views and opinions.[15] The distortion of images is a related problem; evidence from MoneySavingExpert.com cited celebrities who have had their images used to endorse scam money-making businesses, including Martin Lewis, whose face has been used in adverts across Facebook and the internet for scams endorsing products including binary trading and energy products.[16] There are also 'deepfakes', audio and videos that look and sound like a real person, saying something that that person has never said.[17] These examples will only become more complex and harder to spot, the more sophisticated the software becomes.

13. There is no regulatory body that oversees social media platforms and written content including printed news content, online, as a whole. However, in the UK, under the Communications Act 2003, Ofcom sets and enforces content standards for television

12 Fake News: A Roadmap, NATO Strategic Centre for Strategic Communications, Riga and King's Centre for Strategic Communications (KCSE), January 2018.

13 Claire Wardle, Q573

14 Online information and fake news, Parliamentary Office of Science and Technology, July 2017, box 4. Also see First Draft News, Fake news. It's complicated, February 2017; Ben Nimmo (FNW0125); Full Fact, (FNW0097)

15 Micro-targeting of messages will be explored in greater detail in Chapter 4.

16 MoneySavingExpert.com (FKN0068)

17 Edward Lucas, Q881

and radio broadcasters, including rules relating to accuracy and impartiality.[18] On 13 July 2018, Ofcom's Chief Executive, Sharon White, called for greater regulation of social media, and announced plans to release an outline of how such regulation could work in the autumn of this year.[19] We shall assess these plans in our further Report.

14. ***The term 'fake news' is bandied around with no clear idea of what it means, or agreed definition. The term has taken on a variety of meanings, including a description of any statement that is not liked or agreed with by the reader. We recommend that the Government rejects the term 'fake news', and instead puts forward an agreed definition of the words 'misinformation' and 'disinformation'. With such a shared definition, and clear guidelines for companies, organisations, and the Government to follow, there will be a shared consistency of meaning across the platforms, which can be used as the basis of regulation and enforcement.***

15. ***We recommend that the Government uses the rules given to Ofcom under the Communications Act 2003 to set and enforce content standards for television and radio broadcasters, including rules relating to accuracy and impartiality, as a basis for setting standards for online content. We look forward to hearing Ofcom's plans for greater regulation of social media this autumn. We plan to comment on these in our further Report.***

How to spot 'fake news'

16. Standards surrounding fact-checking exist, through the International Fact-Checking Network's Code of Principles, signed by the majority of major fact-checkers.[20] A recent report of the independent High-Level Expert Group on Fake News and Online Disinformation highlighted that, while a Code of Principles exists, fact-checkers themselves must continually improve on their own transparency.[21]

17. Algorithms are being used to help address the challenges of misinformation. We heard evidence from Professor Kalina Bontcheva, who conceived and led the Pheme research project, which aims to create a system to automatically verify online rumours and thereby allow journalists, governments and others to check the veracity of stories on social media.[22] Algorithms are also being developed to help to identify fake news. The fact-checking organisation, Full Fact, received funding from Google to develop an automated fact-checking tool for journalists.[23] Facebook and Google have also altered their algorithms so that content identified as misinformation ranks lower.[24] Many organisations are exploring ways in which content on the internet can be verified, kite-marked, and graded according to agreed definitions.[25]

18. ***The Government should support research into the methods by which misinformation and disinformation are created and spread across the internet: a core part of this is fact-***

18 Ofcom (FNW0107)
19 'It's time to regulate social media sites that publish news' *The Times* 13 July 2018
20 The International Fact-Checking Network website, accessed 21 June 2018.
21 A multi-dimensional approach to disinformation, Report of the independent High Level Expert Group on Fake News and Online Disinformation, March 2018.
22 Pheme website, www.pheme.eu, accessed 21 June 2018
23 Full Fact website, fullfact.org, accessed 21 June 2018
24 Mosseri, Facebook, "Working to stop misinformation and false news". 6/4/2017
25 Full Fact (FNW0097); Disinformation Index (FKN0058); HonestReporting (FKN0047); Factmata Limited, UK (FKN0035).

checking. We recommend that the Government initiate a working group of experts to create a credible annotation of standards, so that people can see, at a glance, the level of verification of a site. This would help people to decide on the level of importance that they put on those sites.

Our recommendations in this Report

19. ***During the course of this inquiry we have wrestled with complex, global issues, which cannot easily be tackled by blunt, reactive and outmoded legislative instruments. In this Report, we suggest principle-based recommendations which are sufficiently adaptive to deal with fast-moving technological developments. We look forward to hearing the Government's response to these recommendations.***

20. **We also welcome submissions to the Committee from readers of this interim Report, based on these recommendations, and on specific areas where the recommendations can incorporate work already undertaken by others. This inquiry has grown through collaboration with other countries, organisations, parliamentarians, and individuals, in this country and abroad, and we want this co-operation to continue.**

2 The definition, role and legal responsibilities of tech companies

21. At the centre of the argument about misinformation and disinformation is the role of tech companies, on whose platforms content is disseminated.[26] Throughout the chapter, we shall use the term 'tech companies' to indicate the different types of social media and internet service providers, such as Facebook, Twitter, and Google. It is important to note that a series of mergers and acquisitions mean that a handful of tech companies own the major platforms. For example, Facebook owns Instagram and WhatsApp; Alphabet owns both Google and YouTube.

22. The word 'platform' suggests that these companies act in a passive way, posting information they receive, and not themselves influencing what we see, or what we do not see. However, this is a misleading term; tech companies do control what we see, by their very business model. They want to engage us from the moment we log onto their sites and into their apps, in order to generate revenue from the adverts that we see. In this chapter, we will explore: the definitions surrounding tech companies; the companies' power in choosing and disseminating content to users; and the role of the Government and the tech companies themselves in ensuring that those companies carry out their business in a transparent, accountable way.

An unregulated sphere

23. Tristan Harris of the Center for Humane Technology[27] provided a persuasive narrative of the development and role of social media platforms, telling us that engagement of the user is an integral part both of tech companies' business model and of their growth strategy:

> They set the dial; they don't want to admit that they set the dial, and instead they keep claiming, "We're a neutral platform," or, "We're a neutral tool," but in fact every choice they make is a choice architecture. They are designing how compelling the thing that shows up next on the news feed is, and their admission that they can already change the news feeds so that people spend less time [on it] shows that they do have control of that.[28]

24. Mr Harris told us that, while we think that we are in control of what we look at when we check our phones (on average, around 150 times a day), our mind is being hijacked, as if we were playing a slot machine:

> Every time you scroll, you might as well be playing a slot machine, because you are not sure what is going to come up next on the page. A slot machine is a very simple, powerful technique that causes people to want to check in all the time. Facebook and Twitter, by being social products—by using your

26 As of February 2018, 79% of the UK population had Facebook accounts, 79% used YouTube, and 47% used Twitter, https://weareflint.co.uk/press-release-social-media-demographics-2018

27 The Center for Humane Technology website, accessed 27 June 2018

28 Tristan Harris, Q3149

> social network—have an infinite supply of new information that they could show you. There are literally thousands of things that they could populate that news feed with, which turns it into that random-reward slot machine.[29]

25. Coupled with this is the relentless feed of information that we receive on our phones, which is driven by tech engineers "who know a lot more about how your mind works than you do. They play all these different tricks every single day and update those tricks to keep people hooked".[30]

Regulatory architecture

The Information Commissioner's Office

26. The Information Commissioner is a non-departmental public body, with statutory responsibility "for regulating the processing of personal data" in the United Kingdom,[31] including the enforcement of the new Data Protection Act 2018 and the General Data Protection Regulation (GDPR).[32] The ICO's written evidence describes the Commission's role as "one of the sheriffs of the internet".[33]

27. The Commissioner, Elizabeth Denham, highlighted the "behind the scenes algorithms, analysis, data matching and profiling" which mean that people's data is being used in new ways to target them with information.[34] She sees her role as showing the public how personal data is collected, used and shared through advertising and through the micro-targeting of messages delivered through social media."[35] She has a range of powers to ensure that personal data is processed within the legislative framework, including the serving of an information notice, requiring specified information to be provided within a defined timeframe.

28. The 2018 Act extends the Commissioner's powers to conduct a full audit where she suspects that data protection legislation has, or is being, contravened and to order a company to stop processing data. Elizabeth Denham told us that these would be "powerful" measures.[36] The recent legislative changes also increased the maximum fine that the Commissioner can levy, from £500,000 to £17 million or 4% of global turnover, whichever is greater, and set out her responsibilities for international co-operation on the enforcement of data protection legislation.[37]

29. The Data Protection Act 2018 created a new definition, called "Applied GDPR", to describe an amended version of the GDPR, when European Union law does not apply (when the UK leaves the EU). Data controllers would still need to assess whether they are subject to EU law, in order to decide whether to follow the GDPR or the Applied GDPR.

29 Q3147
30 Tristan Harris, Q3147
31 Elizabeth Denham, Information Commissioner (FKN0051)
32 The General Data Protection Regulation (GDPR) came into force on 25 May 2018 and is a regulation under EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018).
33 Elizabeth Denham, Information Commissioner (FKN0051)
34 Elizabeth Denham, Information Commissioner (FKN0051)
35 Elizabeth Denham, Information Commissioner (FKN0051)
36 Q907
37 Guide to the GDPR, ICO website, accessed 21 July 2018

Apart from the exceptions laid down in the GDPR, all personal data processed in the United Kingdom comes within the scope of European Union law, until EU law no longer applies to the United Kingdom. However, when the United Kingdom leaves the EU, social media companies could "process personal data of people in the UK from bases in the US without any coverage of data protection law. Organisations that emulate Cambridge Analytica could set up in offshore locations and profile individuals in the UK without being subject to any rules on processing personal data", according to Robert Madge, CEO of the Swiss data management company Xifrat Daten.[38]

30. ***The Data Protection Act 2018 gives greater protection to people's data than did its predecessor, the 1998 Data Protection Act, and follows the law set out in the GDPR. However, when the UK leaves the EU, social media companies will be able to process personal data of people in the UK from bases in the US, without any coverage of data protection law. We urge the Government to clarify this loophole in a White Paper this autumn.***

Investigation into the use of data analytics for political purposes

31. In May 2017, the ICO announced a formal investigation into the use of data analytics for political purposes. The investigation has two strands: explaining how personal data is used in the context of political messaging; and taking enforcement action against any found breaches of data protection legislation.[39] The investigation has involved 30 organisations, including Facebook and Cambridge Analytica. Elizabeth Denham said of the investigation:

> For the public, we need to be able to understand why an individual sees a certain ad. Why does an individual see a message in their newsfeed that somebody else does not see? We are really the data cops here. We are doing a data audit to be able to understand and to pull back the curtain on the advertising model around political campaigning and elections.[40]

32. In response to our request for the ICO to provide an update on the investigation into data analytics in political campaigning, the Commissioner duly published this update on 11 July 2018.[41] We are grateful to the Commissioner for providing such a useful, detailed update on her investigations, and we look forward to receiving her final report in due course.

33. The ICO has been given extra responsibilities, but with those responsibilities should come extra resources. Christopher Wylie, a whistle-blower and ex-SCL employee, has had regular contact with the ICO, and he explained that the organisation has limited resources to deal with its responsibilities: "A lot of the investigators do not have a robust technical background. […] They are in charge of regulating data, which means that they should have a lot of people who understand how databases work".[42]

34. Paul-Olivier Dehaye, founder of PersonalDataIO, told us that he had sent a letter to the ICO in August 2016, asking them if they were investigating Cambridge Analytica, because

38 Brexit risk to UK personal data, Robert Madge, Medium, 22 June 2018
39 Q895
40 Q899
41 Investigation into the use of data analytics in political campaigns: investigation update, ICO, July 2018.
42 Q1460

of the information about the company that was publicly available at that time. He told us that "if the right of access was made much more efficient, because of increased staffing at the ICO, this right would be adopted by [...] educators, journalists, activists, academics, as a tool to connect civil society with the commercial world and to help document what is happening".[43] Data scientists at the ICO need to be able to cope with new technologies that are not even in existence at the moment and, therefore, the ICO needs to be as technically expert, if not more so, than the experts in private tech companies.

35. The Commissioner told us that the Government had given the ICO pay flexibility to retain and recruit more expert staff: "We need forensic investigators, we need senior counsel and lawyers, we need access to the best, and maybe outside counsel, to be able to help us with some of these really big files".[44] We are unconvinced that pay flexibility will be enough to retain and recruit technical experts.

36. ***We welcome the increased powers that the Information Commissioner has been given as a result of the Data Protection Act 2018, and the ability to be able to look behind the curtain of tech companies, and to examine the data for themselves. However, to be a sheriff in the wild west of the internet, which is how the Information Commissioner has described her office, the ICO needs to have the same if not more technical expert knowledge as those organisations under scrutiny. The ICO needs to attract and employ more technically-skilled engineers who not only can analyse current technologies, but have the capacity to predict future technologies. We acknowledge the fact that the Government has given the ICO pay flexibility to retain and recruit more expert staff, but it is uncertain whether pay flexibility will be enough to retain and attract the expertise that the ICO needs. We recommend that the White Paper explores the possibility of major investment in the ICO and the way in which that money should be raised. One possible route could be a levy on tech companies operating in the UK, to help pay for the expanded work of the ICO, in a similar vein to the way in which the banking sector pays for the upkeep of the Financial Conduct Authority.***

The Electoral Commission

37. The Electoral Commission is responsible for regulating and enforcing the rules that govern political campaign finance in the UK. Their priority is to ensure appropriate transparency and voter confidence in the system.[45] However, concerns have been expressed about the relevance of that legislation in an age of social media and online campaigning. Claire Bassett, the Electoral Commission's Chief Executive, told us that, "It is no great secret that our electoral law is old and fragmented. It has developed over the years, and we struggle with the complexity created by that, right across the work that we do."[46]

38. The use of social media in political campaigning has had major consequences for the Electoral Commission's work.[47] As a financial regulator, the Electoral Commission regulates "by looking at how campaigners and parties receive income, and how they spend that."[48] While that is primarily achieved through the spending returns submitted

43 Q1460
44 Q923
45 Electoral Commission (FNW0048)
46 Q2617
47 The Electoral Commission's remit covers the UK only and it has no power to intervene or to stop someone acting if they are outside the UK (Claire Bassett, Q2655)
48 Q2617

by registered campaigners, the Commission also conducts real-time monitoring of campaign activities, including on social media, that it can then compare the facts with what it is being told.[49] Where the Electoral Commission suspects or identifies that rules have been breached it has the power to conduct investigations, refer matters to the police, and issue sanctions, including fines.

39. At present, campaign spending is declared under broad categories such as 'advertising' and 'unsolicited material to electors', with no specific category for digital campaigning, not to mention the many subcategories covered by paid and organic campaigning, and combinations thereof. Bob Posner, the Electoral Commission's Director of Political Finance and Regulation and Legal Counsel, told us that "A more detailed category of spending would be helpful to understand what is spent on services, advertising, leaflets, posters or whatever it might be, so anyone can interrogate and question it."[50] The Electoral Commission has since recommended that legislation be amended so that spending returns clearly detail digital campaigning.[51]

40. Spending on election or referendum campaigns by foreign organisations or individuals is not allowed. We shall be exploring issues surrounding the donation to Leave. EU by Arron Banks in Chapter 4, but another example involving Cambridge Analytica was brought to our attention by Arron Banks himself. A document from Cambridge Analytica's presentation pitch to Leave.EU stated that "We will co-ordinate a programme of targeted solicitation, using digital advertising and other media as appropriate to raise funds for Leave.EU in the UK, the USA, and in other countries."[52] In response to a question asking whether he had taken legal advice on this proposal, Alexander Nix, the then CEO of Cambridge Analytica, replied, "We took a considerable amount of legal advice and, at the time, it was suggested by our counsel that we could target British nationals living abroad for donations. I believe […] that there is still some lack of clarity about whether this is true or not.[53]

41. When giving evidence, the Electoral Commission repeated a recommendation first made in 2003 that online campaign material should legally be required to carry a digital imprint, identifying the source. While the Electoral Commission's remit does not cover the content of campaign material, and it is "not in a position to monitor the truthfulness of campaign claims, online or otherwise", it holds that digital imprints "will help voters to assess the credibility of campaign messages."[54] A recent paper from Upturn, *Leveling the platform: real transparency for paid messages on Facebook*, highlighted the fact that "ads can be shared widely, and live beyond indication that their distribution was once subsidized. And they can be targeted with remarkable precision".[55] For this reason, we believe digital imprints should be clear and make it easy for users to identify what is in adverts and who the advertiser is.

49 Q2717
50 Q2668
51 Digital campaigning: increasing transparency for voters, Electoral Commission, 25 June 2018, p12
52 Arron Banks (FKN0056)
53 Q3331
54 Digital campaigning: increasing transparency for voters, Electoral Commission, 25 June 2018, p9
55 Levelling the platform: real transparency for paid messages on Facebook, Upturn, May 2018

42. The Electoral Commission published a report on 26 June 2018, calling for the law to be strengthened around digital advertising and campaigning, including:

- A change in the law to require all digital political campaign material to state who paid for it, bringing online adverts in line with physical leaflets and adverts;
- New legislation to make it clear that spending in UK elections and referenda by foreign organisations and individuals is not allowed;
- An increase in the maximum fine, currently £20,000 per offence, that the Electoral Commission can impose on organisations and individuals who break the rules;
- Tougher requirements for political campaigns to declare their spending soon after or during a campaign, rather than months later;
- A requirement for all campaigners to provide more detailed paperwork on how they spent money online.[56]

43. Claire Bassett told us that the current maximum fine that the Electoral Commission can impose on wrongdoings in political campaigning is £20,000, which she said is described as "the cost of doing business" for some individuals and organisations. Ms Bassett said that this amount was too low and should be increased, in line with other regulators that can impose more significant fines.[57] She also commented on how she would like a change to the regulated periods, particularly in reference to referenda:

> One of the challenges we have as regulator is that we are a financial regulator, and we regulate the parties and campaigners, usually during just that regulated period or the extended period that is set out. That does create challenges in a referendum setting. We think there is value in looking at those campaign regulated periods and thinking about how they work.[58]

We are aware that the Report of the Independent Commission on Referendums made similar recommendations in its report of July 2018.[59]

44. ***The globalised nature of social media creates challenges for regulators. In evidence Facebook did not accept their responsibilities to identify or prevent illegal election campaign activity from overseas jurisdictions. In the context of outside interference in elections, this position is unsustainable and Facebook, and other platforms, must begin to take responsibility for the way in which their platforms are used.***

45. ***Electoral law in this country is not fit for purpose for the digital age, and needs to be amended to reflect new technologies. We support the Electoral Commission's suggestion that all electronic campaigning should have easily accessible digital imprint requirements, including information on the publishing organisation and who is legally responsible for the spending, so that it is obvious at a glance who has sponsored that campaigning material, thereby bringing all online advertisements and messages into line with physically published leaflets, circulars and advertisements. We note that a***

56 Digital campaigning: increasing transparency for voters, Electoral Commission, 25 June 2018
57 Q2618
58 Claire Bassett, Q2617
59 Report of the Independent Commission on Referendums UCL Constitution Unit, July 2018

similar recommendation was made by the Committee on Standards in Public Life, and urge the Government to study the practicalities of giving the Electoral Commission this power in its White Paper.

46. ***As well as having digital imprints, the Government should consider the feasibility of clear, persistent banners on all paid-for political adverts and videos, indicating the source and making it easy for users to identify what is in the adverts, and who the advertiser is.***

47. ***The Electoral Commission's current maximum fine limit of £20,000 should be changed to a larger fine based on a fixed percentage of turnover, such as has been granted recently to the Information Commissioner's Office in the Data Protection Act 2018. Furthermore, the Electoral Commission should have the ability to refer matters to the Crown Prosecution Service, before their investigations have been completed.***

48. ***Electoral law needs to be updated to reflect changes in campaigning techniques, and the move from physical leaflets and billboards to online, micro-targeted political campaigning, as well as the many digital subcategories covered by paid and organic campaigning. The Government must carry out a comprehensive review of the current rules and regulations surrounding political work during elections and referenda, including: increasing the length of the regulated period; definitions of what constitutes political campaigning; absolute transparency of online political campaigning; a category introduced for digital spending on campaigns; reducing the time for spending returns to be sent to the Electoral Commission (the current time for large political organisations is six months); and increasing the fine for not complying with the electoral law.***

49. ***The Government should consider giving the Electoral Commission the power to compel organisations that it does not specifically regulate, including tech companies and individuals, to provide information relevant to their inquiries, subject to due process.***

50. ***The Electoral Commission should also establish a code for advertising through social media during election periods, giving consideration to whether such activity should be restricted during the regulated period, to political organisations or campaigns that have registered with the Commission. Both the Electoral Commission and the ICO should consider the ethics of Facebook or other relevant social media companies selling lookalike political audiences to advertisers during the regulated period, where they are using the data they hold on their customers to guess whether their political interests are similar to those profiles held in target audiences already collected by a political campaign. In particular, we would ask them to consider whether users of Facebook or other relevant social media companies should have the right to opt out from being included in such lookalike audiences.***

Platform or publisher?

51. How should tech companies be defined—as a platform, a publisher, or something in between? The definition of 'publisher' gives the impression that tech companies have the potential to limit freedom of speech, by choosing what to publish and what not to publish. Monika Bickert, Head of Global Policy Management, Facebook, told us that "our community would not want us, a private company, to be the arbiter of truth".[60] The

60 Q431

definition of 'platform' gives the impression that these companies do not create or control the content themselves, but are merely the channel through which content is made available. Yet Facebook is continually altering what we see, as is shown by its decision to prioritise content from friends and family, which then feeds into users' newsfeed algorithm.[61]

52. Frank Sesno, Director of the School of Media and Public Affairs, George Washington University, told us in Washington D.C. that "they have this very strange, powerful, hybrid identity as media companies that do not create any of the content but should and must—to their own inadequate levels—accept some responsibility for promulgating it. What they fear most is regulation—a requirement to turn over their data".[62]

53. At both our evidence session and at a separate speech in March 2018, the then Secretary of State for DCMS, Rt Hon Matt Hancock MP, noted the complexity of making any legislative changes to tech companies' liabilities, putting his weight behind "a new definition" that was "more subtle" than the binary choice between platform and publisher.[63] He told us that the Government has launched the Cairncross Review to look (within the broader context of the future of the press in the UK) at the role of the digital advertising supply chain, at how fair and transparent it is, and whether it "incentivises the proliferation of inaccurate and/or misleading news." The review is also examining the role and impact of digital search engines and social media companies including an assessment of regulation "or further collaboration between the platforms and publishers." The consultation closes in September 2018.[64]

54. In Germany, tech companies were asked to remove hate speech within 24 hours. This self-regulation did not work, so the German Government passed the Network Enforcement Act, commonly known as NetzDG, which became law in January 2018. This legislation forces tech companies to remove hate speech from their sites within 24 hours, and fines them 20 million Euros if it is not removed.[65]

55. Some say that the NetzDG regulation is a blunt instrument, which could be seen to tamper with free speech, and is specific to one country, when the extent of the content spans many countries. Monika Bickert, from Facebook, told us that "sometimes regulations can take us to a place—you have probably seen some of the commentary about the NetzDG law in Germany—where there will be broader societal concerns about content that we are removing and whether that line is in the right place".[66] The then Secretary of State was also wary of the German legislation because "when a regulator gets to the position where they are policing the publication of politicians then you are into tricky territory".[67] However, as a result of this law, one in six of Facebook's moderators now works in Germany, which is practical evidence that legislation can work.[68]

56. **Within social media, there is little or no regulation. Hugely important and influential subjects that affect us—political opinions, mental health, advertising,**

61 Monika Bickert, Q434
62 Frank Sesno, Q583
63 Matt Hancock MP on 'The Future of the Media' at the Oxford Media Convention, Monday 12 March 2018 and Q977
64 Terms of reference, Cairncross Review, DCMS, 12 March 2018.
65 Germany start enforcing hate speech law, BBC, 1 January 2018
66 Q386
67 Q973
68 Professor Lewandowsky, Q233

data privacy—are being raised, directly or indirectly, in these tech spaces. People's behaviour is being modified and changed as a result of social media companies. There is currently no sign of this stopping.

