



House of Commons
Digital, Culture, Media and
Sport Committee

**Disinformation and
'fake news': Final Report**

Eighth Report of Session 2017–19

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

*Ordered by the House of Commons
to be printed 14 February 2019*

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*)

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

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

Committee reports are published on the Committee's website at www.parliament.uk/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), Mems Ayinla (Second Clerk), Mubeen Bhutta (Second Clerk), Josephine Willows (Senior Committee Specialist), Lois Jeary (Committee Specialist), Andy Boyd (Senior Committee Assistant), Keely Bishop (Committee Assistant), Sarah Potter (Attached Hansard Scholar), Lucy Dargahi (Media Officer) and Anne Peacock (Senior Media and Communication 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

You can follow the Committee on Twitter using [@CommonsCMS](#).

Contents

Summary	5
1 Introduction and background	7
2 Regulation and the role, definition and legal liability of tech companies	10
Definitions	10
Online harms and regulation	10
The new Centre for Data Ethics and algorithms	11
Legislation in Germany and France	12
The UK	13
Use of personal and inferred data	17
Enhanced role of the ICO and a levy on tech companies	18
3 Data use and data targeting	20
Introduction	20
The ICO's fine of Facebook	20
The ICO, SCL Group and Cambridge Analytica	21
Facebook and the Federal Trade Commission Consent Decree 2011	23
Facebook and the Six4Three case	26
White Lists	27
Value of friends' data	29
The linking of data access with spending on advertising at Facebook	30
Facebook's sharing of data with developers	33
Facebook collecting data from Android customers	35
Facebook's monitoring of app usage	36
Facebook targeting competitor apps	38
Facebook's response to the publication of the Six4Three documents	38
Facebook's business model and further challenges for regulators	40
Leave.EU and data from Eldon Insurance allegedly used for campaigning work	43
4 Aggregate IQ	45
Introduction	45
Relationship between AIQ and SCL/Cambridge Analytica before the UK's EU referendum	48
AIQ work related to the EU Referendum	50
Facebook and the Vote Leave £50 million prediction competition	52
AIQ's Capabilities	53
Artificial intelligence	53

Facebook Pixels	53
LinkedIn profile scraper	55
Conclusion	55
5 Advertising and political campaigning	57
Introduction	57
Online adverts	57
Online political adverts	58
Facebook and Mainstream Network	62
Constitutional Research Council (CRC)	64
The Cairncross Review: a sustainable future for journalism	67
6 Foreign influence in political campaigns	68
Introduction	68
Russian interference in UK elections	69
Facebook and Russian disinformation	72
Russian IP addresses at Facebook	72
Facebook data owned by the Cambridge University Psychometrics Centre and shared with Russian APIs	73
Russian interference through other social media platforms	73
Leave.EU, Arron Banks, the US and Russia	74
Further ongoing investigations and criminal complaints	76
7 SCL influence in foreign elections	78
Introduction	78
Further information regarding the work of SCL	78
Citizenship-by-investment schemes	79
Conflicts of interest	82
8 Digital literacy	85
Introduction	85
Friction in the system	86
Regulators and digital literacy	87

Conclusions and recommendations	89
Annex 1 'International Grand Committee' attendees, Tuesday 27 November 2018	98
Annex 2 International Principles on the Regulation of Tech Platforms	99
Formal minutes	100
Witnesses	101
Published written evidence	105
List of Reports from the Committee during the current Parliament	108

Summary

This is the Final Report in an inquiry on disinformation that has spanned over 18 months, covering individuals' rights over their privacy, how their political choices might be affected and influenced by online information, and interference in political elections both in this country and across the world—carried out by malign forces intent on causing disruption and confusion.

We have used the powers of the Committee system, by ordering people to give evidence and by obtaining documents sealed in another country's legal system. We invited democratically-elected representatives from eight countries to join our Committee in the UK to create an 'International Grand Committee', the first of its kind, to promote further cross-border co-operation in tackling the spread of disinformation, and its pernicious ability to distort, to disrupt, and to destabilise. Throughout this inquiry we have benefitted from working with other parliaments. This is continuing, with further sessions planned in 2019. This has highlighted a worldwide appetite for action to address issues similar to those that we have identified in other jurisdictions.