57. **Social media companies cannot hide behind the claim of being merely a 'platform', claiming that they are tech companies and have no role themselves in regulating the content of their sites. That is not the case; they continually change what is and is not seen on their sites, based on algorithms and human intervention. However, they are also significantly different from the traditional model of a 'publisher', which commissions, pays for, edits and takes responsibility for the content it disseminates.**

58. ***We recommend that a new category of tech company is formulated, which tightens tech companies' liabilities, and which is not necessarily either a 'platform' or a 'publisher'. We anticipate that the Government will put forward these proposals in its White Paper later this year and hope that sufficient time will be built in for our Committee to comment on new policies and possible legislation.***

59. ***We support the launch of the Government's Cairncross Review, which has been charged with studying the role of the digital advertising supply chain, and whether its model incentivises the proliferation of inaccurate or misleading news. We propose that this Report is taken into account as a submission to the Cairncross Review. We recommend that the possibility of the Advertising Standards Agency regulating digital advertising be considered as part of the Review. We ourselves plan to take evidence on this question this autumn, from the ASA themselves, and as part of wider discussions with DCMS and Ofcom.***

60. ***It is our recommendation that this process should establish clear legal liability for the tech companies to act against harmful and illegal content on their platforms. This should include both content that has been referred to them for takedown by their users, and other content that should have been easy for the tech companies to identify for themselves. In these cases, failure to act on behalf of the tech companies could leave them open to legal proceedings launched either by a public regulator, and/or by individuals or organisations who have suffered as a result of this content being freely disseminated on a social media platform.***

Transparency

61. What we found, time and again, during the course of our inquiry, was the failure on occasions of Facebook and other tech companies, to provide us with the information that we sought. We undertook fifteen exchanges of correspondence with Facebook, and two oral evidence sessions, in an attempt to elicit some of the information that they held, including information regarding users' data, foreign interference and details of the so-called 'dark ads' that had reached Facebook users.[69] Facebook consistently responded to questions by giving the minimal amount of information possible, and routinely failed to offer information relevant to the inquiry, unless it had been expressly asked for. It provided witnesses who have been unwilling or unable to give full answers to the

69 Oral evidence session, 8 February 2018; oral evidence session, 26 April 2018; exchanges of correspondence between the Chair of the DCMS Committee and Facebook representatives, between 24 October and 8 June 2018, can be found on the DCMS Committee's inquiry page.

Committee's questions. This is the reason why the Committee has continued to press for Mark Zuckerberg to appear as a witness as, by his own admission, he is the person who decides what happens at Facebook.

62. We ask, once more, for Mr Zuckerberg to come to the Committee to answer the many outstanding questions to which Facebook has not responded adequately to date. Edward Lucas, a writer and security policy expert, rightly told us that Facebook should not be in a position of marking its own homework: "They have a duty as a platform to have transparent rules that can be discussed with the outside world and we should be able to check stuff. […] We cannot just trust Facebook to go after the event and say, 'Nothing to see here, move along'. We should be able to see in real time who is advertising".[70]

63. As the then Secretary of State, Rt Hon Matthew Hancock MP, pointed out when he gave evidence to us, the Defamation Act 2013 contains provisions stating that, if a user is defamed on social media, and the offending individual cannot be identified, the liability rests with the platform.[71]

64. **Tech companies are not passive platforms on which users input content; they reward what is most engaging, because engagement is part of their business model and their growth strategy. They have profited greatly by using this model. This manipulation of the sites by tech companies must be made more transparent. Facebook has all of the information. Those outside of the company have none of it, unless Facebook chooses to release it. Facebook was reluctant to share information with the Committee, which does not bode well for future transparency. *We ask, once more, for Mr Zuckerberg to come to the Committee to answer the many outstanding questions to which Facebook has not responded adequately, to date.***

65. ***Facebook and other social media companies should not be in a position of 'marking their own homework'. As part of its White Paper this Autumn, the Government need to carry out proactive work to find practical solutions to issues surrounding transparency that will work for both users, the Government, and the tech companies.***

66. ***Facebook and other social media companies have a duty to publish and to follow transparent rules. The Defamation Act 2013 contains provisions stating that, if a user is defamed on social media, and the offending individual cannot be identified, the liability rests with the platform. We urge the Government to examine the effectiveness of these provisions, and to monitor tech companies to ensure they are complying with court orders in the UK and to provide details of the source of disputed content—including advertisements—to ensure that they are operating in accordance with the law, or any future industry Codes of Ethics or Conduct. Tech companies also have a responsibility to ensure full disclosure of the source of any political advertising they carry.***

Bots

67. Bots are algorithmically-driven computer programmes designed to carry out specific tasks online, such as analysing and scraping data. Some are created for political purposes, such as automatically posting content, increasing follower numbers, supporting political campaigns, or for spreading misinformation and disinformation. Samantha Bradshaw,

70 Q855
71 Section 5, 'Operators', Defamation Act 2013

from the Oxford Internet Institute, University of Oxford, described the different types of bots, with some being completely automated and some with real people who engage with the automated bots, described as 'cyborgs': "Those accounts are a lot harder to detect for researchers, because they feel a lot more genuine. Instead of just automating a bunch of tweets, so that something retweets different accounts 100 times a day, bots might actually post comments and talk with other users—real people—on the accounts".[72]

68. When she gave evidence in February 2018, Monika Bickert, Head of Global Policy Management at Facebook, would not confirm whether there were around 50,000 bot accounts during the US presidential election of 2016.[73] However, when Mike Schroepfer, CTO of Facebook, gave evidence in April 2018, after the Cambridge Analytica events had unfolded, he was more forthcoming about the problem of bots:

> The key thing here is people trying to create inauthentic identities on Facebook, claiming they are someone other than who they are. To give you a sense of the scale of that problem and the means, while we are in this testimony today it is likely we will be blocking hundreds of thousands of attempts by people around the world to create fake accounts through automated systems. This is literally a day-to-day fight to make sure that people who are trying to abuse the platform are kept off it and to make sure that people use Facebook for what we want it for, which is to share it with our friends.[74]

69. Mike Schroepfer also said that removal of such bots can be difficult, and was evasive about how many fake accounts had been removed, telling us: "We are purging fake accounts all the time and dealing with fraudulent ads and we do not tend to report each specific instance. I know we report aggregate statistics on a regular basis, but it is not something we are reporting here or there, so I don't know.[75] The problem with removing such bots without a systematic appraisal of their composition means that valuable information is then lost. Such information would prove invaluable to researchers involved in making connections, in order to prevent future attacks by malign players.

Algorithms

70. Both social media companies and search engines use algorithms, or sequences of instructions, to personalise news and other content for users. The algorithms select content based on factors such as a user's past online activity, social connections, and their location. Samantha Bradshaw, from the Oxford Internet Institute, told us about the power of Facebook to manipulate people's emotions by showing different types of stories to them: "If you showed them more negative stories, they would feel more negatively. If you showed them positive stories, they would feel more positive".[76] The tech companies' business models rely on revenue coming from the sale of adverts and, because the bottom line is profit, negative emotions (which appear more quickly than positive emotions) will always be prioritised. This makes it possible for negative stories to spread.

72 Q18
73 Q465
74 Q2126
75 Q2293
76 Q29

71. Information about algorithms that dictate what users see on their News Feed is not publicly available. But just as information about the tech companies themselves needs to be more transparent, so does information about the algorithms themselves. These can carry inherent biases, such as those involving gender and race, as a result of algorithms development by engineers; these biases are then replicated, spread, and reinforced. Monika Bickert, from Facebook, admitted that Facebook was concerned about "any type of bias, whether gender bias, racial bias or other forms of bias that could affect the way that work is done at our company. That includes working on algorithms". She went on to describe ways in which they were attempting to address this problem, including "initiatives ongoing, right now, to try to develop talent in under-represented communities".[77] In our opinion, Facebook should be taking a more active and urgent role in tackling such inherent biases in algorithm development by engineers, to prevent these biases being replicated and reinforced. Claire Wardle, Executive Director of First Draft News, told us of the importance to get behind the 'black box' of the working of algorithms, in order to understand the rules and motivations of the tech companies:

> What are the questions to ask a platform about why it was created? What are the metrics for that particular algorithm? How can we have more insight into that algorithm? How can we think about frameworks of algorithms? Irrespective of the platform, how can we set up that framework so that platforms have to be not just transparent but transparent across particular aspects and elements?[78]

72. ***Just as the finances of companies are audited and scrutinised, the same type of auditing and scrutinising should be carried out on the non-financial aspects of technology companies, including their security mechanisms and algorithms, to ensure they are operating responsibly. The Government should provide the appropriate body with the power to audit these companies, including algorithmic auditing, and we reiterate the point that the ICO's powers should be substantially strengthened in these respects.***

73. ***If companies like Facebook and Twitter fail to act against fake accounts, and properly account for the estimated total of fake accounts on their sites at any one time, this could not only damage the user experience, but potentially defraud advertisers who could be buying target audiences on the basis that the user profiles are connected to real people. We ask the Competition and Markets Authority to consider conducting an audit of the operation of the advertising market on social media.***

Privacy settings and 'terms and conditions'

74. Facebook and other tech companies make it hard for users to protect their own data. A report by the Norwegian Consumer Council, 'Deceived by Design', published in June 2018, highlighted the fact that Facebook, Google and Microsoft direct users away from privacy-friendly options on their services in an "unethical" way, while giving users "an illusion of control".[79] Users' privacy rights are usually hidden in tech companies' 'terms

77 Q441
78 Q582
79 Deceived by design, Norwegian Consumer Council, 26 June 2018.

and conditions' policies, which themselves are complicated, and do not follow their own terms of conditions in ensuring that they are age appropriate and that age ratification takes place.[80]

75. ***Social media companies have a legal duty to inform users of their privacy rights. Companies give users the illusion of users having freedom over how they control their data, but they make it extremely difficult, in practice, for users to protect their data. Complicated and lengthy terms and conditions, small buttons to protect our data and large buttons to share our data mean that, although in principle we have the ability to practise our rights over our data—through for example the GDPR and the Data Protection Act—in practice it is made hard for us.***

76. ***The UK Government should consider establishing a digital Atlantic Charter as a new mechanism to reassure users that their digital rights are guaranteed. This innovation would demonstrate the UK's commitment to protecting and supporting users, and establish a formal basis for collaboration with the US on this issue. The Charter would be voluntary, but would be underpinned by a framework setting out clearly the respective legal obligations in signatory countries. This would help ensure alignment, if not in law, then in what users can expect in terms of liability and protections.***

'Free Basics' and Burma

77. One of Facebook's unofficial company mottoes was to "move quickly and break things"; to take risks, to not consider the consequences. Sandy Parakilas, an ex-Facebook employee, told us that most of the goals of the company were centred around growth, in terms of the number of people using the service and the subsequent revenue.[81] But with growth comes unintended consequences, if that growth happens unchecked. This unchecked growth of Facebook is continuing. 'Free Basics' is a Facebook service that provides people in developing countries with mobile phone access to various services without data charges. This content includes news, employment, health, information and local information. Free Basics is available in 63 countries around the world.[82]

78. Out of a 50 million population in Burma, there are 30 million monthly active users on Facebook.[83] While Free Basics gives internet access for the majority of people in Burma, at the same time it severely limits the information available to users, making Facebook virtually the only source of information online for the majority of people in Burma.[84] The United Nations accused Facebook of playing a determining role in stirring up hatred against the Rohingya Muslim minority in Rakhine State. In March 2018, the UN Myanmar investigator Yanghee Lee said that the platform had morphed into a 'beast' that helped to spread vitriol against Rohingya Muslins.[85]

79. When Mike Schroepfer, the CTO at Facebook, gave evidence in April 2018, he described the situation in Burma as "awful", and that "we need to and are trying to do a lot more to get hate speech and all this kind of vile content off the platform",[86] but he could

80 The then Secretary of State, Rt Hon Matt Hancock MP Q968
81 Q1208
82 internet.org by Facebook, accessed 21 July 2018.
83 Myanmar group blasts Zuckerberg claim on Facebook hate speech prevention, Techcrunch, 6 April, 2018
84 Unliked: How Facebook is playing a part in the Rohingya genocide, The Conversation, 2 January 2018.
85 UN: Facebook has turned into a beast in Myanmar, BBC, 13 March 2018.
86 Q2490

not tell us when Facebook had started work on limiting hate speech, he could not tell us how many fake accounts had been identified and removed from Burma, and he could not tell us how much revenue Facebook was making from Facebook users in Burma.[87]

80. Mr. Schroepfer promised to submit supplementary evidence to give us that information. However, Facebook's supplementary evidence stated: "We do not break down the removal of fake accounts by country. […] Myanmar [Burma] is a small market for Facebook. We do not publish country advertising revenue figures".[88] We sent yet another letter, asking why Facebook does not break down the removal of fake accounts by country, which seems a serious lapse in demonstrating how it takes responsibility when problems with fake accounts arise.[89] To date, we have not received an answer.

81. UK aid to Burma is planned at £100 million for 2018.[90] The Department for International Development told the International Development Committee that "for our programme to be successful, Burma must work towards the implementation of inclusive peace agreements, a new political settlement; and the military serving, rather than ruling, Burma".[91] To date, the UK's total support for the crisis since August 2017 is £129 million.

82. **The United Nations has named Facebook as being responsible for inciting hatred against the Rohingya Muslim minority in Burma, through its 'Free Basics' service. It provides people free mobile phone access without data charges, but is also responsible for the spread disinformation and propaganda. The CTO of Facebook, Mike Schroepfer described the situation in Burma as "awful", yet Facebook cannot show us that it has done anything to stop the spread of disinformation against the Rohingya minority.**

83. ***The hate speech against the Rohingya—built up on Facebook, much of which is disseminated through fake accounts—and subsequent ethnic cleansing, has potentially resulted in the success of DFID's aid programmes being greatly reduced, based on the qualifications they set for success. The activity of Facebook undermines international aid to Burma, including the UK Government's work. Facebook is releasing a product that is dangerous to consumers and deeply unethical. We urge the Government to demonstrate how seriously it takes Facebook's apparent collusion in spreading disinformation in Burma, at the earliest opportunity. This is a further example of Facebook failing to take responsibility for the misuse of its platform.***

Code of Ethics and developments

84. Facebook has hampered our efforts to get information about their company throughout this inquiry. It is as if it thinks that the problem will go away if it does not share information about the problem, and reacts only when it is pressed. Time and again we heard from Facebook about mistakes being made and then (sometimes) rectified, rather than designing the product ethically from the beginning of the process. Facebook has a 'Code of Conduct', which highlights the principles by which Facebook staff carry

87 Qq 2493 to 2496
88 Facebook letter from Rebecca Stimson, Head of Public Policy, to Damian Collins, 14 May 2018.
89 Letter from Damian Collins to Rebecca Stimson, 21 May 2018
90 Bangladesh, Burma and the Rohingya crisis, International Development Committee, fourth report of session 2017–19, HC 1054, para 11
91 Ibid.

out their work, and states that employees are expected to "act lawfully, honestly, ethically, and in the best interests of the company while performing duties on behalf of Facebook".[92] Facebook has fallen well below this standard in Burma.

85. The then Secretary of State, Rt Hon Matt Hancock MP, talked about the need for tech companies to move from a libertarian attitude—"the foundation of the internet"—to one of "liberal values on the internet, which is supporting and cherishing the freedom but not the freedom to harm others".[93] He warned that tech company leaders have a responsibility, otherwise responsibility will be imposed on them: "I do not, for a moment, buy this idea that just because the internet is global therefore nation states do not have a say in it. We are responsible. We collectively, Parliament is responsible, for the statutory rules where our society lives".[94]

Monopolies and the business models of tech companies

86. The dominance of a handful of powerful tech companies, such as Facebook, Twitter and Google, has resulted in their behaving as if they were monopolies in their specific area. Traditionally, the basis of competition policy with regard to monopolies has been the issue of consumer detriment, such as the risk of overcharging. However, in the tech world, consumer detriment is harder to quantify. In the digital sphere, many of these services have marginal running costs, are free to the consumer at the point of use, and have the potential of benefiting the consumer from being monopolistic—the sharing of information is the point of these companies and improves the accuracy of services such as Google Maps. As the Secretary of State told us, "The whole question of the concept of how we run competition policy in an era where many goods and many other new innovations have zero marginal costs and are free is intellectually difficult."[95]

87. With the free access of services must come the means of funding the businesses; tech companies' business models rely on the data of users for advertisers to utilise, in order to maximise their revenue. Facebook and Google have 60% of US digital ad spend and 20% of total global spend, as of February 2018.[96] Therefore, consumer protection in the modern world is not only about goods, it is about the protection of data. Tech companies' business models have extolled the fact that they are offering innovations that are free to use, but in doing so the users become the product of the companies, and this is where issues of mistrust and misuse arise. The new measures in GDPR allow users to see what data the companies hold about them, and users can request their data to be removed or transferred to other tech companies, but in order for this to be effective, users must have knowledge of and utilise these rights.[97]

88. Professor Bakir, from Bangor University, talked of how technology continually changes, with people adapting to that technology in unpredictable ways.[98] She suggested the establishment of a working group, to monitor what is being developed in the area of misinformation and disinformation because "what is around the corner may be much

92 Code of Conduct, Facebook, 31 May 2018
93 Q954
94 Q954
95 Q979
96 Ian Lucas MP, Q619
97 Guide to the GDPR, ICO website
98 Q233

more worrying than what we have experienced to date".[99] As technology develops so quickly, regulation needs to be based not on specifics, but on principles, and adaptive enough to withstand technological developments.

89. ***A professional global Code of Ethics should be developed by tech companies, in collaboration with this and other governments, academics, and interested parties, including the World Summit on Information Society, to set down in writing what is and what is not acceptable by users on social media, with possible liabilities for companies and for individuals working for those companies, including those technical engineers involved in creating the software for the companies. New products should be tested to ensure that products are fit-for-purpose and do not constitute dangers to the users, or to society.***

90. ***The Code of Ethics should be the backbone of tech companies' work, and should be continually referred to when developing new technologies and algorithms. If companies fail to adhere to their own Code of Ethics, the UK Government should introduce regulation to make such ethical rules compulsory.***

91. ***The dominance of a handful of powerful tech companies, such as Facebook, Twitter and Google, has resulted in their behaving as if they were monopolies in their specific area. While this portrayal of tech companies does not appreciate the benefits of a shared service, where people can communicate freely, there are considerations around the data on which those services are based, and how these companies are using the vast amount of data they hold on users. In its White Paper, the Government must set out why the issue of monopolies is different in the tech world, and the measures needed to protect users' data.***

99 Q233

3 The issue of data targeting, based around the Facebook, GSR and Cambridge Analytica allegations

92. Arguably more invasive than obviously false information is the relentless targeting of hyper-partisan views, which play to the fears and the prejudices of people, in order to alter their voting plans. This targeting formed the basis of the revelations of March 2018, which brought to the general public's attention the facts about how much of their own personal data is in the public domain, unprotected, and available for use by different players. Some of the events surrounding Cambridge Analytica and its use of Facebook data had been revealed at the end of 2015, when Harry Davies published an article in The Guardian, following investigations lasting around a year, and wrote: "a little known data company [Cambridge Analytica] […] paid researchers at Cambridge University to gather detailed psychological profiles about the US electorate using a massive pool of mainly unwitting US Facebook users built with an online survey".[100]

93. Based on our knowledge of this article, we had explored the general issues surrounding the manipulation of data when we questioned Facebook in February 2018. However, it was in March 2018 when facts about this case became better known across the world, including how people's data was used to influence election campaigning, in the US and the UK, through the work of Carole Cadwalladr, at *The Observer*, and the whistle-blower Christopher Wylie, a former employee of SCL Group, and Cambridge Analytica. Shortly after going public with his allegations, Christopher Wylie gave evidence to the Committee.[101] This chapter will focus on the events that highlighted the extent of the misuse of data, involving various organisations including Facebook, Global Science Research (GSR), Cambridge Analytica, and Aggregate IQ (AIQ), and the alleged sharing of data in the EU Referendum. We received written and oral evidence from many of those intimately involved in these revelations. Issues relating to these companies and political campaigning are further examined in Chapter 4, as well as evidence regarding SCL's involvement in overseas elections in Chapter 6.

Cambridge Analytica and micro-targeting

94. Cambridge Analytica was founded in 2012, with backing from the US hedge fund billionaire and Donald Trump donor, Robert Mercer, who became the majority shareholder.[102] He was the largest donor to the super political action committee (PAC) that supported the presidential campaigns of Ted Cruz and Donald Trump in the 2016 presidential election.[103] Christopher Wylie argued that the funding of Cambridge Analytica enabled Mr Mercer to benefit from political campaigns that he supported, without directly spending money on them, thereby bypassing electoral finance laws:

100 Paul-Olivier Dehaye, Q1342, referring to Ted Cruz using firm that harvested data on millions of unwitting Facebook users, Harry Davies, The Guardian, 11 December 2015.

101 The DCMS Committee's oral evidence session with Christopher Wylie and Paul-Olivier Dehaye, 27 March 2018, was described by Mark D'Arcy, parliamentary correspondent at the BBC, as "by a distance, the most astounding thing I've seen in Parliament". Tweet, 17 March 2018, Mark D'Arcy.

102 Christopher Wylie, Q1273

103 Contributors, 2016 cycle, OpenSecrets.org

"[Robert Mercer] can put in $15 million to create something and then only charge $50,000 for it. It would have been physically impossible to get the same value and level of service and data for that amount of money in any other way".[104]

95. Cambridge Analytica was born out of the already established SCL consultancy, which had engaged in political campaigns around the world, using specialist communications techniques previously developed by the military to combat terror organisations, and to disrupt enemy intelligence and to give on the ground support in war zones. Cambridge Analytica's primary purpose would instead be to focus on data targeting and communications campaigns for carefully selected Republican Party candidates in the United States of America.

96. Steve Bannon served as White House chief strategist at the start of President Donald Trump's term, having previously been chief executive of President Trump's general election campaign. He was the executive chairman of Breitbart News, a website he described as 'the platform of the alt-right,'[105] and was the former Vice President of Cambridge Analytica. A Cambridge Analytica invoice to UKIP was billed to the same address as Steve Bannon's company, Glittering Steel.[106] The Committee was also told that Steve Bannon introduced Cambridge Analytica to Arron Banks and to Leave.EU.[107]

97. We heard evidence from Alexander Nix, in February 2018, before the *Observer* and *Guardian* revelations in March 2018, and before the company and its associated company had gone into administration.[108] Alexander Nix described the micro-targeting business of Cambridge Analytica:

> We are trying to make sure that voters receive messages on the issues and policies that they care most about, and we are trying to make sure that they are not bombarded with irrelevant materials. That can only be good. That can only be good for politics, it can only be good for democracy and it can be good in the wider realms of communication and advertising.[109]

98. The use of data analytics, based on the psychological profile of the audience, was at the heart of the work of Cambridge Analytica, "presenting a fact that is underpinned by an emotion", as described by Mr. Nix.[110] In order to match the right type of message to voters, Cambridge Analytica needed information about voters, such as what merchandise they bought, what media they read, what cars they drove.[111] Mr. Nix told us that "we are able to match these data with first-party research, being large, quantitative research instruments, not dissimilar to a poll. We can go out and ask audiences about their preferences […] indeed we can also start to probe questions about personality and other drivers that might be relevant to understanding their behaviour and purchasing decisions".[112] Cambridge Analytica used 'OCEAN psychological analysis' to identify issues people might support and how to position the arguments to them. OCEAN categorises people based on their

104 Christopher Wylie, Qq 1410 and 1411
105 A brief history of Breitbart news, Business Insider UK, November 2016
106 Brittany Kaiser, Qq 1682–1684
107 Q1506
108 Cambridge Analytica and the SCL Group started insolvency proceedings in the US and the UK on 2 May 2018.
109 Q657
110 Q662
111 Alexander Nix, Q679
112 Q675

'Openness', 'Conscientiousness', 'Extraversion', 'Agreeableness' and 'Neuroticism'.[113] As Alexander Nix explained in his talk at the 2016 Concordia Annual Summit, entitled 'The Power of Big Data and Psychographics', this approach helps you, for example, to decide how to persuade American voters on the importance of protection of the second amendment, which guarantees the right to keep and bear arms. In the example Mr Nix showed, you might play on the fears of someone who could be frightened into believing that they needed the right to have a gun to protect their home from intruders.[114]

99. When asked where the data used by Cambridge Analytica came from, Alexander Nix told us: "We do not work with Facebook data, and we do not have Facebook data. We do use Facebook as a platform to advertise, as do all brands and most agencies, or all agencies, I should say. We use Facebook as a means to gather data. We roll out surveys on Facebook that the public can engage with if they elect to".[115] When asked whether Cambridge Analytica was able to use information on users' Facebook profile when they complete surveys, Mr. Nix replied, "No, absolutely not. Absolutely not".[116]

100. Professor David Carroll, a US citizen, made a Subject Access Request (SAR) to Cambridge Analytica in January 2017, under the Data Protection Act 1998, because he believed that his data was being processed in the UK. He told us "there was no indication of where they obtained the data. […] We should be able to know where they got the data, how they processed it, what they used it for, who they shared it with and also whether we have a right to opt out of it and have them delete the data and stop processing it in the future".[117] The ICO's investigation update of 11 July 2018 described Professor Carroll's case as "a specific example of Cambridge Analytica/SCL's poor practice with regard to data protection law".[118]

101. The ICO served an Enforcement Notice on SCL Elections Ltd on 4 May 2018, ordering it to comply with the terms of the SAR, by providing copies of all personal information that SCL held on Professor Carroll. However, the terms of the Enforcement Notice were not complied with by the deadline of 3 June 2018, and the ICO is now considering criminal action against Cambridge Analytica and SCL Elections Ltd.[119]

Global Science Research

102. The Facebook data breach in 2014, and the role of Cambridge Analytica in acquiring this data, has been the subject of intense scrutiny. Ultimately the data breach originated at the source of the data, at Facebook. 'Friends permissions' were a set of permissions on Facebook between 2010 and 2014, and allowed developers to access data related to users' friends, without the knowledge or express consent of those friends.[120] One such developer, Aleksandr Kogan, an American citizen who had been born in the former Soviet Union, was a Research Associate and University Lecturer at the University of Cambridge in the

113 Alexander Nix, Q679
114 Q783
115 Q682
116 Q704
117 Q571
118 Investigation into data analytics for political purposes: investigation update, ICO, 11 July 2018
119 Investigation into data analytics for political purposes: investigation update, ICO, 11 July 2018
120 Sandy Parakilas, Q1202

Department of Psychology. Kogan began collaborating "directly" with Facebook in 2013, and he told us that they "provided me with several macro-level datasets on friendship connections and emoticon usage."[121]

103. Professor Kogan set up his own business, Global Science Research (GSR), in the spring of 2014, and developed an App, called the GSR App, which collected data from users, at an individual level.[122] It was at around this time as well that Dr Kogan was in discussions about working on some projects with SCL Elections and Cambridge Analytica, to see whether his data collection and analysis methods could help the audience targeting of digital campaigns. Professor Kogan explained that he did not sell the GSR App itself as "it is not technically challenging in any way. Facebook explains how to do it, so there is great documentation on this".[123] What was valuable was the data. The aim was to recruit around 200,000 people who could earn money by completing an online survey. Recruits had to download the App before they could collect payment. The App would download some information about the user and their friends. Each person was paid $3 or $4, which totalled $600,000 to $800,000 across all participants. In this case SCL paid that amount, and then returned to get predictions about people's personalities, for which they paid GSR £230,000.[124] In the latter part of 2014, after the GSR App data collection was complete, Professor Kogan revised the application to become an interactive personality "quiz" and renamed the App "thisisyourdigitallife."[125]

104. The exact nature of Dr Kogan's work on this project is set out in the contract he signed with SCL, on 4 June 2014, along with his business partner, Joseph Chancellor, who was later hired to work for Facebook.[126] Alexander Nix also signed this contract on behalf of SCL Elections. In the 'Project and Specification' schedule of the contract it states that 'After data is collected, models are built using psychometric techniques (e.g. factor analysis, dimensional scaling etc) which uses Facebook likes to predict people's personality scores. These models are validity tested on users who were not part of the training sample. Trait predictions based on Facebook likes are at near test-retest levels and have been compared to the predictions that romantic partners, family members and friends make about their traits. In all previous cases the computer-generated scores performed the best. Thus, the computer-generated scores can be more accurate than even the knowledge of very close friends and family members.'[127]

105. Furthermore, Dr Kogan and SCL knew that 'scraping' Facebook user data in this way was in breach of the company's then recently revised terms of service. Instead the work was carried out under the terms of an agreement GSR has with Facebook which predated this change. It is stated in the contract that, "GSR's method relies on a pre-existing application functioning under Facebook's old terms of service. New applications are not able to access friend networks and no other psychometric profiling applications exist under the old Facebook terms."[128]

121 Q1770
122 Aleksandr Kogan, Q1796
123 Q1809
124 Q1809
125 Aleksandr Kogan (FKN0077)
126 Background papers submitted by Christopher Wylie, p67
127 Background papers submitted by Christopher Wylie, p84
128 Background paper submitted by Christopher Wylie, p.84

106. The purpose of the project, however, was not to carry out this testing as part of an experiment into the predictive nature of understanding the insights about an individual that are provided by Facebook likes. Rather, data would be scraped to order to support political campaigns. Cambridge Analytica was involved with in eleven states in the USA in 2014. These were Arkansas, Colorado, Florida, Iowa, Louisiana, Nevada, New Hampshire, North Carolina, Oregon, South Carolina and West Virginia.[129] Dr Kogan and his team were required under the contract to provide SCL with data sets that matched predictive personality scores, including someone's likely political interests, to named individuals on the electoral register in those states.

107. When Dr Kogan gave evidence to us, he stated that he believed using Facebook likes to predict someone's personality and interests was not particularly accurate. However, from the contract he signed with SCL in June 2014, he certainly thought it was at the time. Furthermore, Dr Kogan's colleague at the Cambridge Psychometrics Centre, Michal Kosinski, co-authored an academic paper called 'Tracking the Digital Footprints of Personality', published in December 2014, where he re-states the case or the effectiveness of assessing personality from Facebook likes.[130] This article claims that "Facebook likes are highly predictive of personality and number[s] of other psychodemographic traits, such as age, gender, intelligence, political and religious views, and sexual orientation". The article goes on, rightly, to raise the ethical concerns that should exist in relation to this approach, stating that:

> The results presented here may have considerable negative implications because it can easily be applied to large numbers of people without obtaining their individual consent and without them noticing. Commercial companies, governmental institutions, or even one's Facebook friends could use software to infer personality (and other attributes, such as intelligence or sexual orientation) that an individual may not have intended to share. There is a risk that the growing awareness of such digital exposure may decrease their trust in digital technologies, or even completely deter them from them.[131]

108. When Alexander Nix first gave evidence to us in February 2018, he denied that Dr Kogan and GSR had supplied Cambridge Analytica with any data or information, and that his datasets were not based on information received from GSR.[132] We received evidence from both Dr Kogan and Mr Wylie that conflicted with Mr Nix's evidence; indeed, Mr Wylie described the data obtained from Dr Kogan's GSR App as the foundation dataset of the company, which collected data on up to 87 million users, over 1 million of whom were based in the UK.[133] We believe that Dr Kogan also knew perfectly well what he was doing, and that he was in breach of Facebook's own codes of conduct (which he told us he did not consider to be operative in practice, as they were never enforced).

109. During his second appearance, Mr Nix admitted that "I accept that some of my answers could have been clearer, but I assure you that I did not intend to mislead you". He went on to explain that Cambridge Analytica had *not at that time* been in possession of

129 Background paper submitted by Christopher Wylie, pp.84–85
130 Tracking the digital footprints of personality, Michal Kosinski, proceedings of the IEEE,Vol 102, no 12, December 2014
131 Ibid.
132 Qq 730 to 731
133 Q1281

data from GSR, due to the fact that they had "deleted all such data licensed in good faith from GSR under that research contract".[134] This suggests that Mr. Nix, who by his own admission to the Committee tells lies, was not telling the whole truth when he gave us his previous version of events, in February 2018.

110. In August 2014 Dr Kogan worked with SCL to provide data on individual voters to support US candidates being promoted by the John Bolton Super Pac in the mid-term elections in November of that year. Psychographic profiling was used to micro-target adverts at voters across five distinct personality groups. After the campaign, according to an SCL presentation document seen by the Committee, the company claimed that there was a 39% increase in awareness of the issues featured in the campaign's advertising amongst those who had received targeted messages.[135] In September 2014, SCL also signed a contract to work with the American Conservative advocacy organisation, 'For America'. Again, they used behavioural micro-targeting to support their campaign messages ahead of the mid-term elections that year. SCL would later claim that the 1.5million advertising impressions they generated through their campaign led to a 30% uplift in voter turnout, against the predicted turnout, for the targeted groups.

Facebook

111. Sandy Parakilas worked for Facebook for 16 months in 2011 and 2012, and told us that "once the data passed from Facebook servers to the developer, Facebook lost insight into what was being done with the data and lost control over the data".[136] There was no proper audit trail of where the data went and during Mr Parakilas' 16 months of working there, he did not remember one audit of a developer's storage.[137] This is a fundamental flaw in Facebook's model of holding data; Facebook cannot assure its users that its data is not being used by third parties and of the reasons for which that data may be being used.

112. Once the data had left Facebook, that data, or its derivatives, could be copied multiple times. Chris Vickery, Director of Cyber Risk Research at UpGuard, described to us the 'sticky' nature of data: "In this type of industry, data does not just go away. It does not just disappear. It is sticky. It gathers up. The good stuff stays. Even the bad stuff stays, but it is not used. It is held in an archive somewhere. Nothing disappears".[138]

113. Furthermore, that data was specific and personal to each person with a Facebook account, including their names, their email addresses, and could even include private messages.[139] Tristan Harris, from the Center for Humane Technology, told us that the entire premise of Facebook's App platform was exactly this—to enable third-party developers to have access to people's friends' data: "The premise of the app platform was to enable as many developers as possible to use that data in creative ways, to build creative new social applications on behalf of Facebook".[140]

114. Facebook claimed that Dr Kogan had violated his agreement to use the data solely for academic purposes. On Friday 16 March 2018, Facebook suspended Kogan from the

134 Q3288
135 Background papers submitted by Christopher Wylie
136 Q1188
137 Q1188
138 Q2534
139 Sandy Parakilas, Q1206
140 Q3168

platform, issued a statement saying that he "lied" to the company, and characterised his activities as "a scam—and a fraud".[141] Facebook also suspended Christopher Wylie at the same time. On Wednesday 21 March 2018, Mark Zuckerberg called Dr Kogan's actions a "breach of trust".[142] However, when Facebook gave evidence to us in February 2018, they failed to disclose the existence of this "breach of trust" and its implications.

115. In its commitment to update our Committee on its ongoing investigation, the ICO decided to publish a Notice of Intent to issue a monetary penalty to Facebook of £500,000, "for lack of transparency and security issues relating to the harvesting of data constituting breaches of the first and seventh data protection principles", under the Data Protection Act 1998.[143] It should be noted that, if the new Data Protection Act 2018 had been in place when the ICO started its investigation into Facebook, the ICO's Notice of Intent to impose 4% of its annual turnover of $7.87 billion, which would have totalled £315 million.

116. As recently as 20 July 2018, Facebook suspended another company that it believes harvested data from its site. Crimson Hexagon is based in Boston, US. Facebook is investigating whether this analytics firm's contracts with the US government and a Russian not-for-profit organisation with ties to the Kremlin violated Facebook's policies. For Crimson Hexagon to share such data with government agencies would be incredibly useful to those agencies, as it would show how large groups of people were feeling at a particular time, and could be used during political campaigns.[6] Again, the same opportunities given by Facebook to, unwittingly, share their users' data with Cambridge Analytica, via GSR, were being given, up until a few days ago, to Crimson Hexagon, despite Facebook's reassurances that they were tightening their policies.

Aggregate IQ (AIQ)

117. Jeff Silvester is one of the owners of the Canadian digital advertising web and software development company, Aggregate IQ (AIQ), which was incorporated in 2013. Mr Silvester gave evidence to us in May 2018 and explained that their first work for SCL was to "create a political customer relationship management software tool" for the Trinidad and Tobago election campaigning, in 2014.[144] From that work, AIQ then started developing the Ripon tool, software that was commissioned and would be owned by SCL:[145]

> The Ripon tool has been described in a lot of different ways. The part that we have done was a political customer relationship management tool focused on the US market. This was software that would help with people going door to door. There was a tool in there that you could do phone banking so you could call people and get their opinions on things and keep track of all that sort of information.[146]

118. Christopher Wylie gave us a different version of Ripon: "A lot of the papers that eventually became the foundation of the methods that were used on the Ripon project came out of research that was being done at the University of Cambridge, some of which

141 Suspending Cambridge Analytica and SCL Group from Facebook, Facebook statement, 16 March 2018; Facebook gave data about 57 billion friendships to academic, The Guardian, 22 March 2018
142 Zuckerberg on data debacle: 'It was a breach of trust', CNN interview with Mark Zuckerberg, 22 March 2018
143 Investigation into data analytics for political purposes: investigation update, ICO, July 2018
144 Q2770 and 2771
145 Q2779
146 Q2776

was funded in part by DARPA, which is the US military's research agency".[147] Mr Wylie went on to explain that Ripon was the software that utilised the algorithms from the Facebook data.[148]

119. In its interim report published in July 2018, the ICO confirmed that AIQ had access to the personal data of UK voters, given by the Vote Leave campaign. The ICO is in the process of establishing from where AIQ accessed the personal data, and whether AIQ still holds that data. Furthermore, "we have however established, following a separate report, that [AIQ] hold UK data which they should not continue to hold".[149] In this regard, the ICO is working with the federal Office of the Privacy Commissioner and the Office of the Information and Privacy Commissioner, British Columbia.[150]

120. In the files presented to the committee by Chris Vickery, we have also found evidence that AIQ used tools that could scrape user profile data from LinkedIn. The App acts similarly to online human behaviour, searching LinkedIn user profiles, scraping their contacts, and all accompanying information such as users' place of work, location and job title.[151]

121. There have been data privacy concerns raised about another campaign tool used, but not developed, by AIQ. A company called uCampaign has a mobile App that employs gamification strategy to political campaigns. Users can win points for campaign activity, like sending text messages and emails to their contacts and friends.[152] The App was used in Donald Trump's presidential campaign, and by Vote Leave during the Brexit Referendum.

122. The developer of the uCampaign app, Vladyslav Seryakov, is an Eastern Ukrainian military veteran who trained in computer programming at two elite Soviet universities in the late 1980s. The main investor in uCampaign is the American hedge fund magnate Sean Fieler, who is a close associate of the billionaire backer of SCL and Cambridge Analytica, Robert Mercer. An article published by Business Insider on 7 November 2016 states:

> If users download the App and agree to share their address books, including phone numbers and emails, the App then shoots the data [to] a third-party vendor, which looks for matches to existing voter file information that could give clues as to what may motivate that specific voter. Thomas Peters, whose company uCampaign created Trump's app, said the App is "going absolutely granular", and will—with permission—send different A/B tested messages to users' contacts based on existing information.[153]

The links between Cambridge Analytica, SCL and AIQ

123. AIQ's first substantial work was for SCL, before it went on later to work for Vote Leave in the UK's EU Referendum in 2016. According to evidence we have received, Alexander Nix and SCL also pitched for work in the Referendum to Leave.EU, but were

147 Q1281
148 Q1299
149 Investigation into data analytics for political purposes: investigation update, ICO, July 2018, p4
150 Investigation into data analytics for political purposes: investigation update, ICO, July 2018
151 Evidence to be published in the autumn of 2018, when the next disinformation Report is published.
152 uCampaign website
153 'Donald Trump's campaign is using the same app the 'Leave' campaign used during Brexit to spur voter turnout', Business Insider, 7 November 2016

not successful.[154] Throughout our inquiry, we have been concerned about the links within this seemingly small community involved in political micro-targeting and about the potential for data misuse. These concerns have been heightened by Mr Nix and SCL's own links with organisations involved in the military, defence, intelligence and security realms.

124. Much effort has been expended in trying to untangle the complex web of relationships within what started out as the SCL (Strategic Communications Laboratories) group of companies, in which the founder Nigel Oakes and Alexander Nix have been involved, along with a myriad of changing shareholders. Confusion can perhaps be sourced to the use of the SCL name within both sets of businesses: the defence consultancy (SCL Group Limited), run by Mr Oakes, and the political consultancy (SCL Elections Limited), incorporated by Mr Nix in 2012. In evidence, however, Mr Nix certainly did not help, as he was evasive about the changes in beneficial ownership during the period when Cambridge Analytica operated.[155]

125. In February 2018, in response to a question about the distinction between SCL and Cambridge Analytica, Alexander Nix told us that "SCL is a very different company to Cambridge Analytica. It is a different company that has different employees who sit in a different office. It has a different board and a different board of advisers. It has different datasets, and it has different clients."[156]

126. Christopher Wylie told us, in March 2018, that everyone who worked for Cambridge Analytica was "effectively" employed by SCL: "When I started in June 2013, Cambridge Analytica did not exist yet. It is important for people to understand that Cambridge Analytica is more of a concept or a brand than anything else because it does not have employees. It is all SCL, it is just the front-facing company for the United States".[157] No distinction was made by Mr Nix between SCL Elections Ltd and SCL Group Limited (to which he was apparently referring). In June, 2018, Mr Nix gave us graphics showing the changes to the group's employment structure between 2005–2018, but these were not a map of the ownership changes.[158]

127. Corporate filings, however, show that after a period of independence under Mr Nix from 2012, in November 2015, SCL Elections formally rejoined the orbit of the wider SCL group. Nothwithstanding this, the Committee has seen internal documents from 27 May, 2015 which show political and election projects being discussed under the banner of 'SCL Group'.[159] (We refer to one of these projects, relating to Argentina, in Chapter 6). By the time the whole group went into administration in April 2018, the US employing body, SCL USA Inc, was providing staff both to Cambridge Analytica LLC and the defence consultancy SCL Group.[160]

128. Throughout, Cambridge Analytica was also only 19% owned within the group, with the other shareholders unclear, despite our questioning over two evidence sessions with

154 Q624
155 Qn687 to 691
156 Q687
157 Q1272
158 SCL & Cambridge Aanlytica Corporate Structure Development, Alexander Nix evidence, 7 June 2018
159 Qn3398 and 3399
160 SCL Analytics Ltd, Companies House, accessed 24 July 2018

Mr Nix. Wendy Siegelman and Ann Marlow created a chart in May 2017, including 30 companies, with shareholders, interlinked within the SCL Group Ltd.[161] That structure was again soon to change, however.

129. Brittany Kaiser told us, in April 2018, that when she joined the SCL Group, "it was a parent company of a few different divisions. One would be SCL Commercial, SCL Election, SCL Defence, SCL Social, and then Cambridge Analytica, which I understood was the US-acting subsidiary." She further explained that, once Cambridge Analytica had become a popular brand, it "subsumed most of those companies and divisions and the SCL Group became just our defence company, SLC Group or SCL.gov, based in Arlington".[162]

130. In August 2017, a new ultimate holding company, Emerdata Limited, was incorporated at the same address, in Canary Wharf in London, as SCL Group.[163] Alexander Nix was appointed a director of Emerdata Ltd in January 2018. Its other directors included the former SCL Group Chairman, Julian Wheatland (who also became the new acting CEO of Cambridge Analytica on 11 April, 2018) and the former Chief Data Officer of Cambridge Analytica, Alexander Tayler (who took over as acting CEO of Cambridge Analytica on 20 March, 2018, when Mr Nix was suspended, before resigning on 11 April 2018).