This is the Final Report in our inquiry, but it will not be the final word. We have always experienced propaganda and politically-aligned bias, which purports to be news, but this activity has taken on new forms and has been hugely magnified by information technology and the ubiquity of social media. In this environment, people are able to accept and give credence to information that reinforces their views, no matter how distorted or inaccurate, while dismissing content with which they do not agree as 'fake news'. This has a polarising effect and reduces the common ground on which reasoned debate, based on objective facts, can take place. Much has been said about the coarsening of public debate, but when these factors are brought to bear directly in election campaigns then the very fabric of our democracy is threatened.

This situation is unlikely to change. What does need to change is the enforcement of greater transparency in the digital sphere, to ensure that we know the source of what we are reading, who has paid for it and why the information has been sent to us. We need to understand how the big tech companies work and what happens to our data. Facebook operates by monitoring both users and non-users, tracking their activity and retaining personal data. Facebook makes its money by selling access to users' data through its advertising tools. It further increases its value by entering into comprehensive reciprocal data-sharing arrangements with major app developers who run their businesses through the Facebook platform.

Meanwhile, among the countless innocuous postings of celebrations and holiday snaps, some malicious forces use Facebook to threaten and harass others, to publish revenge porn, to disseminate hate speech and propaganda of all kinds, and to influence elections and democratic processes—much of which Facebook, and other social media companies, are either unable or unwilling to prevent. We need to apply widely-accepted democratic principles to ensure their application in the digital age.

The big tech companies must not be allowed to expand exponentially, without constraint or proper regulatory oversight. But only governments and the law are powerful enough to contain them. The legislative tools already exist. They must now be applied to digital

activity, using tools such as privacy laws, data protection legislation, antitrust and competition law. If companies become monopolies they can be broken up, in whatever sector. Facebook's handling of personal data, and its use for political campaigns, are prime and legitimate areas for inspection by regulators, and it should not be able to evade all editorial responsibility for the content shared by its users across its platforms.

In a democracy, we need to experience a plurality of voices and, critically, to have the skills, experience and knowledge to gauge the veracity of those voices. While the Internet has brought many freedoms across the world and an unprecedented ability to communicate, it also carries the insidious ability to distort, to mislead and to produce hatred and instability. It functions on a scale and at a speed that is unprecedented in human history. One of the witnesses at our inquiry, Tristan Harris, from the US-based Center for Humane Technology, describes the current use of technology as "hijacking our minds and society". We must use technology, instead, to free our minds and use regulation to restore democratic accountability. We must make sure that people stay in charge of the machines.

1 Introduction and background

1. The DCMS Committee's Interim Report, "Disinformation and 'fake news'" was published in July 2018.¹ Since the summer of 2018, the Committee has held three further oral evidence sessions, inviting UK regulators and the Government to give oral evidence, and we received a further 23 written submissions.² We also held an 'International Grand Committee' in November 2018, inviting parliamentarians from nine countries: Argentina, Belgium, Brazil, Canada, France, Ireland, Latvia, Singapore and the UK.

2. Our long inquiry into disinformation and misinformation has highlighted the fact that definitions in this field matter. We have even changed the title of our inquiry from "fake news" to "disinformation and 'fake news'", as the term 'fake news' has developed its own, loaded meaning. As we said in our Interim Report, 'fake news' has been used to describe content that a reader might dislike or disagree with. US President Donald Trump has described certain media outlets as 'The Fake News Media' and being 'the true enemy of the people'.³

3. We are, therefore, pleased that the Government accepted the recommendations in our Interim Report and, instead of using the term 'fake news', is using 'disinformation' to describe "the deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain".⁴

4. This Final Report builds on the main issues highlighted in the seven areas covered in the Interim Report: the definition, role and legal liabilities of social media platforms; data misuse and targeting, based around the Facebook, Cambridge Analytica and Aggregate IQ (AIQ) allegations, including evidence from the documents we obtained from Six4Three about Facebook's knowledge of and participation in data-sharing; political campaigning; Russian influence in political campaigns; SCL influence in foreign elections; and digital literacy. We also incorporate analysis by the consultancy firm, 89up, of the repository data we received from Chris Vickery, in relation to the AIQ database.