131. On 18 March 2018 (the day after *The Guardian* first published articles relating to Cambridge Analytica), Rebekah and Jennifer Mercer, daughters of Robert Mercer, were also appointed directors. Another director of Emerdata is Johnson Chun Shun Ko, Deputy Chairman and Executive Director of Frontier Services Group, which is a private security firm that operates mostly in Africa. Emerdata is chaired by the US businessman Erik Prince, who founded the private military group Blackwater USA. All of Emerdata's subsidiaries went into administration in April 2018, following the Cambridge Analytica scandal, and it is uncertain what activities have continued since.

132. Companies House published the 'Notice of administrators' proposals', in respect of SCL Elections Ltd., in July 2018. It sets out the circumstances surrounding SCL Election Ltd.'s administration. Emerdata is the ultimate holding company and first called in the insolvency practitioner, Vincent Green, who then became an administrator. The notice highlights the fact that laptops from the SCL offices were not returned, and that some laptops returned by the ICO were subsequently stolen. There is also a list of SCL Election's creditors. Emerdata is listed as a creditor/claimant, with the amount of debt totalling £6,381,778.05. The administrators propose that the company go into compulsory liquidation. We are concerned about what data was remaining on the stolen laptops and why Emerdata, the parent company, is the major creditor and is owed over £6.3 million, and why SCL USA Inc, a US affiliate, is owed over £1 million.[164]

133. **Over the past month, Facebook has been investing in adverts globally, proclaiming the fact that "Fake accounts are not our friends." Yet the serious failings in the company's operations that resulted in data manipulation, resulting in misinformation and disinformation, have occurred again. Over four months after Facebook suspended Cambridge Analytica for its alleged data harvesting, Facebook suspended another**

161 SCL Group - companies and shareholders, May 2018
162 Q1559
163 Chart: Emerdata Ltd - the new Cambridge Analytica/SCL Group?, Wendy Siegelman, 26 March 2018; Emerdata Ltd, Companies House;
164 SCL Analytics, Companies House, accessed 22 July 2018

company, Crimson Hexagon—which has direct contracts with the US government and Kremlin-connected Russian organisations—for allegedly carrying out the same offence.

134. ***We are concerned about the administrators' proposals in connection with SCL Elections Ltd, as listed in Companies House, and the fact that Emerdata Ltd is listed as the ultimate parent company of SCL Elections Ltd, and is the major creditor and owed over £6.3 million. The proposals also describe laptops from the SCL Elections Ltd offices being stolen, and laptops returned by the ICO, following its investigations, also being stolen. We recommend that the National Crime Agency, if it is not already, should investigate the connections between the company SCL Elections Ltd and Emerdata Ltd.***

135. **The allegations of data harvesting revealed the extent of data misuse, made possible by Cambridge University's Dr Kogan and facilitated by Facebook, GSR, and manipulated into micro-targeting Cambridge Analytica and its associated companies, through AIQ. The SCL Group and associated companies have gone into administration, but other companies are carrying out very similar work. Many of the individuals involved in SCL and Cambridge Analytica appear to have moved on to new corporate vehicles. Cambridge Analytica is currently being investigated by the Information Commissioner's Office (ICO) (and, as a leading academic institution, Cambridge University also has questions to answer from this affair about the activities of Dr Kogan).**

136. **We invited Alexander Nix twice to give evidence; both times he was evasive in his answers and the standard of his answers fell well below those expected from a CEO of an organisation. His initial evidence concerning GSR was not the whole truth. There is a public interest in getting to the heart of what happened, and Alexander Nix must take responsibility for failing to provide the full picture of events, for whatever reason. With respect to GSR, he misled us. We will give a final verdict on Mr Nix's evidence when we complete the inquiry.**

4 Political campaigning

137. It is important to recognise the role that social media plays in encouraging political debate. However, the ability of social media companies to target content to individuals, and in private, is new. This creates new issues in relation to the regulation of elections, including the nature of content and the cost of dissemination, both of which have in the past been strictly controlled.

138. The importance of social media has been recognised by businesses and campaigners at a much faster rate than by legislators and regulators. This has resulted in candidates using social media to secure elections and win votes without the regulatory framework or laws to govern modern elections. Businesses such as SCL and Cambridge Analytica have exploited this freedom, using social media to persuade candidates that targeting voters individually can have a much bigger impact than traditional untargeted advertising.

What is a political advert?

139. Facebook told us that in June 2018 that they had no way of categorising which adverts could be classified as political:

> Our systems do not have a perfect or reliable way to classify the category that advertisements (which are developed and distributed by third-parties on our platform) fall in, whether it is political or housing or educational or otherwise. We are heavily investing in advanced technologies and machine learning to better assess advertisements that fall into specific categories (like political and issues adverts) so we can identify and enforce policies and tools that may apply [...] In addition, issue-based advertising is particularly difficult to define at a global scale as there is no universal definition of a political issue advert and this concept varies by culture and geography. We are continuing to refine our definition of this in collaboration with external stakeholders in anticipation of rolling out our transparency tools in the UK.[165]

140. The Electoral Commission's recently published report describes the nature of 'dark ads': "Only the voter, the campaigner and the platform know who has been targeted with which messages. Only the company and campaigner know why a voter was targeted and how much was spent on a particular campaign. This is why the term 'dark ads' has been used to describe micro-targeting, although it is perfectly legal".[166]

141. Some organisations such as the Institute of Practitioners in Advertising (IPA) support creating a central public register of online political adverts, rather than leaving it to the social media companies themselves. The IPA's written evidence calls for a total ban on micro-targeting political advertising online, with a minimum limit on the number of voters who are sent individual political messages, which would go some way to promote a standard line for politicians to follow.[167] While it might be difficult to advocate a total ban on micro-targeting political advertising online, a preferable alternative could be to limit the amount of 'lookalike micro-targeting', where people with similar views and opinions

165 Facebook letter from Rebecca Stimson to Damian Collins, 8 June 2018
166 Digital campaigning: increasing transparency for voters, The Electoral Commission, June 2018, Para 43
167 The Institute of Practitioners in Advertising (IPA) (FKN0093)

to core voters are also targeted.[168] Micro-targeting, when carried out in a transparent manner, can be a useful political tool. Christopher Wylie told us that it can and should be done in an ethical way "that respects the consent of people, that is transparent so that people are aware that you are sending them a political message or a commercial message, and why it is that they are being sent it".[169]

142. ***We recommend that the Government look at ways in which the UK law defines digital campaigning. This should include online adverts that use political terminology that are not sponsored by a specific political party. There should be a public register for political advertising, requiring all political advertising work to be listed for public display so that, even if work is not requiring regulation, it is accountable, clear, and transparent for all to see. There should be a ban on micro-targeted political advertising to lookalikes online, and a minimum limit for the number of voters sent individual political messages should be agreed, at a national level.***

143. ***We reiterate our support for the Cairncross Review and will engage with the consultation in the coming months. In particular, we hope that Frances Cairncross will give due weight to the role of digital advertising in elections, and will make concrete recommendations about how clearer rules can be introduced to ensure fairness and transparency.***

144. ***The Government should investigate ways in which to enforce transparency requirements on tech companies, to ensure that paid-for political advertising data on social media platforms, particularly in relation to political adverts, are publicly accessible, are clear and easily searchable, and identify the source, explaining who uploaded it, who sponsored it, and its country of origin. This information should be imprinted into the content, or included in a banner at the top of the content. Such transparency would also enable members of the public to understand the behaviour and intent of the content providers, and it would also enable interested academics and organisations to conduct analyses and to highlight trends.***

145. ***Tech companies must also address the issue of shell corporations and other professional attempts to hide identity in advert purchasing, especially around election advertising. There should be full disclosure of targeting used as part of advert transparency. The Government should explore ways of regulating on the use of external targeting on social media platforms, such as Facebook's Custom Audiences. We expect to see the detail of how this will be achieved in its White Paper later this year.***

Electoral questions concerning the EU Referendum

Co-ordinated campaigns

146. Currently, the cost of campaigns is regulated strictly with defined legal limits. In the EU Referendum, campaigns were permitted to work together on joint campaigns for a particular outcome. However, the nature of the joint work determined how it applied to spending limits: any spending on a joint campaign counted towards the limits for each campaigner involved; and where spending was on a joint campaign with a designated

168 Facebook website, for a description of lookalike audiences, accessed 12 July 2018
169 Q1413

lead campaigner, all spending counted towards the spending limit of the designated lead campaigner only.[170] In other words, if campaigns were co-ordinated, then the cost of co-ordinated campaigns would be accumulated when assessing campaign limits.

147. Vote Leave (as the designated lead 'Leave' group) had a permitted expenditure limit of £7 million during the Referendum campaign. As we stated in our Special Report of June 2018, Vote Leave was under investigation by the Electoral Commission, over whether it breached this limit by making a £675,315 payment to another campaign group, BeLeave.[171] These revelations came from both Christopher Wylie, in his evidence to the Committee, and from another whistleblower, Shahmir Sanni, who worked with Vote Leave.[172] The £675,315 payment was registered with the Electoral Commission as a donation from Vote Leave to Darren Grimes, the founder of BeLeave.[173] Some witnesses and outside commentators raised questions about the extent to which it was a genuine donation.[174]

148. The Electoral Commission published the conclusions of its investigation into the campaign spending of Vote Leave and other campaign groups on 17 July 2018. The findings show that:

- Vote Leave and Darren Grimes, the founder of the BeLeave campaign group, broke electoral law;
- there was significant evidence of joint working between the lead campaign, Vote Leave, and BeLeave;
- BeLeave spent more than £675,000 with AIQ, under a common plan with Vote Leave, which should have been declared by Vote Leave. This extra money resulted in Vote Leave exceeding its legal spending limit of £7 million by almost £500,000;
- Vote Leave also returned an incomplete and inaccurate spending report, with nearly £234,501 reported incorrectly, and invoices missing for £12,849,99 of spending.[175]

149. As a result of these findings, The Electoral Commission has referred David Halsall, the responsible person for Vote Leave, and Darren Grimes to the Metropolitan Police, for the false declaration of campaign spending.[176] As we have previously said, Dominic Cummings, the campaign director of Vote Leave, refused to appear before our Committee. Likewise, the Electoral Commission wrote that "Vote Leave declined to be interviewed.

170 Working together for EU referendum campaigners, The Electoral Commission, p12
171 The Electoral Commission's investigation was into Vote Leave Limited, Mr Darren Grimes and Veterans for Britain Limited.
172 Christopher Wylie, Q1307
173 The named recipient was Darren Grimes. Donations and loans received by campaigners in the EU Referendum. Fourth pre-poll report: 10 June 2016 to 22 June 2016, The Electoral Commission.
174 For example, Q1307
175 Report of an investigation in respect of Vote Leave Ltd, Mr Darren Grimes, BeLeave, Veterans for Britain: concerning campaign funding and spending for the 2016 referendum on the UK's membership of the EU, Electoral Commission, 17 July 2018
176 Report of an investigation in respect of Vote Leave Ltd, Mr Darren Grimes, BeLeave, Veterans for Britain: concerning campaign funding and spending for the 2016 referendum on the UK's membership of the EU, Electoral Commission, 17 July 2018

Its lack of co-operation is reflected in the penalties". The level of fines are £61,000 for Vote Leave, £20,000 for Darren Grimes, and £250 for Veterans for Britain (for inaccurately reporting a donation it received from Vote Leave.)

150. As we also highlighted in our Special Report, evidence to the Committee from Facebook showed that BeLeave used AggregateIQ datasets covering the "exact same audiences".[177] AIQ had a working relationship with SCL/Cambridge Analytica, focused on the use of data in campaigns. AIQ had links with Vote Leave and other Brexit campaigns, including Be Leave, Veterans for Britain and the DUP and all used the company in the short period immediately prior to the EU Referendum. We believe that the precise nature of the co-ordination between the different organisations and campaigns should be investigated further to establish if the law concerning spending limits and data protection was observed.

Leave.EU and data from Eldon Insurance allegedly used for campaigning work

151. Insurance companies have access to detailed personal information about their customers. Arron Banks described Leave.EU's method of campaigning, by using the micro-targeting of individual voters:

> My experience of social media is it is a firestorm that, just like a bush fire, it blows over the thing. Our skill was creating bush fires and then putting a big fan on and making the fan blow. […] the immigration issue was the one that set the wild fires burning.[178]

152. The question that then arises is how did Leave.EU acquire data to set "wild fires burning" on the immigration issue? We heard evidence from various witnesses and from written statements that, during the Referendum campaign, Leave.EU used insurance data for such micro-targeting of voters, data from Arron Banks' company, Eldon Insurance Services Ltd. Arron Banks described the way Leave.EU carried out psychological profiling, and told us that "insurance is all about how you target your product to the person you want to target to".[179]

> The three things that were of interest to me were: obviously, the Referendum campaign, my insurance business—could they offer services that were along those sorts of lines?—and thirdly, with the UKIP hat on, would it be a useful messaging tool for UKIP? I can see why you would think there would be a conflict, but there really wasn't.[180]

153. Paul-Olivier Dehaye, founder of PersonalDataIO, told us that Leave.EU mailings had had insurance adverts for one of Arron Banks' companies at the bottom of the mailings.[181] Evidence submitted to the inquiry recorded Andy Wigmore, Director of Communications for the Leave.EU campaign, in conversation with Dr Emma Briant, Senior Lecturer at Essex

177 Letter from Rebecca Stimson, Facebook, to the Chair, 14 May 2018
178 Q3609
179 Q3502
180 Q3502
181 Q1388

University, explaining that the insurance companies' actuaries used data to determine which 12 UK regions Nigel Farage, the then leader of the UKIP, should visit during the campaign.

154. Andy Wigmore described in the taped conversations with Dr Emma Briant the power of using emotion, rather than facts, which "created a wave of hatred and racism and all this right movement, empowering all those things". He spoke of the Nazis' propaganda strategy: "If you take away all the hideous horror […] it was very clear, the way they managed to do what they did. In its pure marketing sense. […] You can see the logic of how they presented things and the imagery, everything from that".[182]

155. However, when Andy Wigmore gave evidence to the Committee and was asked about the recorded conversation with Dr. Briant, his reference to actuaries using data to locate the regions that Mr. Farage should visit, and whether the work of the actuaries was recorded in Leave.EU's spending returns, Andy Wigmore replied, "No, I was wrong. I apologise because that was completely misinterpreted and that was incorrect".[183] In the ICO's interim report on their investigation into data harvesting, they made reference to these allegations of customer data from Eldon Insurance Services being shared with Leave.EU, and then used for political campaign purposes during the EU Referendum. This is contrary to the first and second data protection principles under the Data Protection Act 1998.[184]

156. The ICO's current investigation is also looking into this issue of whether Eldon Insurance Ltd's call centre staff used customer databases to make calls on behalf of Leave.EU. This would be in contravention of the Privacy and Electronic Communication Regulations 2003.[185] Brittany Kaiser told us that she visited the Eldon Insurance and Leave.EU headquarters, "which was in the same building with the same staff. When a senior data scientist and I spent time with their phone bank I was told by the people using the phone bank that the individuals they were calling were from the insurance database", to which Arron Banks responded, "A flat lie".[186] Yet on 25 January 2016, a French news documentary showed Arron Banks' insurance call centre employees working at the call centre for Leave.EU, with Liz Bilney, on tape, confirming this.[187]

157. The ICO is also investigating whether Eldon Insurance Services Ltd transferred its insurance customer data to the USA, specifically to the University of Mississippi, which would be in contravention of the eighth data protection principle, under the Data Protection Act 1998. A UK resident, Kyle Taylor, has filed a law suit in Mississippi to determine whether UK data was transferred to Mississippi. The ICO's line of inquiry "is ongoing".[188]

158. Determining whether there was collusion between (technically separate) campaigns in the EU Referendum, in breach of rules on spending limits, has been a matter primarily for the Election Commission, which has now reported its highly critical findings into

182 Dr Emma Briant (FKN0071)
183 Q3619
184 Investigation into data analytics for political purposes: investigation update, ICO, July 2018
185 Investigation into data analytics for political purposes: investigation update, ICO, July 2018, page 4
186 Q3615
187 The French documentary link can be found on YouTube.
188 Investigation into the use of data analytics in political campaigns: investigation update, ICO, July 2018, p38

the activities of Vote Leave, Darren Grimes and BeLeave.[189] Determining whether data protection law was breached by any use of shared datasets by BeLeave and AIQ is similarly a matter for the Information Commissioner and the police. We look forward to the ICO's findings, on which we may wish to comment further in our second Report later this year. The Electoral Commission's report has vindicated evidence given to the Committee about the breaching of spending limits, and we look forward to the ICO's final findings.[190]

159. **Data sets allegedly enabled Leave.EU to push their message to groups of people that they might not otherwise have had information about. This evidence informed our inquiry, backing up concerns that data is being harvested and utilised from many people unwittingly and used for purposes of which they may not be aware. It is alleged that Leave.EU obtained data used during the Referendum from insurance data from companies owned by Arron Banks. The Information Commissioner's Office is investigating both the alleged misuse of customer data from Arron Banks' Eldon Insurance Services Ltd and the misuse of that data by the call centre staff, to make calls on behalf of Leave.EU. These are extremely serious allegations. We look forward to hearing the final results of the ICO's investigations, when it reports in October 2018.**

189 Report of an investigation in respect of Vote Leave Ltd, Mr Darren Grimes, BeLeave, Veterans for Britain: concerning campaign funding and spending for the 2016 referendum on the UK's membership of the EU, Electoral Commission, 17 July 2018

190 Ibid.

5 Russian influence in political campaigns

Introduction

160. The speed of technological development has coincided with a crisis of confidence in institutions and the media in the West. There is a global phenomenon of foreign countries wanting to influence public opinion through disinformation. A report from the University of Oxford published in July 2018 identified evidence of formally-organised social media manipulation campaigns in 48 countries, up from 28 countries last year.[191] The evidence led us to the role of Russia specifically, in supporting organisations that create and disseminate disinformation, false and hyper-partisan content, with the purpose of undermining public confidence and of destabilising democratic states. This activity we are describing as 'disinformation' and it is an active threat.

161. The Committee heard evidence of a co-ordinated, long-standing campaign by the Russian Government to influence UK elections and referenda, and similar evidence of foreign interference is being investigated by the US Congress in respect of the 2016 US Presidential Election. Thanks to these hearings we know that, during the Presidential Election, the Russians ran over 3,000 adverts on Facebook and Instagram to promote 120 Facebook pages in a campaign that reached 126 million Americans. In further evidence from Facebook given to our Committee, we know that the Russians used sophisticated targeting techniques and created customized audiences to amplify extreme voices in the campaign, particular those on sensitive topics such as race relations and immigration.[192]

162. Disinformation is an unconventional warfare, using technology to disrupt, to magnify, and to distort.[193] According to research from 89up, the communications agency, Russia Today (RT) and Sputnik published 261 media articles on the EU Referendum, with an anti-EU sentiment, between 1 January 2016 and 23 June 2016. Their report also showed that RT and Sputnik had more reach on Twitter for anti-EU content than either Vote Leave or Leave.EU, during the Referendum campaign.[194] A joint research project by the Universities of Swansea and of Berkeley, at the University of California, also identified 156,252 Russian accounts tweeting about #Brexit and that they posted over 45,000 Brexit messages in the last 48 hours of the campaign.[195]

163. In the context of this inquiry, we first learnt about the enormity of the problem when we visited New York in February 2018, and heard from Clint Watts, senior fellow at the Center for Cyber and Homeland Security, George Washington University, about the prevalence of disinformation, perpetrated by Russia Today and Sputnik News, and disseminated through pro-Russia accounts on Twitter and Facebook.[196] Back at home, Bill Browder, CEO and co-founder of Hermitage Capital Management, told us that "the

191 Challenging Truth and Trust: a global inventory of organized social media manipulation, Samantha Bradshaw, Philip N. Howard, Computational Propaganda Research Project, Oxford Internet Institute, July 2018.

192 Facebook letter from Rebecca Stimson to Damian Collins, 8 June 2018

193 Fake News: A Roadmap, ed Jente Althuis and Leonie Haiden, NATO Strategic Communications Centre of Excellence, the King's Centre for Strategic Communications, January 2018

194 Putin's Brexit? The influence of Kremlin media and bots during the 2016 UK EU referendum, 89up, February 2018.

195 Russian Twitter accounts promoted Brexit ahead of EU referendum, Reuters, 15 November 2017.

196 An example of the work of Clint Watts is his statement prepared for the US Senate Select Committee on Intelligence, Disinformation: a primer in Russian active measures and influence campaigns, Clint Watts, March 2017.

purpose of Russian disinformation and Russian propaganda is to plant a seed of doubt in everybody's mind. If they can create that kind of confusion, they have accomplished their objectives".[197] Edward Lucas, writer and security-policy expert, described the power of Russia to influence, even though Russia is weaker economically:

> It is true that Russia is a lot weaker than the West. Its population is about one-seventh of ours. Its GDP is about one-fourteenth. But it still has the capacity to do us harm. It poses a military threat in the Baltic states, where geography and NATO's weaknesses make it hard to muster a strong conventional defence. It has a proven ability to confuse, distract and distort decision-making, both by targeted attacks on elites, and exerting broader influence on public opinion.[198]

164. This chapter will study the extent of Russian interference in UK politics, specifically focussing on the EU Referendum of 2016. We will also comment on the Catalonia Referendum of 2017, and the use that Russia makes of tech companies, specifically Facebook.

Use of the data obtained by Aleksandr Kogan in Russia

165. Jeff Silvester, from AIQ, confirmed to us that there was an 80% overlap in terms of common members of audiences that had been used in campaigns run by both SCL/Cambridge Analytica and by AIQ. He confirmed that during the presidential primaries, AIQ advertised, using specific custom audiences with names and email addresses, saying "It is very possible and likely that that information came in, but whether it came directly from the campaign or from SCL I do not know".[199] These datasets were created using Ripon, and "the information that was fed into Ripon once the campaign started was the typical type: who has been contacted and said they would support the campaign".[200] Aleksandr Kogan was supplying information to go into the system to help targeting those adverts.[201]

166. Aleksandr Kogan told us that he worked at the University of St Petersburg, Russia, in the summer of 2013.[202] As a result of that initial work, Dr Kogan was involved in a research group at the same university, studying the issue of cyber-bullying, between 2014 and 2016. Dr Kogan carried out this work at the same time as he was working with Cambridge Analytica.[203] When asked about the financing of the research group, Dr Kogan told us he thought that the Russian Government gave a block grant to the university. When asked about whether a research paper was published, he told us "I truly don't know the exact details of that project. I don't know the final results. The methodology I loosely understand and remember. Just keep in mind I was a name on a grant rather than an active participant and collaborator on this".[204]

197 Q851
198 Edward Lucas (FKN0052)
199 Q2922
200 Q2924
201 Q2925
202 Qq2043 and 2044
203 Qq2045 to 2047
204 Q2076

167. Dr Kogan gave evidence to us in April 2018. Since that time, the ICO has been investigating Dr Kogan and his data. The Information Commissioner, Elizabeth Denham, and her deputy recently met with law enforcement agencies in the US. The Information Commissioner's deputy, James Dipple-Johnstone, confirmed that "some of the systems linked to the investigation were accessed from IP addresses that resolve to Russia and other areas of the CIS (Commonwealth of Independent States)".[205] It is of concern that people in Russia could have benefitted from the work that Dr Kogan carried out in the UK, in connection with his work for Cambridge Analytica. We look forward to reading the ICO's findings on this issue in due course.

The role of social media companies in disseminating Russian disinformation

168. Throughout this inquiry, from October 2017 to June 2018, we attempted to gain information from Facebook about the extent of Russian interference in UK political campaigns. Time and again, Facebook chose to avoid answering our written and oral questions, to the point of obfuscation.

169. Facebook finally agreed, in January 2018, to expand its US investigation into alleged Russian interference in the EU Referendum. However, it downplayed the extent of the problem, and told us that the St Petersburg-based Internet Research Agency (IRA) had bought only three adverts for $0.97 in the days before the Brexit vote.[206] This did not include unpaid posts, and Facebook did not broaden its investigation beyond those IRA 'troll farms' identified during the US presidential election investigation.

170. According to evidence that Facebook submitted to Congress, and later released publicly, Russian anti-immigrant adverts were placed in October 2015 targeting the UK, as well as Germany and France. These amounted to 5,514.85 roubles (around £66).[207] We asked Facebook to confirm the total amount of political advertising paid for by Russian agencies targeting Facebook users in the UK since October 2015, to date, and it replied with the following statement, in June 2018:

> As we have previously reported to the Committee, we have not found any systematic targeting of the UK by the IRA in the Referendum period (15 April to 23 June 2016), only the minimal activity we reported to the Committee already. Looking further back over the activity of the IRA accounts from as early as January 2015 (including the period of over a year before the start of the regulated referendum period), the total spend on impressions delivered to the UK is approximately $463. This is inclusive of all of the adverts released by the US Congress last month. The $1 spend we previously reported reflects the amount spent during the regulated referendum period by the IRA which is the time period which the Election Commission asked us to investigate.[208]

171. When we heard from Facebook in Washington D.C., Simon Milner, the then Policy Director UK, Middle East and Africa, Facebook, said that: "Unlike the US election, we have still not been furnished with any intelligence reports from the UK authorities to suggest

205 Elizabeth Denham: data crimes are real crimes, Carole Cadwalladr, The Observer, 15 July 2018
206 Letter from Simon Milner to Damian Collins, 20 December 2017, not published
207 Letter from Rebecca Stimson to Damian Collins, 8 June 2018
208 Letter from Rebecca Stimson to Damian Collins, 8 June 2018

that there was direct Russian interference using Facebook in the Brexit Referendum".[209] However, it was pressure from the US Senate, and not specific US intelligence staff, that made Facebook do its research into the US election.[210] We deem Mr Milner's comments to the Committee to have been disingenuous and typical of Facebook's handling of our questions.

172. There has been a continual reluctance on the part of Facebook to conduct its own research on whether its organisation has been used by Russia to influence others. Facebook knows its system better than anyone else, and should not be passively reacting to outside concerns before they carry out their own research and take action.

173. In January 2018, the Prime Minister, Rt Hon Theresa May MP, announced the establishment of a dedicated national security communications unit, to be charged with combating fake news and disinformation by state actors and by others.[211] This followed her speech a few months earlier, when she accused Russia of meddling in elections and planting fake news, in an attempt to 'weaponise information' and sow discord in the West.[212]

174. When we took evidence from the then Secretary of State for DCMS in March, Rt Hon Matt Hancock MP, he accepted that Russia had been involved in directing disinformation at countries including the UK.[213] He said that tackling the "multiple threats" of disinformation and fake news "is incredibly important to safeguarding our democracy," and, indeed, was "the No. 1 issue faced by our media."[214]

175. Over and above the Review, the then Secretary of State said that he was "actively waiting for [the DCMS Committee's] report". He did not want to "rule out legislative options to insist on the transparency of platforms." While he detected a "noticeable" improvement in the level of engagement from the big social media companies over the past six months, there was "a lot more to do."[215] He said that the Government was exploring a range of ideas, including the option of tightening existing rules to tackle illegal content online, and working under the Digital Charter with publishers, tech companies, civil society and others to establish a new framework that protects user' rights.[216]

176. ***In November 2017, the Prime Minister accused Russia of meddling in elections and planting 'fake news' in an attempt to 'weaponise information' and sow discord in the West. It is clear from comments made by the then Secretary of State in evidence to us that he shares her concerns. However, there is a disconnect between the Government's expressed concerns about foreign interference in elections, and tech companies intractability in recognising the issue. We would anticipate that this issue will be addressed, with possible plans of action, in the White Paper this Autumn.***

209 Q369
210 Chair, Q377. The information was obtained during a private meeting, when the Committee was in Washington D.C.
211 The Unit is cross-Government but sits within the Cabinet Office. Domestic disinformation and the role of digital and digital policy, and policy towards the big digital companies and the lead for interactions with those, sit in DCMS' Digital and Tech Policy Directorate.
212 Prime Minister's Speech at Lord Mayor's Banquet, 13 November 2017, reported in *The Times*.
213 Q950
214 Q949
215 Q953
216 The Future of the Media, Rt Hon Matt Hancock MP, the Oxford Media Convention, 12 March 2018.

Leave.EU, Arron Banks, and Russia

177. Our inquiry into Russian interference broadened even further when we were contacted by three different individuals, with information surrounding email exchanges between Arron Banks and representatives from the Russian Embassy in London.[217] The emails describe multiple meetings between Arron Banks, Andy Wigmore and Russian officials, including the Russian Ambassador to the UK, Alexander Yakovenko, involving discussions around gold and diamond acquisitions, the passing of confidential documents, and the exchange of information surrounding the EU Referendum. These meetings, so far as we are aware, began in the period from November 2015, immediately prior to the EU Referendum.

178. In these emails, Mr. Banks talked of briefing the Ambassador about the Referendum, and that there was a lot of interest about it in America.[218] He met with the Ambassador, Mr. Yakovenko, and wrote afterward that "I'm very bullish on gold so keen to have a look".[219] In January 2016, Andrew Umbers, chairman of Oakwell Capital Partners, a marketing company to the sports and media tech industry,[220] wrote to Siman Povarenkin, a Russian businessman with a tier one visa, suggesting a meeting with "the appropriate Sberbank decision maker" in Moscow, to discuss co-operation with individuals at Sberbank, the state-owned bank that, according to the email, are the "major lenders to all six Russian gold companies."[221] Arron Banks and Andy Wigmore were copied into this email. The emails that we have seen cover different areas, including Alrosa, the Russian diamond monopoly, "touted as one of the companies which could be privatised."[222]

179. Another email links Arron Banks with Alexander Nekrassov, a former Kremlin and government adviser:

> I have been in touch with Alexander Nekrassov and he is willing to help us from any angle in the Leave campaign. I realise he is a controversial, outspoken person and that there may be some clash of personalities. However, if managed well, he could be a valuable asset to the campaign.[223]

180. Mr Nekrassov is also Director of Financial Services of New Century Media. New Century Media's Chairman is David Burnside, who was previously a Democratic Unionist Party (DUP) MP and who has had close connections with Vincent Tchenguiz, who himself used to be the largest shareholder in SCL.[224]

181. Another email from Arron Banks states: "OK, so there are 11,425 emails that have been filtered from the 43,000. I would suggest that half of these are irrelevant but the main searches for subjects and people are all here—I have checked".[225] We asked Andy Wigmore if, in addition to arranging social meetings for Arron Banks with the Russian Embassy in London, he sent documents to the Russian Embassy. In particular, we asked

217 These contacts occurred at the same time as *The Sunday Times* and *The Observer* published articles surrounding Russian contact with Arron Banks and Andy Wigmore, in June 2018.
218 12 October 2015 email, not published.
219 17 November 2015 email, not published.
220 Oakwell Capital Partners website, accessed 7 July 2018.
221 18 January 2016 email, from Andrew Umbers to Siman Povarenkin, Sergey Kuznetsov, Andy Wigmore, Arron Banks, not published.
222 Email from Vick van den Brul to Andy Wigmore, 2 February 2016, not published.
223 Email, date unknown, labelled, "Very strange email chain", not published
224 Ibid.
225 Email from Andy Wigmore to Isabel Oakeshott and others, 24 August 2016

whether he had contacted the Russian Embassy about George Cottrell, a former UKIP fundraiser and adviser to Nigel Farage. He denied doing this.[226] However, an email, sent by him, has been made public, which has six attachments, including FBI documents and the George Cottrell indictment.[227]

182. When asked about the contents of some of these emails that state that Arron Banks was in Russia in 2016, Mr Banks showed the Committee two Russian visas, photocopied from his two passports, one dated 22 October 2014 and one dated 13 March 2015, and said, "*The Sunday Times* article that said I travelled to Moscow, I have fairly definitive proof here that I did not and there we are".[228] He told us that he did not have a second passport.[229]

183. At the time of the email exchanges in 2016, Andy Wigmore had told reporters that Arron Banks was in Russia, but he swept this aside when giving evidence to us: "I can remember teasing many journalists when they asked, 'Where is Arron?' I would often say, 'He's in Moscow. He's in Russia.'"[230] Mr Wigmore said that information "had just come out about Arron being an agent from a document that is called the Atlantic Council document accusing him of being absolutely all of those things. We teased people about it".[231]

184. The document to which Mr. Wigmore was referring was the Atlantic Council's "The Kremlin's Trojan Horses" which claims that the Kremlin used politicians, experts, and individuals who had expressed support for the Kremlin's action as Trojan horses, to destabilise European politics, and referred specifically to UKIP campaigners working with the Leave.EU and Grassroots Out campaigns.[232] However, the Atlantic Council document was published on 15 November 2016, a date after the email exchanges to which Mr. Wigmore referred. Mr. Wigmore told us, "My job is to be provocative. That is my job. I am trying to give you—I have this sense of humour.[233] […] My job is to spin".[234]

185. **Arron Banks is, reportedly, the largest individual donor in UK political history. As far as we understand, he met with the Russian Ambassador, for the first time, in the run up to the EU Referendum. Evidence discloses that he discussed business ventures within Russia and beyond, and other financial ventures, in a series of meetings with Russian Embassy staff. Arron Banks and Andy Wigmore have misled the Committee on the number of meetings that took place with the Russian Embassy and walked out of the Committee's evidence session to avoid scrutiny of the content of the discussions with the Russian Embassy.**

186. ***From the emails that we have seen, it is evident that Arron Banks had many meetings with Russian officials, including the Russian Ambassador, Alexander Yakovenko, between 2015 and 2017. The meetings involved discussions about business deals involving Alrosa, the Russian diamond monopoly, the purchase of gold mines,***

226 Email from Andy Wigmore to Sergey Fedichkin, Russian Embassy, 20 August 2016
227 George Cottrell was arrested in July 2016 while visiting the US by the FBI and was indicted on 21 counts for conspiracy to commit money-laundering, wire fraud, blackmail and extortion. He served eight months in prison.
228 Q3737
229 Q3739
230 Q3519
231 Q3519
232 The Kremlin's Trojan Horses, Atlantic Council, 15 November 2016.
233 Q3741
234 Q3519

funded by Sberbank, the Russian-state bank, and the transferring of confidential documents to Russian officials. Mr. Banks seemed to want to hide the extent of his contacts with Russia, while his spokesman Andy Wigmore's statements have been unreliable—by his own admission—and cannot be taken at face value. Mr Wigmore is a self-confessed liar and, as a result, little significance can be attached to anything that he says. It is unclear whether Mr. Banks profited from business deals arising from meetings arranged by Russian officials. We understand that the National Crime Agency (NCA) is investigating these matters. We believe that they should be given full access to any relevant information that will aid their inquiry.

Foreign investment in the EU Referendum

Arron Banks and his own donations

187. Arron Banks is, to date, the person who has given the largest donation to a political campaign in British history, reported to be £8.4 million.[235] When questioned by us in June 2018, Mr. Banks could not give a clear answer about where the money for his donations to support the different Leave campaigns came from. Previously, in April 2018, Mr Wigmore had reported that the sale of NewLaw Legal in 2014 had generated Mr Banks' donation for the Referendum, yet allegedly he was not a shareholder or a director at the time (although Mr Banks insisted he *was* a shareholder at the time of the sale).[236]

188. There have been persistent questions over the extent of Mr Banks' wealth. Arron Banks refused to answer the question over the solvency of the Southern Rock Insurance Company, which he owns.[237] Alan Kentish, another Brexit-connected associate, was on the board of directors of Southern Rock, as well as being involved in ICS Risk Solutions (the parent company of Eldon Insurance, the insurer behind Go Skippy, and owned by Arron Banks, and a holding company on the Isle of Man). The day after the Referendum, Alan Kentish became a director of ICS.[238] STM founded Better for the Country, which gave £1.95 million to the umbrella Leave group, Grassroots Out. Better for the Country is owned by Arron Banks. A Channel 4 investigation has revealed court documents in South Africa that pre-date evidence to our Committee. They relate to Mr Banks seeking contact with Russian investors, which suggests he was actively seeking financial support in Russia for his mining businesses in southern Africa.[239]

189. In 2015, STM became the first company in Jersey to be prosecuted for money-laundering compliance failures. STM was managing operations for Henley & Partners, the company involved in foreign campaigns with Cambridge Analytica.[240] Previously, in 2010, STM had used Henley & Partners to help the Ukrainian politician, Viacheslav Suprunenko, apply for a passport in St Kitts and Nevis. He was at the time wanted by Interpol for assault during an armed robbery to recover documents in a business dispute.[241]

235 Q3582
236 Qq3627 and 3628
237 Qq3554–3561.This has been investigated by the Gibraltar Finance Services Commission.
238 STM Group PLC is a multi-jurisdictional financial services group listed on the Alternative Investment Market (AIM) of the London Stock Exchange. The Board of STM consists of: Robin Ellison (Interim Chairman); Therese Neish (CFO); and Malcolm Berryman (NED).
239 https://www.channel4.com/news/exclusive-court-documents-claim-new-arron-banks-links-with-russia
240 See Chapter 6
241 https://www.opendemocracy.net/uk/brexitinc/marcus-leroux-leigh-baldwin/brexit-s-offshore-secrets-0

190. The Electoral Commission is carrying out an investigation to trace the source of the money that Arron Banks donated to Leave.EU and Better for the Country.[242]

191. ***Arron Banks is believed to have donated £8.4 million to the Leave campaign, the largest political donation in British politics, but it is unclear from where he obtained that amount of money. He failed to satisfy us that his own donations had, in fact, come from sources within the UK. At the same time, we have evidence of Mr. Banks' discussions with Russian Embassy contacts, including the Russian Ambassador, over potential gold and diamond deals, and the passing of confidential information by Mr Banks. The Electoral Commission should pursue investigations into donations that Arron Banks made to the Leave campaign, to verify that the money was not sourced from abroad. Should there be any doubt, the matter should be referred to the NCA. The Electoral Commission should come forward with proposals for more stringent requirements for major donors to demonstrate the source of their donations.***

192. ***The Electoral Commission has recommended that there should be a change in the rules covering political spending, so that limits are put on the amount of money an individual can donate. We agree with this recommendation, and urge the Government to take this proposal on board.***

Catalonia Referendum

193. An example of alleged Russian interference in other countries' affairs is provided by the Catalan independence Referendum. This was held on 1 October 2017, having been passed by the Parliament of Catalonia and the Law on the Referendum on Self-determination of Catalonia. It was declared illegal on 7 September 2017 and suspended by the Constitutional Court of Spain, declaring it a breach of the Spanish Constitution of 1978.[243]

194. Francisco de Borja Lasheras told us about the context in which alleged Russian interference occurred:

> In the case of Catalonia, we saw a mixture of things that were right—that there were instances of police violence—and of fake news, biased reporting and a misleading account. With all of those patterns, we cannot attribute all of that to Russia; that would just not be correct. It is important to distinguish between proper fake news—there were cases of fake news—and biased reporting. In the case of the Russian-affiliated outlets, you see a little bit of both: you see instances of balanced reporting with instances of biased reporting and fake news.[244]

195. Information operations should not be studied in isolation; they are part of a complex, interrelated group of actions that disseminate confusion and unrest. Francisco de Borja Lasheras described the context: "You had democratic rule of law versus the right to decide, protest versus the constitutional order, and territorial integrity versus succession.

242 Digital Campaigning: increasing transparency for voters, The Electoral Commission, June 2018

243 The referendum question was "Do you want Catalonia to become an independent state in the form of a republic", and the 'yes' side won with 92.01% voting for independence, and 7.99% voting against, on a turnout of 43.03%.

244 Q52

So it did provide an opening for a democratic crisis that is ongoing and very complex".[245] Our witnesses talked about the prevalence of up to 70% to 80% of bots that retweet disinformation.[246] Furthermore, journalists who reported on Russian troll farms were attacked verbally and so the established media was undermined by disseminating false information purporting to be fact, such as the claim that 900 people had been injured in Catalonia, which did not happen.[247]

196. David Alandete told us about Sputnik's editor-in-chief, Margarita Simonyan, who is close to Putin, and advised that "I would seriously look into RT and Sputnik, what information they do and what they cover here in the United Kingdom about all sorts of issues because I think it is worth seeing. The State Department in the United States has just requested that they register as foreign agents. Twitter has banned them from buying advertisements, because they think it is propaganda and not advertisement for commercial reasons".[248]

197. **We heard evidence that showed alleged Russian interference in the Spanish Referendum, in October 2017. During the Referendum campaign, Russia provoked conflict, through a mixture of misleading information and disinformation, between people within Spain, and between Spain and other member states in the EU, and in NATO. We heard evidence that showed that Russia had a special interest in discrediting the Spanish democratic system, through Russian state affiliated TV organisations spreading propaganda that benefitted those wanting independence in Catalonia.**

Co-ordination between UK Departments and between countries

198. The UK Government has made Russia a tier 1 national security threat.[249] With that should come a united Government approach, but Edward Lucas told us that "everybody's treading on everybody else's toes, and what we have seen so far in Whitehall is that there's been a massive turf war, rather than anything that's actually dealing seriously with Russia".[250] The problem has been to treat Russia as an emerging economy, which has "created lobbies in this country who are extremely unhappy at the thought of relations with Russia going downhill, and you get those lobbies exercising power in all the political powers".[251]

199. Six Committees at the House of Commons, including our own, formed the Russian Co-ordination Group in April 2018. It comprises of the Chairs (and selected members) of Select Committees with an interest in Russia.[252] The Group aims to co-ordinate Committee work relating to scrutiny of Russian-related activity by sharing knowledge about relevant inquiries by Committees. The chair of the Group, Tom Tugendhat MP, said about its launch: "We want to produce a system of work that answers the malign influence we are seeing in a collective way from Russia."[253]

245 Q52
246 David Alandete, Q53
247 David Alandete, Q60; Francisco de Borja Lasheras, Q61
248 Q68
249 Edward Lucas, Q887
250 Q888
251 Q888
252 The Select Committees in the Russian Co-ordination group are Defence, Foreign Affairs (who provides the Chair, Tom Tugendhat MP, and the Secretary, Bob Seely MP), Treasury, DCMS, JCNSS and Home Affairs. It is anticipated that the Intelligence and Security Committee will also be represented, with its involvement subject to the necessary restrictions around the confidentiality of its work.
253 The launch was on 20 April 2018.

200. This type of collaboration should be mirrored in the Government, with cross-Departmental work. Edward Lucas cites the work carried out in Estonia, Latvia, and Lithuania, and in Sweden and Finland, where people have been warning the UK since the 1990s about this emerging threat.[254] Departments should be working together, sharing data, intelligence and expert knowledge, involving universities, the criminal justice system, intelligence agencies, and the financial system.[255]

201. Representatives of this Committee participated in the inter-parliamentary meeting at the Atlantic Council, on 16 July 2018, in Washington D.C., in partnership with the Transatlantic Commission on Election Integrity. The event brought together US, Canadian and EU political representatives, led by Senator Warner and Senator Rubio, to discuss Russian interference in democratic elections around the world. We have included the recommendations from this meeting in the Annex to this Report. One of the recommendations encourages greater sharing of information and best practices between countries:

> We support greater and sustained transatlantic cooperation, including between national governments, NATO, and the European Union, to share information on risks, vulnerabilities, and best practices to counter interference. Coordination between parliamentarians and open, regular dialogue with social media, technology companies, and civil society can strengthen these efforts.[256]

202. ***We recommend that the UK Government approaches other governments and follows the recommendation agreed by US and EU representatives, including representatives from this Committee, at the recent inter-parliamentary meeting at the Atlantic Council. The Government should share information on risks, vulnerabilities, and best practices to counter Russian interference, and co-ordinate between parliamentarians across the world. Only by sharing information, resources, and best practice will this Government be able to combat Russian interference in our elections. We look forward to a White Paper this autumn, and the opportunity for the Government to set out the practical steps that it will follow to ensure greater global co-operation to combat Russian interference.***

203. ***Just as six Select Committees have joined forces in an attempt to combat Russian influence in our political discourse, so the Government should co-ordinate joint working with the different relevant Departments. Those Departments should not be working in silos, but should work together, sharing data, intelligence and expert knowledge, to counter the emerging threat of Russia, and other malign players.***

204. ***We note that the Mueller Inquiry into Russian interference in the United States is ongoing. It would be wrong for Robert Mueller's investigation to take the lead about related issues in the UK. We recommend that the Government makes a statement about how many investigations are currently being carried out into Russian interference in UK politics and ensures that a co-ordinated structure exists, involving the Electoral Commission and the Information Commissioner, as well as other relevant authorities.***

254 Edward Lucas, Q889
255 Edward Lucas, Q892
256 Refer to Annex for the full set of recommendations

6 SCL influence in foreign elections

Introduction

205. The influencing of elections by foreign powers, through the distortion of facts, or by the micro-targeting of voters, to persuade them to vote in a certain way, or to suppress their desire to vote at all, has been a reoccurring theme throughout this inquiry. This chapter will explore the disturbing inter-relation between disinformation and the manipulation of election campaigns, concentrating on the work of SCL Elections, and associated companies.