5. In this Final Report, we build on the principle-based recommendations made in the Interim Report. We look forward to hearing the Government's response to these recommendations within two months. We hope that this will be much more comprehensive, practical, and constructive than their response to the Interim Report, published in October 2018.⁵ Several of our recommendations were not substantively answered and there is now an urgent need for the Government to respond to them. We were pleased that the Secretary of State, Rt Hon Jeremy Wright MP, described our exchanges as being part of "an iterative process", and that this Report will be "quite helpful, frankly, in being able to feed into our further conclusions before we write the White Paper" and that our views

1 The 'Disinformation and 'fake news': Interim Report' was the most looked at HTML on the parliamentary website this calendar year, with 13,646 unique page views of the 'Contents' page (the average is around 650 views). The PDF had 4,310 unique visits to it from the parliamentary website, whereas the committee-wide average is around 280 views. The Interim Report was the most viewed HTML and second most viewed PDF of any House of Commons Committee Report in the past five years (statistics supplied by the Web and Publications Unit, House of Commons).

2 [Written evidence - Disinformation and 'fake news'](#)

3 [Donald J.Trump tweet](#), 29 October 2018.

4 [Disinformation and 'fake news': Government Response to the Committee's Fifth Report of Session 2017-19](#), 23 October 2018, HC 1630 Government response to Interim Report, page 2.

5 As above.

will form part of the Government's considerations.⁶ We look forward to the Government's *Online Harms* White Paper, issued by both the Department for Digital, Culture, Media and Sport and the Home Office, which we understand will be published in early 2019, and will tackle the issues of online harms, including disinformation.⁷ We have repeated many of the recommendations in our Interim Report to which the Government did not respond. We presume and expect that the Government will respond to both recommendations in this Final Report and those unanswered in the Interim Report.

6. This Final Report is the accumulation of many months of collaboration with other countries, organisations, parliamentarians and individuals from around the world. In total, the Committee held 23 oral evidence sessions, received over 170 written submissions, heard evidence from 73 witnesses, asking over 4,350 questions at these hearings, and had many exchanges of public and private correspondence with individuals and organisations.

7. It has been an inquiry of collaboration, in an attempt to get to grips with the complex technical, political and philosophical issues involved, and to seek practical solutions to those issues. As we did in our Interim Report, we thank all those many individuals and companies, both at home and abroad—including our colleagues and associates in America—for being so generous with sharing their views and information.⁸

8. We would also like to acknowledge the work of other parliamentarians who have been exploring similar issues at the same time as our inquiry. The Canadian Standing Committee on Access to Information, Privacy and Ethics published its report, "Democracy under threat: risks and solutions in the era of disinformation and data monopoly" in December 2018.⁹ The report highlights the Canadian Committee's study of the breach of personal data involving Cambridge Analytica and Facebook, and broader issues concerning the use of personal data by social media companies and the way in which such companies are responsible for the spreading of misinformation and disinformation. Their recommendations chime with many of our own in this Report.

9. The US Senate Select Committee on Intelligence has an ongoing investigation into the extent of Russian interference in the 2016 US elections. As a result of data sets provided by Facebook, Twitter and Google to the Intelligence Committee—under its Technical Advisory Group—two third-party reports were published in December 2018. New Knowledge, an information integrity company, published "The Tactics and Tropes of the Internet Research Agency", which highlights the Internet Research Agency's tactics and messages in manipulating and influencing Americans, and includes a slide

6 [Q263](#), Evidence session, 24 October 2018, The Work of the Department for Digital, Culture, Media and Sport.

7 [Disinformation and 'fake news': Government Response to the Committee's Fifth Report of Session 2017–19](#), 23 October 2018, HC 1630 Government response to Interim Report, page 1.

8 Our expert advisor for the inquiry was Dr Charles Kriel. His Declaration of Interests are: Associate Fellow at the King's Centre for Strategic Communications (KCSC), King's College London; Founder, Kriel.Agency; Co-founder and shareholder, Lightful; Advisor, Trinidad and Tobago parliamentary committee on national security. The Committee also commissioned the following people to carry out specific pieces of research for this inquiry: Mike Harris, CEO of 89up; Martin Barnard, CTO of 89up; Josh Feldberg, Director of Digital at 89up; and Peter Pomerantsev, Visiting Fellow at the London School of Economics (LSE). We are also grateful to Ashkan Soltani, independent researcher and consultant and former Chief Technologist at the Federal Trade Commission, who advised on paragraphs related to the FTC in Chapter 3.