General

206. The Committee received evidence about the role of SCL Elections, a company that Alexander Nix formed, as an offshoot of SCL Group, in 2011, and its role in foreign elections, including its use of misinformation, disinformation and micro-targeting, which may have crossed the line into unethical, or even illegal behaviour. A Channel 4 undercover investigation, broadcast in March 2018, filmed Mark Turnbull, former Managing Director of SCL Elections, and Alexander Nix, the then CEO of Cambridge Analytica, talking about using misinformation, dirty tricks and the manipulation of social media to influence elections around the world, and boasting of using bribery, honey traps and sex workers to discredit politicians and to influence the political outcome of elections in elections in several countries.[257]

207. Mr Turnbull also talked about the manipulation of social media companies, in order to distribute negative material on political opponents, done in such a way so as not to be identified as the source of the material:

> You're creating social media content that you're putting out into social media and you're just gently amplifying, by hitting influential people who have huge following on Facebook and Twitter, so they retweet, re-post, and so this stuff infiltrates the online community and expands, but with no brand, so it's unattributable, untrackable. […] [W]e just put information into the bloodstream to the Internet, and then watch is grow, give it a little push every now and again, over time, to watch it take shape.[258]

208. Mark Turnbull described how they "ghosted in and ghosted out" of election campaigns.[259] In a recorded telephone conversation with the Channel 4 reporter, Alexander Nix said that "we do incognito very well indeed, in fact we have many clients who never wish to have our relationship with them made public. […] And, we're used to that, we're used to operating through different vehicles, in the shadows, and I look forward to building a very long-term and secretive relationship with you".[260]

209. When Alexander Nix first gave evidence to us, he described SCL's political work:

257 Exposed: Undercover secrets of Trump's data firm, Channel 4 News, March 2018.
258 Exposed: Undercover secrets of Trump's data firm, Channel 4 News, March 2018.
259 Exposed: Undercover secrets of Trump's data firm, Channel 4 News, March 2018.
260 Exposed: Undercover secrets of Trump's data firm, Channel 4 News, March 2018.

> We have been running election campaigns since 1994. We take on a number of national elections every year. That could be three, four, five, six, seven elections across the world in every single year for prime ministers and presidents. That could be in Asia, Latin America, Europe, Africa or beyond. […] We have a political division, but our political division is only, say, 20% or 25% of our entire business.[261]

210. The following election and referenda campaigns were mentioned by Mr. Turnbull and Mr. Nix, over the course of the Channel 4 meetings: Kenya, Kenyatta campaign 2013; Kenya, Kenyatta campaign 2017; Ghana 2013; Mexico; Brazil; Australia; Thailand; Malaysia; Indonesia; India; Nigeria; Pakistan; Philippines; Germany; England; Slovakia; Czech Republic; and Kosovo.[262] Ex-SCL employees have also mentioned: France; Guyana; Gambia; Germany; Italy; Kenya; Malaysia; Mongolia; Niger; Nigeria; Peru; St Kitts and Nevis; St. Lucia; and Trinidad and Tobago. SCL may also have worked on the Mayoral election campaign in Buenos Aires in 2015 for Mauricio Macri, including delivering some target audience analysis work.[263]

211. We were told that, behind much of SCL Elections' campaigning work was the hidden hand of Christian Kalin, Chairman of Henley and Partners, who arranged for investors to supply the funding to pay for campaigns, and then organised SCL to write their manifesto and oversee the whole campaign process. In exchange, Alexander Nix told us, Henley and Partners would gain exclusive passport rights for that country, under a citizenship-by-investment (CBI) programme.[264] Alexander Nix and Christian Kalin have been described as having a 'Faustian pact'.[265] With the exclusive passport rights came a government that would be conducive to Mr. Kalin and his clients.[266]

212. Alexander Nix told the Committee that, at times, SCL Elections would undertake eight, nine or 10 elections a year, "and we are not limited by geography, so this really could be from the Caribbean to Asia to Africa to Europe or everywhere".[267] When asked about his involvement in the elections with Mr Kalin, including in St Kitts and Nevis, Dominica, St Vincent and the Grenadines, and the Referendum in St Vincent and the Grenadines, he responded:

> I was familiar with Christian Kalin because he had worked in some of the Caribbean islands. I know he used to run a citizen-by-investment programme, certainly in St Kitts and possibly the Dominica. I do not know about the other countries.[268]

213. He told us that Mr Kalin "may well have made contributions towards the election campaigns, but you would have to talk to him about that. […] [M]y understanding is that he may well have financed some of the elections or given contributions towards some

261 Q735
262 Information from Channel 4.
263 Confidential evidence/meetings with ex-SCL employees.
264 Alexander Nix, Q3381
265 What was it really like to work for Cambridge Analytica, Freddy Gray, Spectator podcast, 4 May 2018
266 How Cambridge Analytica fueled a shady global passport bonanza, Ann Marlowe, 1 July 2018
267 Qq816, 3334
268 Q3381

of the elections".[269] This chapter will explore the specific examples of misinformation, disinformation, and malign manipulation that the SCL Group, SCL Elections, SCL Social, and associated companies undertook in certain countries.

St Kitts and Nevis

214. SCL worked on a campaign to win the 2010 general election in St Kitts and Nevis, in the Caribbean, and, according to Freddy Gray, of *The Spectator*:

> SCL practised the dirty trick—or 'counter ops'—that Nix was caught bragging about to undercover reporters in [… the] Channel 4 expose. Nix was not exaggerating. One of the dirty tricks was a sting operation in St Kitts and Nevis. SCL filmed the opposition leader, Lindsay Grant, being offered a bribe by an undercover operative posing as a real-estate investor. Grant didn't exactly help himself by accepting the bribe and even suggesting which offshore bank accounts the money could be paid into.[270]

215. According to evidence we received, this sting operation was arranged entirely by SCL, with the undercover operative—a temporary SCL employee—being paid around £10,000 by Alexander Nix, for the work that they had carried out. Alexander Nix told us that Christian Kalin had run a citizenship-by investment programme in St. Kitts and Nevis.[271]

216. When asked to comment on whether the sting on Lindsay Grant, orchestrated and filmed by SCL, happened, Mr Nix told us that that was nothing more sinister than the undercover reporting that Channel 4 was undertaking itself, and implied that both the SCL and Channel 4's reporting were equivalent in nature. Nothing could be further from the truth. Channel 4's investigation was legitimate journalism; SCL's activities involved the offering of a bribe to an Opposition Leader, with the explicit intention of influencing an election.[272] In the Channel 4 exposé, Mr Nix and Mr Turnbull talked to who they thought was a potential client, and voluntarily exposed techniques that they stated were standard procedure in the company.

217. Henley & Partners have held the exclusive passport rights for St Kitts and Nevis since before 2009. According to the article by Ann Marlowe: "For the bargain price of $150,000, approved applicants who donate to the island's sustainable growth fund can now obtain a passport that, as of 2009, allows visa-free travel to over 100 countries, including the UK and the 26-nation European Schengen zone". By 2014, passports had become St Kitts and Nevis' biggest export (St Kitts does not require citizens to live there), with the revenue accounting for around 25% of GDP.[273] Ann Marlowe wrote:

> Many of the passport holders are from countries with unpopular passports who may otherwise have trouble obtaining travel visas—think Iran, China, Russia, Afghanistan, Pakistan. The firms say their well-heeled clients are seeking protection against unpredictable situations at home amid an era of terrorism fears and economic instability.[274]

269 Qq 3388–3389.
270 'Revealed: Cambridge Analytica and the passport King', Freddy Gray, *The Spectator*, 27 March 2018, accessed June 2018.
271 Q3381
272 Exposed: Undercover secrets of Trump's data firm, Channel 4 news, March 2018.
273 How Cambridge Analytica Fuelled a shady global passport bonanza, Ann Marlowe, Fast Company, 1 July 2018.
274 How Cambridge Analytica Fuelled a shady global passport bonanza, Ann Marlowe, Fast Company, 1 July 2018.

Trinidad and Tobago

218. Evidence submitted by Christopher Wylie highlighted the fact that SCL was influencing the election by disseminating disinformation about the voting preferences of young adults, by fabricating content that they said had come from young people, and then acting on those views:

> Trinidadian elections are affected by the population's mixed ethnicity: political leaders from one group have difficulty in making their messages resonate with those outside of it. Working from this 2009 finding, SCL designed an ambitious campaign of political graffiti that disseminated campaign messages that ostensibly came from the youth. The client party was then able to adopt related policies and claim credit for listening to a 'united youth'.[275]

SCL worked on elections in Trinidad and Tobago in 2010, where their main contact for organising payments related to the campaign appears to have been the disgraced former FIFA executive Jack Warner.

Argentina

219. The Committee saw confidential evidence—a summary of a management meeting at SCL Group from 27 May 2015—in relation to an anti-Kirchner[276] campaign in Argentina, describing "close proximity intelligence gathering efforts" and "information warfare", and the use of "retired Intelligence and Security agency officers from Israel, USA, UK, Spain, and Russia", and the creation of false Facebook and Twitter accounts to support the anti-Kirchner campaign.[277] When questioned whether SCL Group had worked for an opposition party, or some other person interested in influencing politics in Argentina, against the Government, Alexander Nix replied, "That would be the appearance of that, yes".[278]

Malta

220. Henley & Partners has been Malta's exclusive passport agent since it helped to launch its citizenship-by-investment (CBI) programme in 2013. Henley & Partners was granted permission to control the selling of citizenship to eligible investors in Malta, at a cost of €650,000 per passport. As Malta is in the EU, this was especially valuable.[279] We have evidence to show that Dr Kalin was meeting representatives from both political sides in Malta, with a view to mutually-beneficial arrangements. The evidence also shows that Christian Kalin asked SCL to introduce him to Joseph Muscat, the Leader of the Opposition at the time, in June 2011, and indicates that SCL had been advising Malta's Labour Party for several years before the 2013 elections.[280] It is believed that SCL, or its associated companies, worked with the Labour Party there, on the 2013 general election campaign in Malta.

275 Background papers submitted by Christopher Wylie
276 Cristina Kirchner was President of Argentina from 2007 to 2015
277 Confidential evidence shown to the Committee, 5 June 2018
278 Q3399
279 Malta is not for sale website, accessed 23 July 2018
280 Henley asked SCL/Cambridge Analytica to introduce it to Joseph Muscat in 2011, manueldelia.com, 8 April 2018

221. Daphne Caruana Galizia, the Maltese investigative journalist, was investigating the Maltese CBI passport scheme, as well as organised crime in Malta. In October 2017, she was assassinated by a car bomb. On her blog, she wrote "The damage caused to Malta by the sale of citizenship is unquantifiable. Malta is not St. Kitts & Nevis. It is interlocked with the rest of the European Union and has a European economy. […] And the Maltese government is the only EU member state government with which they [Henley & Partners] have a contract".[281]

222. In April 2018, a consortium of 45 journalists from 18 news organisations, including The Guardian, The New York Times, Le Monde, and the Times of Malta, published "The Daphne Project", a collaborative effort to complete Caruana Galizia's investigative work.[282] A week after Daphne Caruana Galizia's assassination, the Maltese Prime Minister Joseph Muscat attended a 'Global Citizenship' conference in Dubai, which was hosted by Henley & Partners, saying that Malta was 'open for business'. Recently, Lord Ashcroft extolled the virtues of Malta, as the "best destination for ambitious UK firms" to have a post-Brexit presence in the EU.[283]

Nigeria and Black Cube

223. Black Cube, a corporate intelligence organisation, is "a select group of veterans from the Israeli elite intelligence units that specialises in tailored solutions to complex business and litigation challenges" and claims that "using our unique intelligence methodology, Black Cube enhances its clients' decision making by providing otherwise unobtainable information".[284] Mark Turnbull told the Channel 4 news reporter: "We have relationships and partnerships with specialist organisations that do that kind of work." He went on to say, "So that […] you know who the opposition is, you know their secrets, you know their tactics."[285]

224. Alexander Nix later told the Channel 4 reporter: "We use some British companies, we use some Israeli companies." One of the Israeli companies he said that Cambridge Analytica used was Black Cube.[286] When asked in oral evidence to confirm this, Alexander Nix said: "I think in the transcript—because I did read this—he said, "Have you worked with Black Cube?" and I replied, "Yes". I was totally mistaken. We have never worked with Black Cube".[287]

225. When Brittany Kaiser gave evidence, she denied that she knew the Israeli cyber security contractors, but told the Committee that two people "came to the office for maybe an hour one day, and plugged something into a computer to show some pieces of information that they had obtained from the opposing campaign".[288] Christopher Wylie told us that "Black Cube was engaged to hack the now President of Nigeria, Buhari, to get access to his medical records and private emails. AIQ worked on that project."[289]

281 No wonder Henley & Partners have broken out into a cold sweat, Running Commentary: Daphne Caruana Galizia's Notebook, 12 May 2017
282 The Daphne Project, The Organized Crime and Corruption Reporting Project (OCCRP), accessed 1 July 2018.
283 Lord Ashcroft: Special Report – Malta makes a strong case to host the EU outposts of British companies after Brexit, Lord Ashcroft, Conservativehome, 28 June 2018.
284 Black Cube website, accessed 12 July 2018
285 Channel 4 transcript of exchanges, not published
286 Channel 4 News transcript of exchanges, not published
287 Q3406
288 Q1617
289 Q1299, also verified by another source

226. We also received an extremely disturbing video from both Brittany Kaiser and Christopher Wylie. Mr. Wylie described the video: "people were being dismembered, were having their throats cut and bleeding to death in a ditch, being burned alive. There are incredibly anti-Islamic and threatening messages portraying Muslims as violent".[290] Jeff Silvester, from AIQ, wrote in evidence to us that AIQ were asked by SCL to promote the video with online advertising, but AIQ refused.[291]

227. Furthermore, a promotional case study of international projects includes a section on Nigeria, which explains how SCL encouraged potential opposition voters not to vote:

> SCL was able to advise that rather than trying to motivate swing voters to vote for our clients, a more effective strategy might be to persuade opposition voters not to vote at all—an action that could be easily monitored. This was achieved by organising anti-election rallies on the day of polling in opposition strongholds. These were conducted by local religious figures to maximise their appeal especially among the spiritual, rural communities.[292]

228. Equally worrying is the fact that the SCL Group carried out work "for the British Government, the US Government and other allied Governments",[293] which meant that Mr. Nix and the SCL Group and associated companies were working for the UK Government, alongside working on campaigning work for other countries. Mr. Nix also told us that Christian Kalin was working for the UK Government at the same time.[294] We published a Ministry of Defence approbation of SCL, after SCL provided psychological operations training for MOD staff, which revealed that SCL was given classified information about operations in Helmand, Afghanistan, as a result of their security clearances.[295] Alexander Nix explained that SCL "is a company that operates in the government and defence space, it acts as a company that has secret clearance".[296]

Conclusion

229. Alexander Nix appeared twice before the Committee, in February and in May 2018. His second appearance was after the Channel 4 undercover report had filmed him describing the work that SCL carried out in foreign campaigns: "These are just examples of what can be done […] and what has been done". When we asked about the report, Mr Nix told the Committee that he had sullied his own reputation, by "exaggeration and hyperbole", in order to win a client contract: "I alluded to services that we do not make and never made as a company. Yes, it was extremely foolish of me".[297] Given the evidence that we received through the course of this inquiry, it is hard to believe that Mr Nix's admissions on Channel 4 were as a result of 'exaggeration and hyperbole', rather than based on his direct experience of overseeing many elections abroad.

230. The work of SCL and its associates in foreign countries involved unethical and dangerous work, and we have heard worrying accounts of SCL employees being put in

290 Q1299
291 AggregateIQ (FKN0086)
292 Background papers submitted by Christopher Wylie, published 29 March 2018
293 Q819
294 Q3384
295 Background papers submitted by Christopher Wylie, published 29 March 2018
296 Q688
297 Q3378

grave danger. Paul Oliver Dehaye described the work that Dan Muresan, an employee of SCL, had to do, while employed by SCL: "He was working for Congress, according to reports from India, but he was really paid for by an Indian billionaire who wanted Congress to lose. He was pretending to work for one party but was really paid underhand by someone else".[298]

231. ***We received disturbing evidence, some of which we have published, some of which we have not, of activities undertaken by the SCL-linked companies in various political campaigns dating from around 2010, including the use of hacking, of disinformation, and of voter suppression, and the use of the services of Black Cube, an Israeli private intelligence service, whose work allegedly included illegal hacking. We also heard of the links between SCL and Christian Kalin of Henley and Partners and their involvement in election campaigns, in which Mr Kalin already ran or subsequently launched citizenship-by-investment programmes, involving the selling of countries passports to investors. SCL's alleged undermining of democracies in many countries, by the active manipulation of the facts and events, was happening alongside work done by the SCL Group on behalf of the UK Government, the US Government, and other allied governments. We do not have the remit or the capacity to investigate these claims ourselves, but we urge the Government to ensure that the National Crime Agency thoroughly investigates these allegations.***

298 Paul-Olivier Dehaye, Q1374

7 Digital literacy

232. Throughout the inquiry, we heard about the powerful influencing nature of social media and the fact that it is hard to differentiate between what is true, what is misleading, and what is false, especially when messages are targeted at an individual level. Children, young adults, and adults—all users of digital media—need to be equipped in general with sufficient digital literacy, to be able to understand content on the Internet, and to work out what is accurate or trustworthy, and what is not. Time and again, we heard people saying that "when the service is free, you are the product" and, as the product, individual users are continually being manipulated, without their even realising.

233. This chapter will explore how people, especially children and young adults, engage with social media, and what can be done to ensure that they understand the digital space, and can make informed choices about how they spend their time, how they identify sites that they can trust or are safe, how they appraise the content of what they read, and what information they share with others.

The need for digital literacy

Why people connect on social media

234. The point of social media is to interact with other people, and to share ideas. Dr Caroline Tagg, from the Open University, carried out research that showed that people use Facebook to maintain social relationships, and to many people Facebook was not seen as a news media site, but "a place where they carry out quite complex maintenance and management of their social relationships".[299]

235. Within those social relationships, people tend to connect and want to spend time with others who share their same views and interests, which is when the spread of misinformation can happen so quickly. Professor Lewandowsky, from the University of Bristol, told us about an Australian study on climate change:

> Only 8% of people were found to completely negate the idea that the climate is changing but those 8% thought that their opinion was shared by half the population and that was because they were all in this echo chamber and talked to each other and felt their opinions confirmed. I think that is a novel problem that is inherent to the technology. That people think, whatever they think, everybody else thinks the same way.[300]

236. This dependency and reliance on social media comes with worrying consequences, as Tristan Harris told us:

> There are many different issues emerging out of the attention economy. The externalities range from public health, addiction, culture, children's well-being, mental well-being, loneliness, sovereignty of identity and things like that to election democracy, truth, discernment of truth and a shared reality, anti-trust and power. There are multiple issues. There are even more,

299 Q191
300 Q197

> because when you control the minds of people, you control society. How people make sense of the world and how they make choices are what ID is, and that can affect every aspect of society.[301]

Content on social media

237. Most users do not understand how the content they read has got there, but accept it without question. A significant part of digital literacy is understanding how social media works, and how the content that each user reads has appeared, as a result of specific algorithms:

> If we are talking about news and media literacy curricula, that has to include teaching about how to evaluate an algorithm and how to understand how what you see on Amazon, Netflix or Facebook has been decided by an algorithm, how an algorithm gets developed, how it is created by a certain person and how their biases might shape that. That has to be part of the teaching that we give to people.[302]

238. What appears on individuals' newsfeeds is there either by an algorithm, based on their behaviour and profile, or it is targeted at their demographic by paid promotion. Indeed, it is common for publishers to pay for their content to be posted so that they can reach a wider audience, due to the fact that Facebook, for example, does not recognise or seek to categorise good journalism or news over other material.[303]

239. Once content is on social media, it is hard for people to disregard what they have just read. Professor Stephan Lewandowsky told us that there are hundreds of studies have shown that "if we try to correct people's beliefs based on what they have heard they may adjust their belief slightly but there is a lot of evidence to suggest that they continue to rely on that information nonetheless. […] The cognitive consequences of fake news are pervasive".[304]

Data on social media

240. When we share information about ourselves on social media, there is a tacit understanding that that information will become public. When Alexander Nix first gave evidence, in February 2018, he told us that people understand the reciprocity of businesses giving an offer in exchange of people's data through, for example, loyalty cards and that "their data is being taken in return to help that brand to drive its marketing. […] People are not naïve".[305] However, in the context of the data extraction by Aleksandr Kogan, Sandy Parakilas, a former Facebook manager, rightly said that Facebook users "may have understood in theory that there were privacy concerns but they did not know how much of their data was being sent to developers whom they had no relationship with".[306]

241. People also need to be aware of rights they have with regard to how their personal data is used, and what to do when they want their data to be removed. Social media

301 Q3150
302 Q581
303 Facebook creates Orwellian headache as news is labelled politics, Emily Bell, The Guardian, 24 June 2018
304 Q189
305 Q768
306 Q1197

companies do not make it easy for their users to control their own data. It is hard to find privacy controls, and there is no simple explanation of how users can look after their data and their privacy. Facebook's terms of its data and cookies policy had a large button for accepting Facebook's 'updated Terms to continue using Facebook'. If the user did not want to accept the Terms, they followed a small link 'see your options', which let them delete the account.

242. The Information Commissioner's Office is planning to work with the Electoral Commission, the Cabinet Office, and political parties to launch a "Your Data Matters" campaign, before the next General Election, with the aim "to increase transparency and build trust and confidence amongst the electorate on how their personal data is being used during political campaigns".[307] We hope that this campaign will be proactive in telling people about their own data, and how they should share it, and their rights over their data.