9 [Democracy under threat: risks and solutions in the era of disinformation and data monopoly](#), Report of the Standing Committee on Access to Information, Privacy and Ethics, 42nd Parliament, 1st Session, December 2018.

desk, highlighting statistics, infographics and thematic presentation of memes.¹⁰ The Computational Propaganda Research Project and Graphika published the second report, which looks at activities of known Internet Research Agency accounts, using Facebook, Instagram, Twitter and YouTube between 2013 and 2018, to impact US users.¹¹ These two reports will be incorporated into the Intelligence Committee's own report in 2019.

10. Our 'International Grand Committee' meeting, held in November 2018, was the culmination of this collaborative work. The Committee was composed of 24 democratically-elected representatives from nine countries, including the 11 members of the DCMS Committee, who together represent a total of 447 million people. The representatives signed a set of International Principles at that meeting.¹² We exchanged ideas and solutions both in private and public, and held a seven-hour oral evidence session. We invited Mark Zuckerberg, CEO of Facebook—the social media company that has over 2.25 billion users and made \$40 billion in revenue in 2017—to give evidence to us and to this Committee; he chose to refuse, three times.¹³ Yet, within four hours of the subsequent publication of the documents we obtained from Six4Three—about Facebook's knowledge of and participation in data sharing—Mr Zuckerberg responded with a post on his Facebook page.¹⁴ We thank our 'International Grand Committee' colleagues for attending the important session, and we look forward to continuing our collaboration this year.

10 [The Disinformation Report](#), New Knowledge (Renee DiResta, Dr Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, New Knowledge, and Dr Jonathan Albright, Tow Center for Digital Journalism, Columbia University, and Ben Johnson, Canfield Research, LLC), December 2018.

11 [The IRA and Political Polarization in the United States, 2012 - 2018](#), Philip N. Howard, Bharath Ganesh, Dimitri Liotsiou, University of Oxford, and John Kelly, Camille Francois, Graphika, December 2018.

12 See Annex 2. The Principles will form the basis of the Grand Committee's work, and have been reported to the House of Commons as a memorandum. The original will be placed in the House of Commons parliamentary archive.

13 Dominic Cummings also refused to give oral evidence to the DCMS Committee. The Committee published its Third Special Report of Session 2017–18, [Failure of a witness to answer an Order of the Committee: conduct of Mr Dominic Cummings](#), on 5 June 2018. The Report informed the House of Mr Cummings' failure to report to the Committee. The Committee sought an Order of the House requiring Mr Cummings to agree a date for his appearance before the Committee. The House issued the Order, with which Mr Cummings did not comply. The Matter was referred to the Committee of Privileges on 28 June 2018.

14 Details of Mark Zuckerberg's post can be found in Chapter 3.

2 Regulation and the role, definition and legal liability of tech companies

Definitions

11. In our Interim Report, we disregarded the term 'fake news' as it had "taken on a variety of meanings, including a description of any statement that is not liked or agreed with by the reader" and instead recommended the terms 'misinformation' and 'disinformation'. With those terms come "clear guidelines for companies, organisations and the Government to follow" linked with "a shared consistency of meaning across the platforms, which can be used as the basis of regulation and enforcement".¹⁵

12. We were pleased that the Government accepted our view that the term 'fake news' is misleading, and instead sought to address the terms 'disinformation' and 'misinformation'. In its response, the Government stated:

In our work we have defined disinformation as the deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain. 'Misinformation' refers to the inadvertent sharing of false information.¹⁶

13. We also recommended a new category of social media company, which tightens tech companies' liabilities, and which is not necessarily either a 'platform' or a 'publisher'. The Government did not respond at all to this recommendation, but Sharon White, Chief Executive of Ofcom, called this new category "very neat" because "platforms do have responsibility, even if they are not the content generator, for what they host on their platforms and what they advertise".¹⁷

14. Social media companies cannot hide behind the claim of being merely a 'platform' and maintain that they have no responsibility themselves in regulating the content of their sites. We repeat the recommendation from our Interim Report 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'. This approach would see the tech companies assume legal liability for content identified as harmful after it has been posted by users. We ask the Government to consider this new category of tech company in its forthcoming White Paper.

Online harms and regulation

15. Earlier in our inquiry, we heard evidence from both Sandy Parakilas and Tristan Harris, who were both at that time involved in the US-based Center for Human Technology. The Center has compiled a 'Ledger of Harms', which summarises the "negative impacts of technology that do not show up on the balance sheets of companies, but on the balance

15 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 14.

16 [Disinformation and 'fake news': Government Response to the Committee's Fifth Report of Session 2017–19](#), 23 October 2018, HC 1630 Government response to Interim Report, p 2.

17 [Q3789](#)

sheet of society”.¹⁸ The Ledger of Harms includes negative impacts of technology, including loss of attention, mental health issues, confusions over personal relationships, risks to our democracies, and issues affecting children.¹⁹

16. This proliferation of online harms is made more dangerous by focussing specific messages on individuals as a result of ‘micro-targeted messaging’—often playing on and distorting people’s negative views of themselves and of others. This distortion is made even more extreme by the use of ‘deepfakes’, audio and videos that look and sound like a real person, saying something that that person has never said.²⁰ As we said in our Interim Report, these examples will only become more complex and harder to spot, the more sophisticated the software becomes.²¹

17. The Health Secretary, Rt Hon Matthew Hancock MP, recently warned tech companies, including Facebook, Google and Twitter, that they must remove inappropriate, harmful content, following the events surrounding the death of Molly Russell who, aged 14, took her own life in November 2017. Her Instagram account contained material connected with depression, self harm and suicide. Facebook, which owns Instagram, said that it was ‘deeply sorry’ over the case.²² The head of Instagram, Adam Mosseri, had a meeting with the Health Secretary in early February 2019, and said that Instagram was “not where we need to be on issues of self-harm and suicide” and that it was trying to balance “the need to act now and the need to act responsibly”.²³

18. We also note that in her speech on 5 February 2019 that Margot James MP, the Minister for Digital, at the Department for Digital, Culture, Media and Sport expressed her concerns that:

For too long the response from many of the large platforms has fallen short. There have been no fewer than fifteen voluntary codes of practice agreed with platforms since 2008. Where we are now is an absolute indictment of a system that has relied far too little on the rule of law. The White Paper, which DCMS are producing with the Home Office, will be followed by a consultation over the summer and will set out new legislative measures to ensure that the platforms remove illegal content, and prioritise the protection of users, especially children, young people and vulnerable adults.²⁴

The new Centre for Data Ethics and algorithms

19. As we said in our Interim Report, 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. The tech companies’ business models rely on revenue

18 [Ledger of Harms](#), Center for Humane Technology, accessed 29 November 2018.

19 We will explore issues of addiction and digital health further in our immersive and addictive technologies inquiry in 2019.

20 Edward Lucas, [Q881](#)

21 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 12.

22 [Health secretary tells social media firms to protect children after girl's death](#), Michael Savage, The Observer, 27 January 2019.

23 [Instagram vows to remove all graphic self-harm images from site](#), BBC, 7 February 2019.

24 [Margot James speech on Safer Internet Day](#), gov.uk, 5 February 2018.

coming from the sale of adverts and, because the bottom line is profit, any form of content that increases profit will always be prioritised. Therefore, negative stories will always be prioritised by algorithms, as they are shared more frequently than positive stories.²⁵

20. Just as information about the tech companies themselves needs to be more transparent, so does information about their algorithms. These can carry inherent biases, as a result of the way that they are developed 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”. 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.²⁶

21. Following an announcement in the 2017 Budget, the new Centre for Data Ethics and Innovation was set up by the Government to advise on “how to enable and ensure ethical, safe and innovative uses of data, including for AI”. The Secretary of State described its role:

The Centre is a core component of the Government’s Digital Charter, which seeks to agree norms and rules for the online world. The Centre will enable the UK to lead the global debate about how data and AI can and should be used.²⁷

22. The Centre will act as an advisory body to the Government and its core functions will include: analysing and anticipating gaps in governance and regulation; agreeing and articulating best practice, codes of conduct and standards in the use of Artificial Intelligence; and advising the Government on policy and regulatory actions needed in relation to innovative and ethical uses of data.²⁸

23. The Government response to our Interim Report highlighted consultation responses, including the Centre’s priority for immediate action, including “data monopolies, the use of predictive algorithms in policing, the use of data analytics in political campaigning, and the possibility of bias in automated recruitment decisions”. We welcome the introduction of the Centre and look forward to taking evidence from it in future inquiries.