A unified approach to digital literacy

Young people

243. The Education Policy Initiative reports that 95% of 15-year-olds in the UK use social media before or after school, and that half of 9 to 16-year-olds use smart phones daily.[308] From an early age, young children are growing up with digital devices. Our education system should be equipping children with the necessary tools to live in our digital world, so that their mental health, emotional well-being and faculty for critical thinking are protected. They need to be aware of the issues surrounding social media, and be aware of their actions when interacting with digital arenas. Finding ways to involve parents and carers is equally important.[309]

School curriculum

244. Our schools play a crucial role in helping students to differentiate between fact and fiction, and there are various initiatives to tackle the growing issue of the use of social media by children and young adults. The PSHE Association recommended that the secondary school Personal, Social, Health and Economic (PSHE) curriculum should cover the issues that young people are concerned about online, including compulsive use, data gathering and body image.[310] *The Times* and *The Sunday Times* have recently launched a media literacy scheme in schools, to help pupils how to spot 'fake news'. The scheme will be available for pupils in secondary schools, colleges and sixth form. The programme is in partnership with News UK's News Academy.[311]

245. In a letter sent to social media companies in April 2018, the then Secretary of State for Health, Rt Hon Jeremy Hunt MP, warned those companies that they needed to ensure the protection of children's mental health from the dangers of social media, and discussed the possibility of introducing legislation for social media platforms, to curb the dangers

307 Democracy disrupted: Personal information and political influence, ICO, 11 July 2018
308 The Science and Technology Committee launched its current inquiry into the Impact of social media and screen-use on young people's health.
309 Same as above
310 Life Online planning resource, PSHE Association, 17 April 2018.
311 Times titles launch media literacy scheme in schools to help teach children how to spot 'fake news, Freddy Mayhew, Press Gazette, 28 June 2018.

of cyber-bullying of young adults.[312] California's Consumer Privacy Act of 2018 will establish special protections for children under the age of sixteen, including independent reviews, age ratings and other guidance to help children and their adults to navigate the world of social media.[313]

246. ***We recommend that the Government put forward proposals in its White Paper for an educational levy to be raised by social media companies, to finance a comprehensive educational framework (developed by charities and non-governmental organisations) and based online. Digital literacy should be the fourth pillar of education, alongside reading, writing and maths. The DCMS Department should co-ordinate with the Department for Education, in highlighting proposals to include digital literacy, as part of the Physical, Social, Health and Economic curriculum (PSHE). The social media educational levy should be used, in part, by the Government, to finance this additional part of the curriculum.***

247. ***There should be a unified public awareness initiative, supported by the Departments for DCMS, Health, and Education, with additional information and guidance from the Information Commissioner's Office and the Electoral Commission, and funded in part by the tech company levy. Such an initiative would set the context of social media content, explain to people what their rights over their data are, within the context of current legislation, and set out ways in which people can interact with political campaigning on social media. This initiative should be a rolling programme, and not one that occurs only before general elections or referenda.***

248. **The public should be made more aware of their ability to report digital campaigning that they think is misleading, or unlawful. We look forward to the work that the Electoral Commission is planning, to bring this to the fore.**

312 Jeremy Hunt threatens social media with new child-protection laws, BBC, 22 April 2018.
313 California legislative information

Conclusions and recommendations

Introduction and background

1. *The term 'fake news' is bandied around with no clear idea of what it means, or agreed definition. The term has taken on a variety of meanings, including a description of any statement that is not liked or agreed with by the reader. We recommend that the Government rejects the term 'fake news', and instead puts forward an agreed definition of the words 'misinformation' and 'disinformation'. With such a shared definition, and clear guidelines for companies, organisations, and the Government to follow, there will be a shared consistency of meaning across the platforms, which can be used as the basis of regulation and enforcement.* (Paragraph 14)

2. *We recommend that the Government uses the rules given to Ofcom under the Communications Act 2003 to set and enforce content standards for television and radio broadcasters, including rules relating to accuracy and impartiality, as a basis for setting standards for online content. We look forward to hearing Ofcom's plans for greater regulation of social media this autumn. We plan to comment on these in our further Report.* (Paragraph 15)

3. *The Government should support research into the methods by which misinformation and disinformation are created and spread across the internet: a core part of this is fact-checking. We recommend that the Government initiate a working group of experts to create a credible annotation of standards, so that people can see, at a glance, the level of verification of a site. This would help people to decide on the level of importance that they put on those sites.* (Paragraph 18)

4. *During the course of this inquiry we have wrestled with complex, global issues, which cannot easily be tackled by blunt, reactive and outmoded legislative instruments. In this Report, we suggest principle-based recommendations which are sufficiently adaptive to deal with fast-moving technological developments. We look forward to hearing the Government's response to these recommendations.* (Paragraph 19)

5. We also welcome submissions to the Committee from readers of this interim Report, based on these recommendations, and on specific areas where the recommendations can incorporate work already undertaken by others. This inquiry has grown through collaboration with other countries, organisations, parliamentarians, and individuals, in this country and abroad, and we want this co-operation to continue. (Paragraph 20)

The definition, role and legal responsibilities of tech companies

6. *The Data Protection Act 2018 gives greater protection to people's data than did its predecessor, the 1998 Data Protection Act, and follows the law set out in the GDPR. However, when the UK leaves the EU, social media companies will be able to process personal data of people in the UK from bases in the US, without any coverage of data protection law. We urge the Government to clarify this loophole in a White Paper this Autumn.* (Paragraph 30)

7. *We welcome the increased powers that the Information Commissioner has been given as a result of the Data Protection Act 2018, and the ability to be able to look behind the curtain of tech companies, and to examine the data for themselves. However, to be a sheriff in the wild west of the internet, which is how the Information Commissioner has described her office, the ICO needs to have the same if not more technical expert knowledge as those organisations under scrutiny. The ICO needs to attract and employ more technically-skilled engineers who not only can analyse current technologies, but have the capacity to predict future technologies. We acknowledge the fact that the Government has given the ICO pay flexibility to retain and recruit more expert staff, but it is uncertain whether pay flexibility will be enough to retain and attract the expertise that the ICO needs. We recommend that the White Paper explores the possibility of major investment in the ICO and the way in which that money should be raised. One possible route could be a levy on tech companies operating in the UK, to help pay for the expanded work of the ICO, in a similar vein to the way in which the banking sector pays for the upkeep of the Financial Conduct Authority.* (Paragraph 36)

8. *The globalised nature of social media creates challenges for regulators. In evidence Facebook did not accept their responsibilities to identify or prevent illegal election campaign activity from overseas jurisdictions. In the context of outside interference in elections, this position is unsustainable and Facebook, and other platforms, must begin to take responsibility for the way in which their platforms are used.* (Paragraph 44)

9. *Electoral law in this country is not fit for purpose for the digital age, and needs to be amended to reflect new technologies. We support the Electoral Commission's suggestion that all electronic campaigning should have easily accessible digital imprint requirements, including information on the publishing organisation and who is legally responsible for the spending, so that it is obvious at a glance who has sponsored that campaigning material, thereby bringing all online advertisements and messages into line with physically published leaflets, circulars and advertisements. We note that a similar recommendation was made by the Committee on Standards in Public Life, and urge the Government to study the practicalities of giving the Electoral Commission this power in its White Paper.* (Paragraph 45)

10. *As well as having digital imprints, the Government should consider the feasibility of clear, persistent banners on all paid-for political adverts and videos, indicating the source and making it easy for users to identify what is in the adverts, and who the advertiser is.* (Paragraph 46)

11. *The Electoral Commission's current maximum fine limit of £20,000 should be changed to a larger fine based on a fixed percentage of turnover, such as has been granted recently to the Information Commissioner's Office in the Data Protection Act 2018. Furthermore, the Electoral Commission should have the ability to refer matters to the Crown Prosecution Service, before their investigations have been completed.* (Paragraph 47)

12. *Electoral law needs to be updated to reflect changes in campaigning techniques, and the move from physical leaflets and billboards to online, micro-targeted political campaigning, as well as the many digital subcategories covered by paid and organic campaigning. The Government must carry out a comprehensive review of the current rules and regulations surrounding political work during elections and referenda,*

including: increasing the length of the regulated period; definitions of what constitutes political campaigning; absolute transparency of online political campaigning; a category introduced for digital spending on campaigns; reducing the time for spending returns to be sent to the Electoral Commission (the current time for large political organisations is six months); and increasing the fine for not complying with the electoral law. (Paragraph 48)

13. *The Government should consider giving the Electoral Commission the power to compel organisations that it does not specifically regulate, including tech companies and individuals, to provide information relevant to their inquiries, subject to due process.* (Paragraph 49)

14. *The Electoral Commission should also establish a code for advertising through social media during election periods, giving consideration to whether such activity should be restricted during the regulated period, to political organisations or campaigns that have registered with the Commission. Both the Electoral Commission and the ICO should consider the ethics of Facebook or other relevant social media companies selling lookalike political audiences to advertisers during the regulated period, where they are using the data they hold on their customers to guess whether their political interests are similar to those profiles held in target audiences already collected by a political campaign. In particular, we would ask them to consider whether users of Facebook or other relevant social media companies should have the right to opt out from being included in such lookalike audiences.* (Paragraph 50)

15. Within social media, there is little or no regulation. Hugely important and influential subjects that affect us—political opinions, mental health, advertising, data privacy—are being raised, directly or indirectly, in these tech spaces. People's behaviour is being modified and changed as a result of social media companies. There is currently no sign of this stopping. (Paragraph 56)

16. Social media companies cannot hide behind the claim of being merely a 'platform', claiming that they are tech companies and have no role themselves in regulating the content of their sites. That is not the case; they continually change what is and is not seen on their sites, based on algorithms and human intervention. However, they are also significantly different from the traditional model of a 'publisher', which commissions, pays for, edits and takes responsibility for the content it disseminates. (Paragraph 57)

17. *We recommend that a new category of tech company is formulated, which tightens tech companies' liabilities, and which is not necessarily either a 'platform' or a 'publisher'. We anticipate that the Government will put forward these proposals in its White Paper later this year and hope that sufficient time will be built in for our Committee to comment on new policies and possible legislation.* (Paragraph 58)

18. *We support the launch of the Government's Cairncross Review, which has been charged with studying the role of the digital advertising supply chain, and whether its model incentivises the proliferation of inaccurate or misleading news. We propose that this Report is taken into account as a submission to the Cairncross Review. We recommend that the possibility of the Advertising Standards Agency regulating digital*

advertising be considered as part of the Review. We ourselves plan to take evidence on this question this autumn, from the ASA themselves, and as part of wider discussions with DCMS and Ofcom. (Paragraph 59)

19. *It is our recommendation that this process should establish clear legal liability for the tech companies to act against harmful and illegal content on their platforms. This should include both content that has been referred to them for takedown by their users, and other content that should have been easy for the tech companies to identify for themselves. In these cases, failure to act on behalf of the tech companies could leave them open to legal proceedings launched either by a public regulator, and/or by individuals or organisations who have suffered as a result of this content being freely disseminated on a social media platform.* (Paragraph 60)

20. Tech companies are not passive platforms on which users input content; they reward what is most engaging, because engagement is part of their business model and their growth strategy. They have profited greatly by using this model. This manipulation of the sites by tech companies must be made more transparent. Facebook has all of the information. Those outside of the company have none of it, unless Facebook chooses to release it. Facebook was reluctant to share information with the Committee, which does not bode well for future transparency *We ask, once more, for Mr Zuckerberg to come to the Committee to answer the many outstanding questions to which Facebook has not responded adequately, to date.* (Paragraph 64)

21. *Facebook and other social media companies should not be in a position of 'marking their own homework'. As part of its White Paper this Autumn, the Government need to carry out proactive work to find practical solutions to issues surrounding transparency that will work for both users, the Government, and the tech companies.* (Paragraph 65)

22. *Facebook and other social media companies have a duty to publish and to follow transparent rules. The Defamation Act 2013 contains provisions stating that, if a user is defamed on social media, and the offending individual cannot be identified, the liability rests with the platform. We urge the Government to examine the effectiveness of these provisions, and to monitor tech companies to ensure they are complying with court orders in the UK and to provide details of the source of disputed content—including advertisements—to ensure that they are operating in accordance with the law, or any future industry Codes of Ethics or Conduct. Tech companies also have a responsibility to ensure full disclosure of the source of any political advertising they carry.* (Paragraph 66)

23. *Just as the finances of companies are audited and scrutinised, the same type of auditing and scrutinising should be carried out on the non-financial aspects of technology companies, including their security mechanisms and algorithms, to ensure they are operating responsibly. The Government should provide the appropriate body with the power to audit these companies, including algorithmic auditing, and we reiterate the point that the ICO's powers should be substantially strengthened in these respects.* (Paragraph 72)

24. *If companies like Facebook and Twitter fail to act against fake accounts, and properly account for the estimated total of fake accounts on their sites at any one time, this*

could not only damage the user experience, but potentially defraud advertisers who could be buying target audiences on the basis that the user profiles are connected to real people. We ask the Competition and Markets Authority to consider conducting an audit of the operation of the advertising market on social media. (Paragraph 73)

25. *Social media companies have a legal duty to inform users of their privacy rights. Companies give users the illusion of users having freedom over how they control their data, but they make it extremely difficult, in practice, for users to protect their data. Complicated and lengthy terms and conditions, small buttons to protect our data and large buttons to share our data mean that, although in principle we have the ability to practise our rights over our data—through for example the GDPR and the Data Protection Act—in practice it is made hard for us.* (Paragraph 75)

26. *The UK Government should consider establishing a digital Atlantic Charter as a new mechanism to reassure users that their digital rights are guaranteed. This innovation would demonstrate the UK's commitment to protecting and supporting users, and establish a formal basis for collaboration with the US on this issue. The Charter would be voluntary, but would be underpinned by a framework setting out clearly the respective legal obligations in signatory countries. This would help ensure alignment, if not in law, then in what users can expect in terms of liability and protections.* (Paragraph 76)

27. The United Nations has named Facebook as being responsible for inciting hatred against the Rohingya Muslim minority in Burma, through its 'Free Basics' service. It provides people free mobile phone access without data charges, but is also responsible for the spread disinformation and propaganda. The CTO of Facebook, Mike Schroepfer described the situation in Burma as "awful", yet Facebook cannot show us that it has done anything to stop the spread of disinformation against the Rohingya minority. (Paragraph 82)

28. *The hate speech against the Rohingya—built up on Facebook, much of which is disseminated through fake accounts—and subsequent ethnic cleansing, has potentially resulted in the success of DFID's aid programmes being greatly reduced, based on the qualifications they set for success. The activity of Facebook undermines international aid to Burma, including the UK Government's work. Facebook is releasing a product that is dangerous to consumers and deeply unethical. We urge the Government to demonstrate how seriously it takes Facebook's apparent collusion in spreading disinformation in Burma, at the earliest opportunity. This is a further example of Facebook failing to take responsibility for the misuse of its platform.* (Paragraph 83)

29. *A professional global Code of Ethics should be developed by tech companies, in collaboration with this and other governments, academics, and interested parties, including the World Summit on Information Society, to set down in writing what is and what is not acceptable by users on social media, with possible liabilities for companies and for individuals working for those companies, including those technical engineers involved in creating the software for the companies. New products should be tested to ensure that products are fit-for-purpose and do not constitute dangers to the users, or to society.* (Paragraph 89)

30. *The Code of Ethics should be the backbone of tech companies' work, and should be continually referred to when developing new technologies and algorithms. If companies fail to adhere to their own Code of Ethics, the UK Government should introduce regulation to make such ethical rules compulsory.* (Paragraph 90)

31. *The dominance of a handful of powerful tech companies, such as Facebook, Twitter and Google, has resulted in their behaving as if they were monopolies in their specific area. While this portrayal of tech companies does not appreciate the benefits of a shared service, where people can communicate freely, there are considerations around the data on which those services are based, and how these companies are using the vast amount of data they hold on users. In its White Paper, the Government must set out why the issue of monopolies is different in the tech world, and the measures needed to protect users' data.* (Paragraph 91)

The issue of data targeting, based around the Facebook, GSR and Cambridge Analytica allegations

32. Over the past month, Facebook has been investing in adverts globally, proclaiming the fact that "Fake accounts are not our friends." Yet the serious failings in the company's operations that resulted in data manipulation, resulting in misinformation and disinformation, have occurred again. Over four months after Facebook suspended Cambridge Analytica for its alleged data harvesting, Facebook suspended another company, Crimson Hexagon—which has direct contracts with the US government and Kremlin-connected Russian organisations—for allegedly carrying out the same offence. (Paragraph 133)

33. *We are concerned about the administrators' proposals in connection with SCL Elections Ltd, as listed in Companies House, and the fact that Emerdata Ltd is listed as the ultimate parent company of SCL Elections Ltd, and is the major creditor and owed over £6.3 million. The proposals also describe laptops from the SCL Elections Ltd offices being stolen, and laptops returned by the ICO, following its investigations, also being stolen. We recommend that the National Crime Agency, if it is not already, should investigate the connections between the company SCL Elections Ltd and Emerdata Ltd.* (Paragraph 134)

34. The allegations of data harvesting revealed the extent of data misuse, made possible by Cambridge University's Dr Kogan and facilitated by Facebook, GSR, and manipulated into micro-targeting Cambridge Analytica and its associated companies, through AIQ. The SCL Group and associated companies have gone into administration, but other companies are carrying out very similar work. Many of the individuals involved in SCL and Cambridge Analytica appear to have moved on to new corporate vehicles. Cambridge Analytica is currently being investigated by the Information Commissioner's Office (ICO) (and, as a leading academic institution, Cambridge University also has questions to answer from this affair about the activities of Dr Kogan). (Paragraph 135)

35. We invited Alexander Nix twice to give evidence; both times he was evasive in his answers and the standard of his answers fell well below those expected from a CEO of an organisation. His initial evidence concerning GSR was not the whole truth. There is a public interest in getting to the heart of what happened, and Alexander

Nix must take responsibility for failing to provide the full picture of events, for whatever reason. With respect to GSR, he misled us. We will give a final verdict on Mr Nix's evidence when we complete the inquiry. (Paragraph 136)

Political campaigning

36. *We recommend that the Government look at ways in which the UK law defines digital campaigning. This should include online adverts that use political terminology that are not sponsored by a specific political party. There should be a public register for political advertising, requiring all political advertising work to be listed for public display so that, even if work is not requiring regulation, it is accountable, clear, and transparent for all to see. There should be a ban on micro-targeted political advertising to lookalikes online, and a minimum limit for the number of voters sent individual political messages should be agreed, at a national level.* (Paragraph 142)

37. *We reiterate our support for the Cairncross Review and will engage with the consultation in the coming months. In particular, we hope that Frances Cairncross will give due weight to the role of digital advertising in elections, and will make concrete recommendations about how clearer rules can be introduced to ensure fairness and transparency.* (Paragraph 143)

38. *The Government should investigate ways in which to enforce transparency requirements on tech companies, to ensure that paid-for political advertising data on social media platforms, particularly in relation to political adverts, are publicly accessible, are clear and easily searchable, and identify the source, explaining who uploaded it, who sponsored it, and its country of origin. This information should be imprinted into the content, or included in a banner at the top of the content. Such transparency would also enable members of the public to understand the behaviour and intent of the content providers, and it would also enable interested academics and organisations to conduct analyses and to highlight trends.* (Paragraph 144)

39. *Tech companies must also address the issue of shell corporations and other professional attempts to hide identity in advert purchasing, especially around election advertising. There should be full disclosure of targeting used as part of advert transparency. The Government should explore ways of regulating on the use of external targeting on social media platforms, such as Facebook's Custom Audiences. We expect to see the detail of how this will be achieved in its White Paper later this year.* (Paragraph 145)

40. Data sets allegedly enabled Leave.EU to push their message to groups of people that they might not otherwise have had information about. This evidence informed our inquiry, backing up concerns that data is being harvested and utilised from many people unwittingly and used for purposes of which they may not be aware. It is alleged that Leave.EU obtained data used during the Referendum from insurance data from companies owned by Arron Banks. The Information Commissioner's Office is investigating both the alleged misuse of customer data from Arron Banks' Eldon Insurance Services Ltd and the misuse of that data by the call centre staff, to make calls on behalf of Leave.EU. These are extremely serious allegations. We look forward to hearing the final results of the ICO's investigations, when it reports in October 2018. (Paragraph 159)

Russian influence in political campaigns

41. *In November 2017, the Prime Minister accused Russia of meddling in elections and planting 'fake news' in an attempt to 'weaponise information' and sow discord in the West. It is clear from comments made by the then Secretary of State in evidence to us that he shares her concerns. However, there is a disconnect between the Government's expressed concerns about foreign interference in elections, and tech companies intractability in recognising the issue. We would anticipate that this issue will be addressed, with possible plans of action, in the White Paper this Autumn.* (Paragraph 176)

42. *Arron Banks is, reportedly, the largest individual donor in UK political history. As far as we understand, he met with the Russian Ambassador, for the first time, in the run up to the EU Referendum. Evidence discloses that he discussed business ventures within Russia and beyond, and other financial ventures, in a series of meetings with Russian Embassy staff. Arron Banks and Andy Wigmore have misled the Committee on the number of meetings that took place with the Russian Embassy and walked out of the Committee's evidence session to avoid scrutiny of the content of the discussions with the Russian Embassy.* (Paragraph 185)

43. *From the emails that we have seen, it is evident that Arron Banks had many meetings with Russian officials, including the Russian Ambassador, Alexander Yakovenko, between 2015 and 2017. The meetings involved discussions about business deals involving Alrosa, the Russian diamond monopoly, the purchase of gold mines, funded by Sberbank, the Russian-state bank, and the transferring of confidential documents to Russian officials. Mr. Banks seemed to want to hide the extent of his contacts with Russia, while his spokesman Andy Wigmore's statements have been unreliable—by his own admission—and cannot be taken at face value. Mr Wigmore is a self-confessed liar and, as a result, little significance can be attached to anything that he says. It is unclear whether Mr. Banks profited from business deals arising from meetings arranged by Russian officials. We understand that the National Crime Agency (NCA) is investigating these matters. We believe that they should be given full access to any relevant information that will aid their inquiry.* (Paragraph 186)

44. *Arron Banks is believed to have donated £8.4 million to the Leave campaign, the largest political donation in British politics, but it is unclear from where he obtained that amount of money. He failed to satisfy us that his own donations had, in fact, come from sources within the UK. At the same time, we have evidence of Mr. Banks' discussions with Russian Embassy contacts, including the Russian Ambassador, over potential gold and diamond deals, and the passing of confidential information by Mr Banks. The Electoral Commission should pursue investigations into donations that Arron Banks made to the Leave campaign, to verify that the money was not sourced from abroad. Should there be any doubt, the matter should be referred to the NCA. The Electoral Commission should come forward with proposals for more stringent requirements for major donors to demonstrate the source of their donations.* (Paragraph 191)

45. *The Electoral Commission has recommended that there should be a change in the rules covering political spending, so that limits are put on the amount of money an individual can donate. We agree with this recommendation, and urge the Government to take this proposal on board.* (Paragraph 192)

46. *We heard evidence that showed alleged Russian interference in the Spanish Referendum, in October 2017. During the Referendum campaign, Russia provoked conflict, through a mixture of misleading information and disinformation, between people within Spain, and between Spain and other member states in the EU, and in NATO. We heard evidence that showed that Russia had a special interest in discrediting the Spanish democratic system, through Russian state affiliated TV organisations spreading propaganda that benefitted those wanting independence in Catalonia.* (Paragraph 197)

47. *We recommend that the UK Government approaches other governments and follows the recommendation agreed by US and EU representatives, including representatives from this Committee, at the recent inter-parliamentary meeting at the Atlantic Council. The Government should share information on risks, vulnerabilities, and best practices to counter Russian interference, and co-ordinate between parliamentarians across the world. Only by sharing information, resources, and best practice will this Government be able to combat Russian interference in our elections. We look forward to a White Paper this autumn, and the opportunity for the Government to set out the practical steps that it will follow to ensure greater global co-operation to combat Russian interference.* (Paragraph 202)

48. *Just as six Select Committees have joined forces in an attempt to combat Russian influence in our political discourse, so the Government should co-ordinate joint working with the different relevant Departments. Those Departments should not be working in silos, but should work together, sharing data, intelligence and expert knowledge, to counter the emerging threat of Russia, and other malign players.* (Paragraph 203)

49. *We note that the Mueller Inquiry into Russian interference in the United States is ongoing. It would be wrong for Robert Mueller's investigation to take the lead about related issues in the UK. We recommend that the Government makes a statement about how many investigations are currently being carried out into Russian interference in UK politics and ensures that a co-ordinated structure exists, involving the Electoral Commission and the Information Commissioner, as well as other relevant authorities.* (Paragraph 204)

SCL influence in foreign elections

50. *We received disturbing evidence, some of which we have published, some of which we have not, of activities undertaken by the SCL-linked companies in various political campaigns dating from around 2010, including the use of hacking, of disinformation, and of voter suppression, and the use of the services of Black Cube, an Israeli private intelligence service, whose work allegedly included illegal hacking. We also heard of the links between SCL and Christian Kalin of Henley Partners and their involvement in election campaigns, in which Mr Kalin already ran or subsequently launched citizenship-by-investment programmes, involving the selling of countries passports to investors. SCL's alleged undermining of democracies in many countries, by the active*

manipulation of the facts and events, was happening alongside work done by the SCL Group on behalf of the UK Government, the US Government, and other allied governments. We do not have the remit or the capacity to investigate these claims ourselves, but we urge the Government to ensure that the National Crime Agency thoroughly investigates these allegations. (Paragraph 231)

Digital literacy

51. *We recommend that the Government put forward proposals in its White Paper for an educational levy to be raised by social media companies, to finance a comprehensive educational framework (developed by charities and non-governmental organisations) and based online. Digital literacy should be the fourth pillar of education, alongside reading, writing and maths. The DCMS Department should co-ordinate with the Department for Education, in highlighting proposals to include digital literacy, as part of the Physical, Social, Health and Economic curriculum (PSHE). The social media educational levy should be used, in part, by the Government, to finance this additional part of the curriculum.* (Paragraph 246)

52. *There should be a unified public awareness initiative, supported by the Departments for DCMS, Health, and Education, with additional information and guidance from the Information Commissioner's Office and the Electoral Commission, and funded in part by the tech company levy. Such an initiative would set the context of social media content, explain to people what their rights over their data are, within the context of current legislation, and set out ways in which people can interact with political campaigning on social media. This initiative should be a rolling programme, and not one that occurs only before general elections or referenda.* (Paragraph 247)

53. The public should be made more aware of their ability to report digital campaigning that they think is misleading, or unlawful. We look forward to the work that the Electoral Commission is planning, to bring this to the fore. (Paragraph 248)

Annex

Recommendations from the July 16 Inter-Parliamentary Meeting at the Atlantic Council

- Foreign interference in elections is an attack on citizens' fundamental right to freely select their representatives and to determine the path forward for their countries.
- Democracies in the United States (US), Europe and elsewhere have experienced foreign interference in their elections through the spread of fake information, the amplification of divisive news, the leaking of sensitive information, the covert funding of candidates, and the targeting of voting systems.
- Governments, legislatures, social media companies, and civil society should raise public awareness of the challenge -- reaching out in a non-partisan fashion about the dangers of malicious foreign interference and ways to minimize the threat. Public resilience to malign foreign influence starts with clear communication. Further, governments should evaluate the appropriate role for government in educating the public about recognizing Russian and other propaganda.
- We urge the executive branches in the US, Canada, and European countries to develop whole-of government strategies to increase election security and combat electoral interference. Efforts in the US should focus on the mid-term and 2020 elections. This should involve a collaborative, end-to-end evaluation of the security of election systems including federal, state, and local officials and election vendors; the development of a strong, coherent deterrence strategy to prevent an adversary from considering interfering; punitive options should that interference occur; and contingency plans for ensuring resiliency and bolstering public confidence in elections.
- As legislators, we welcome non-partisan legislative initiatives to build resilience of electoral systems and to counter foreign interference and urge that they be debated and voted on.
- Governments and legislatures on both sides of the Atlantic should allocate funds to counter election interference and disinformation. This should include empowering civil society groups to monitor and report foreign and malicious interference in elections.
- We encourage technology companies to cooperate with governments and civil society organizations to develop tools and procedures to fight interference, dramatically increase transparency, promote accountability, reduce vulnerabilities on social media platforms, including in relation to online political advertising, and raise public awareness about ways messages and news can be manipulated.
- We support greater and sustained Transatlantic cooperation, including between national governments, NATO, and the European Union, to share information on risks, vulnerabilities, and best practices to counter interference. Coordination between parliamentarians and open, regular dialogue with social media, technology companies, and civil society can strengthen these efforts.
- If Kremlin interference in upcoming elections continues, governments on both sides of the Atlantic should impose heavy costs, including sanctions, preferably coordinated between the US and Europe.

Convened by the Atlantic Council and Transatlantic Commission on Election Integrity

Endorsed by:

Mr. Emilio Carelli
Member, Chamber of Deputies
Italian Parliament

Ms. Margareta Cederfelt
Member
Riksdag of the Kingdom of Sweden

Mr. Damian Collins
Member, House of Commons
Parliament of the United Kingdom

Ambassador Eileen Donahoe
Executive Director, Global Digital Policy Incubator,Stanford University;
Member
Transatlantic Commission on Election Integrity

Mr. Nathaniel Erskine-Smith
Member, House of Commons
Parliament of Canada

Ms. Anna Fotyga
Chair, Defense and Security Committee
European Parliament

Dr. Hanna Hopko
Member
Verkhovna Rada of Ukraine

Minister Natalie Jaresko
Former Minister of Finance
Government of Ukraine;
Member
Transatlantic Commission on Election Integrity

Ambassador Ojārs Ēriks Kalniņš
Member
Saeima of the Republic of Latvia

Mr. Jan Lipavsky
Member, House of Commons
Parliament of the Czech Republic

Mr. Ian Lucas
Member, House of Commons
Parliament of the United Kingdom

Dr. Hryhoriy Nemyria
Member
Verkhovna Rada of Ukraine

Minister Keit Pentus-Rosimannus
Member
Riigikogu of the Republic of Estonia

Mr. Bob Zimmer
Member, House of Commons
Parliament of Canada

The Hon. Marco Rubio
Senator from Florida
US Senate

The Hon. Mark Warner
Senator from the Commonwealth of Virginia
US Senate

Formal minutes

Tuesday 24 July 2018

Damian Collins, in the Chair

Julie Elliott	Ian Lucas
Paul Farrelly	Jo Stevens
Simon Hart	Giles Watling
Julian Knight	

Draft Report (*Disinformation and 'fake news': Interim Report*), proposed by the Chairman, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 248 read and agreed to.

Summary agreed to.

Annex agreed to.

Resolved, That the Report be the Fifth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

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

[Adjourned till Wednesday 5 September 2018 at 2.00 p.m.

Witnesses

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

Tuesday 19 Dec 2017

Samantha Bradshaw, Oxford Internet Institute, and **Professor Kalina Bontcheva**, Professor of Text Analysis, the University of Sheffield — Q1–51

David Alandete, Editor, El País, **Francisco de Borja Lasheras**, Director, Madrid Office, European Council on Foreign Relations, and **Mira Milosevich-Juaristi**, Senior Fellow for Russia and Euroasia at Elcano Royal Institute and Associate Professor, History of International Relations, Instituto de Empresa, Madrid — Q52–85

Tuesday 16 January 2018

Bethan Crockett, Senior Director, Brand Safety and Digital Risk, GroupM EMEA, **Eitan Jankelewitz**, Partner, Sheridans, and **Matt Rogerson**, Head of Public Policy, Guardian News and Media — Q86–159

Tim Elkington, Chief Digital Officer, Internet Advertising Bureau, **Phil Smith**, Managing Director, Incorporated Society of British Advertisers, and **Ben Williams**, Adblock Plus — Q160–188

Tuesday 23 January 2018

Professor Stephan Lewandowsky, University of Bristol; **Professor Vian Bakir**, Bangor University; and **Dr Caroline Tagg**, the Open University — Q189–237

Dr Charles Kriel, Corsham Institute; **Adam Hildreth**, CEO and Founder, Crisp; and **Matt Breen**, Commercial Director of Media Chain (part of the Social Chain Group) — Q238–272

Thursday 8 February 2018

Juniper Downs, Global Head of Public Policy, YouTube; and **Richard Gingras**, Vice President of News, Google — Q273–342

Monika Bickert, Head of Global Policy Management, Facebook; and **Simon Milner**, Policy Director UK, Middle East and Africa, Facebook — Q343–478

Carlos Monje, Director, Public Policy and Philanthropy, US and Canada, Twitter; and **Nick Pickles**, Head of Public Policy and Philanthropy, UK, Twitter — Q479–568

David Carroll, Associate Professor of Media Design, The New School; **Amy Mitchell**, Director of Journalism Research, Pew Research Centre; **Frank Sesno**, Director, School of Media and Public Affairs, George Washington University; and **Claire Wardle**, Research Fellow, Shorenstein Centre on Media, Politics and Public Policy — Q569–600

David Chavern, President and CEO, News Media Alliance; **Major Garrett**, Chief White House Correspondent, CBS News; **Tony Maddox**, Executive VP and MD, CNN International; and **Kinsey Wilson**, Special Advisor to the President/CEO of the New York Times Q601–620

Tuesday 27 February 2018

Alexander Nix, Chief Executive, Cambridge Analytica Q621–848

Tuesday 6 March 2018

Bill Browder, founder and CEO, Hermitage Capital Management, and **Edward Lucas**, Senior Vice President, the Center for European Policy Analysis (CEPA) Q849–894

Elizabeth Denham, Commissioner, Information Commissioner's Office (ICO) Q895–942

Wednesday 14 March 2018

Rt Hon Matt Hancock, Secretary of State for Digital, Culture, Media and Sport Q943–1186

Wednesday 21 March 2018

Sandy Parakilas, former Facebook operations manager Q1187–1270

Tuesday 27 March 2018

Paul-Olivier Dehaye and **Christopher Wylie** Q1270–1461

Tuesday 17 April 2018

Brittany Kaiser, former Director of Program Development, Cambridge Analytica Q1462–1769

Tuesday 24 Apr 2018

Dr Aleksandr Kogan, Senior Research Associate, Department of Psychology, Cambridge University Q1769–2086

Thursday 26 April 2018

Mike Schroepfer, Chief Technical Officer, Facebook Q2087–2500

Wednesday 2 May 2018

Chris Vickery, Director, Cyber Risk Research, UpGuard — Q2501–2616

Tuesday 15 May 2018

Claire Bassett, Chief Executive, Electoral Commission, **Louise Edwards**, Head of Regulations, Electoral Commission, and **Bob Posner**, Director of Political Finance and Regulation and Legal Counsel, Electoral Commission — Q2617–2760

Wednesday 16 May 2018

Jeff Silvester, Chief Operating Officer, AggregateIQ — Q2761–3145

Tuesday 22 May 2018

Tristan Harris, Co-founder and Executive Director, Center for Humane Technology — Q3146–3190

Wednesday 6 June 2018

Alexander Nix, former CEO, Cambridge Analytica — Q3191–3480

Tuesday 12 June 2018

Arron Banks, co-founder of Leave.EU, and **Andy Wigmore,** Director of Communications, Leave.EU — Q3481–3780

Published written evidence

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

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

Fake News (Former inquiry)

Written evidence received and published in April 2017 before inquiry was relaunched after election:

1 Bangor University, Network for Media & Persuasive Communication (FNW0054)

2 BBC (FNW0114)

3 Ben Nimmo (FNW0125)

4 Bob Goodall (FNW0078)

5 British Law Education and Technology Association (FNW0074)

6 Campaign for Responsible Financial Journalism (FNW0080)

7 Centre for the Study of Media, Communication and Power at King's College London (FNW0089)

8 Committee on Standards in Public Life (FNW0049)

9 Darren Parmenter (FNW0016)

10 Dr Alexander Douglas and Professor Katherine Hawley (FNW0072)

11 Dr Ansgar Koene (FNW0116)

12 Dr David Manning (FNW0064)

13 Dr David Miller and others (FNW0094)

14 Dr Dominic Thorrington (FNW0010)

15 Dr Karol Lasok (FNW0021)

16 Dr Lucas Black (FNW0031)

17 Dr Michael Holland (FNW0104)

18 Dr Sandra Leaton Gray and Professor Andy Phippen (FNW0029)

19 Dr David Coast, Prof. Jo Fox, Prof. David Welch (FNW0085)

20 Edmund Wisty (FNW0056)

21 Electoral Commission (FNW0048)

22 Facebook (FNW0121)

23 Full Fact (FNW0097)

24 Google (FNW0123)

25 Guardian News & Media (FNW0096)

26 Himsworths Legal Limited (FNW0046)

27 Home Marketing Limited (FNW0059)

28 IMPRESS (FNW0112)

29 InformAll and the CILIP Information Literacy Group (FNW0079)

30 Internet Advertising Bureau UK (FNW0081)

31 Internews (FNW0034)

32 Isabel Pakowski (FNW0076)

33 ITN (FNW0118)

34 ITV (FNW0115)

35 JAG Shaw Baker (FNW0090)

36 Kohei Watanabe (FNW0030)

37 Linda Greenwood (FNW0014)

38 Master Josh Traynor (FNW0068)

39 Members of the Centre for Politics & Media Research, Faculty for Media & Communication, Bournemouth University (FNW0083)

40 Michael Leidig (FNW0052)

41 Mr Gianfranco Polizzi (FNW0071)

42 Mr Jacob Rowbottom (FNW0070)

43 Mr Jane Winter (FNW0045)

44 Mr Mark Leiser (FNW0035)

45 Mr Vernon Moat (FNW0012)

46 Mr Xander Ward (FNW0037)

47 Ms Gemma MacNaught (FNW0102)

48 Muslim Council of Britain (FNW0120)

49 National Union of Journalists (FNW0053)

50 New Political Communication Unit - Royal Holloway, University of London (FNW0066)

51 Newgate Communications (FNW0073)

52 News Media Alliance (FNW0098)

53 News Media Association (FNW0087)

54 Ofcom (FNW0107)

55 politicaladvertising.co.uk (FNW0088)

56 Press Association (FNW0042)

57 Professor Brian Cathcart (FNW0050)

58 Professor Jim Ridgway (FNW0067)

59 Professor Julian Petley (FNW0099)

60 Professor Leighton Andrews (FNW0061)

61 Professor Stephan Lewandowsky, Professor James Ladyman, and Professor Jason Reifler (FNW0065)

62 Public Relations and Communications Association (FNW0077)

63 Research Libraries UK (FNW0062)

64 Simple Politics (FNW0024)

65 Society of Editors (FNW0060)
66 Stephen Saunders (FNW0013)
67 Stop Funding Hate (FNW0091)
68 The Open University (FNW0092)
69 The Royal Statistical Society (FNW0084)
70 The Rt. Hon. the Lord David Blencathra (FNW0063)
71 Tobacco Control Research Group (FNW0075)
72 Transparify (FNW0040)
73 UCL Knowledge Lab (FNW0110)
74 University of Bristol (FNW0095)
75 University of Portsmouth, Alison Wakefield (FNW0103)
76 University of South Wales (FNW0086)
77 Voice of the Listener & Viewer (FNW0122)
78 WebRoots Democracy (FNW0124)
79 Wikimedia UK (FNW0058)

Fake News (Current inquiry)

Written evidence received in the relaunched inquiry:

1 Adblock Plus (FKN0046)
2 Age of Autism (FKN0010)
3 Age of Autism supplementary (FKN0027)
4 AggregateIQ (FKN0086)
5 Alexander Nix supplementary (FKN0072)
6 Amy Mitchell, Pew Research Centre (FKN0041)
7 Arron Banks (FKN0056)
8 Arron Banks supplementary (FKN0059)
9 Arron Banks further supplementary (FKN0080)
10 Association for Citizenship Teaching (FKN0012)
11 Avaaz (FKN0073)
12 Bangor University (FKN0003)
13 Borden Ladner Gervais LLP (FKN0089)
14 Brian Deer (FKN0019)
15 Brittany Kaiser (FKN0076)
16 Cambridge Analytica (FKN0045)
17 Chris Wylie supplementary (FKN0079)
18 Corsham Institute (FKN0007)
19 David Brear (FKN0065)
20 David Chavern, President and CEO, News Media Alliance (FKN0039)

21 Disinformation Index (FKN0058)
22 Dr Aleksandr Kogan (FKN0077)
23 Dr Claire Wardle, Shorenstein Centre on Media, Politics and Public Policy (FKN0040)
24 Dr Emma Briant (FKN0071)
25 Dr Emma Briant, Senior Lecturer at University of Essex (FKN0092)
26 Dr Mils Hills (FKN0014)
27 Dr Paul Reilly (FKN0084)
28 Dr Sander van der Linden, et al (FKN0049)
29 Edmund Wisty (FKN0008)
30 Edward Lucas (FKN0052)
31 Electoral Commission (FKN0031)
32 Elizabeth Denham, Information Commissioner (FKN0051)
33 Elizabeth Denham, Information Commissioner supplementary (FKN0057)
34 Erin Anzelmo (FKN0074)
35 Facebook (FKN0048)
36 Facebook - Mike Schroepfer (FKN0082)
37 Facebook - Rebecca Stimson (FKN0095)
38 Facebook supplementary (FKN0078)
39 Factmata Limited, UK (FKN0035)
40 Google Supplementary (FKN0038)
41 Helena Kennedy Centre for International Justice (FKN0005)
42 Helena Kennedy Centre for International Justice (FKN0090)
43 HonestReporting (FKN0047)
44 Incorporated Society of British Advertisers (ISBA) supplementary (FKN0036)
45 Independent Press Standards Organisation (FKN0004)
46 Internet Advertising Bureau UK Supplementary (FKN0043)
47 IPA (FKN0093)
48 Isabella Weatherley (FKN0002)
49 Kalina Bontcheva supplementary (FKN0054)
50 M C McGrath (FKN0067)
51 Major Garrett, Chief Whitehouse Correspondent, CBS News (FKN0042)
52 MoneySavingExpert.com (FKN0068)
53 Mr Alistair McHugh (FKN0020)
54 Mr C Miller (FKN0009)
55 Mr Dominic Penna (FKN0021)
56 Mr Kevin Cahill (FKN0062)
57 Mr Kevin Cahill supplementary (FKN0063)
58 Mr Richard Ebley (FKN0015)

59 Mr Samuel Townsend (FKN0018)

60 Ms Susie Alegre (FKN0081)

61 Muslim Engagement and Development (MEND) (FKN0011)

62 National Literacy Trust (FKN0037)

63 Paul-Olivier Dehaye (FKN0055)

64 Professor Dr G. Keith Still (FKN0070)

65 Professor Leighton Andrews (FKN0006)

66 Professor Neville Morley (FKN0091)

67 Pupils 2 Parliament (FKN0025)

68 Ruchi Hajela (FKN0066)

69 Second Draft (FKN0050)

70 Stuart Mercer (FKN0016)

71 The Open University (FKN0026)

72 The Open University supplementary (FKN0044)

73 The Stonehenge Alliance (FKN0053)

74 University of Westminster - Communication and Media Research Institute & Westminster Institute for Advanced Studies (FKN0013)

75 W Morris (FKN0085)

Correspondence

Letter from Rebecca Stimson, Facebook, to the Chair 8 June 2018

Letter from the Chair to Rebecca Stimson, Facebook, 21 May 2018

Letter from Rebecca Stimson, Facebook, to the Chair, 14 May 2018

Annex to letter from Rebecca Stimson, Facebook, to the Chair, 14 May 2018: Letter from Gareth Lambe

Letter from the Chair to Rebecca Stimson, Facebook, 1 May 2018

Letter from the Chair to Alexander Nix, 28 March 2018

Letter from the Chair to Rebecca Stimson, Facebook, 28 March 2018

Letter from Rebecca Stimson, Facebook, to the Chair, 26 March 2018

Letter from the Chair to Alexander Nix, 22 March 2018

Letter from the Chair to Mark Zuckerberg, Facebook, 20 March 2018

Letter from Simon Milner, Facebook, to the Chair, 28 February 2018

Letter from the Chair to Jack Dorsey, Twitter, 25 January 2018

Letter from Nick Pickles, Twitter, to the Chair, 19 January 2018

Letter from Simon Milner, Facebook, to the Chair, 17 January 2018

Letter from the Chair to Jack Dorsey, Twitter, 14 December 2017

Letter from Nick Pickles, Twitter, to the Chair, 13 December 2017

Letter from Nick Pickles, Twitter, to the Chair, 24 November 2017

Letter from Simon Milner, Facebook, to Chair, 21 November 2017

Letter from the Chair to Jack Dorsey, Twitter, re Russian-linked accounts, 3 November 2017

Letter from the Chair to Mark Zuckerberg, Facebook, re Russian-linked accounts, 19 October 2017

Letter from the Chair to Dara Nasr, Twitter, 19 October 2017

Background papers

Background paper – Arron Banks, Andy Wigmore

Alexander Nix evidence – SCL & Cambridge Analytica Corporate Structure Development

Dr Emma Briant – Audio file links & transcripts, 4 June 2018

Chris Vickery - data flow illustration, 2 May 2018

Dr Aleksandr Kogan - PowerPoint slides, 24 April 2018

Brittany Kaiser – submitted emails

Brittany Kaiser – written statement

Brittany Kaiser – Background paper – Cambridge Analytica: Leave.EU: Psychographic Targeting for Britain

Britany Kaiser – Legal opinion on Cambridge Analytica and UKIP

Dr Emma Briant – Audio file links & transcripts

Dr Emma Briant – Explanatory essays giving context and analysis to submitted evidence

Matrix Chambers legal opinion: Referendum expenses 2016

Background papers submitted by Christopher Wylie

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website. The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2017–19

First Report	Appointment of the Chair of Ofcom	HC 508
Second Report	The potential impact of Brexit on the creative industries, tourism and the digital single market	HC 365 (HC 1141)
Third Report	Appointment of the Chair of the Charity Commission	HC 509 (HC 908)
Fourth Report	Combatting doping in sport	HC 366 (HC 1050)
First Special Report	Appointment of the Chair of the Charity Commission: Government Response to the Committee's Third Report of Session 2017–19	HC 908
Second Special Report	Combatting doping in sport: Government Response to the Committee's Fourth Report of Session 2017–19	HC 1050
Third Special Report	Failure of a witness to answer an Order of the Committee: conduct of Mr Dominic Cummings	HC 1115
Fourth Special Report	The potential impact of Brexit on the creative industries, tourism and the digital single market: Government Response to the Committee's Second Report of Session 2017–19	HC 1141