Legislation in Germany and France

24. Other countries have legislated against harmful content on tech platforms. As we said in our Interim Report, tech companies in Germany were initially asked to remove hate speech within 24 hours. When this self-regulation did not work, 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

25 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 70.

26 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 71.

27 Centre for Data Ethics and Innovation: Government response to consultation, November 2018.

28 As above.

sites within 24 hours, and fines them €20 million if it is not removed.²⁹ 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.³⁰

25. A new law in France, passed in November 2018, allows judges to order the immediate removal of online articles that they decide constitute disinformation, during election campaigns. The law states that users must be provided with "information that is fair, clear and transparent" on how their personal data is being used, that sites have to disclose money they have been given to promote information, and the law allows the French national broadcasting agency to have the power to suspend television channels controlled by or under the influence of a foreign state if they "deliberately disseminate false information likely to affect the sincerity of the ballot". Sanctions imposed in violation of the law includes one year in prison and a fine of €75,000.³¹

The UK

26. As the UK Information Commissioner, Elizabeth Denham, told us in November 2018, a tension exists between the social media companies' business model, which is focused on advertising, and human rights, such as the protection of privacy: "That is where we are right now and it is a very big job for both the regulators and the policymakers to ensure that the right requirements, oversight and sanctions are in place."³² She told us that Facebook, for example, should do more and should be "subject to stricter regulation and oversight".³³ Facebook's activities in the political sphere, indeed, have been expanding; it has recently launched a 'Community Actions' News Feed petition feature, for instance, to allow users to organise around local political issues, by starting and supporting political petitions. It is hard to understand how Facebook will be able to self-regulate such a feature; the more controversial and contentious the local issue, the more engagement there will be on Facebook, with the accompanying revenue from adverts.³⁴

Facebook and regulation

27. Despite all the apologies for past mistakes that Facebook has made, it still seems unwilling to be properly scrutinised. Several times throughout the oral evidence session at the 'International Grand Committee', Richard Allan, Vice President of Policy Solutions at Facebook, was asked about Facebook's views on regulation, and each time he stated that Facebook was very open to the debate on regulation, and that working together with governments would be the best way forward:

I am pleased, personally, and the company is very much engaged, all the way up to our CEO—he has spoken about this in public—on the idea of getting the right kind of regulation so that we can stop being in this confrontational mode. It doesn't serve us or our users well. Let us try to

29 [Germany start enforcing hate speech law](#), BBC, 1 January 2018.

30 Professor Lewandovsky, [Q233](#)

31 [France passes controversial 'fake news' law](#), Michael-Ross Fiorentino, Euronews, November 2018.

32 [Q3918](#)

33 [Q3916](#)

34 [Facebook's new 'Community Actions' will bring user-made petitions to your feed](#), Techregister, 21 January 2019.

get to the right place, where you agree that we are doing a good enough job and you have powers to hold us to account if we are not, and we understand what the job is that we need to do. That is on the regulation piece.³⁵

28. Ashkan Soltani, an independent researcher and consultant, and former Chief Technologist to the US Federal Trade Commission (FTC), called into question Facebook's willingness to be regulated. When discussing Facebook's internal culture, he said, "There is a contemptuousness—that ability to feel like the company knows more than all of you and all the policy makers".³⁶ He discussed the California Consumer Privacy Act, which Facebook supported in public, but lobbied against, behind the scenes.³⁷

29. Facebook seems willing neither to be regulated nor scrutinised. It is considered common practice for foreign nationals to give evidence before committees. Indeed, in July 2011, the then Culture, Media and Sport Committee heard evidence from Rupert Murdoch, during the inquiry into phone hacking³⁸ and the Treasury Committee has recently heard evidence from three foreign nationals.³⁹ **By choosing not to appear before the Committee and by choosing not to respond personally to any of our invitations, Mark Zuckerberg has shown contempt towards both the UK Parliament and the 'International Grand Committee', involving members from nine legislatures from around the world.**

30. The management structure of Facebook is opaque to those outside the business and this seemed to be designed to conceal knowledge of and responsibility for specific decisions. Facebook used the strategy of sending witnesses who they said were the most appropriate representatives, yet had not been properly briefed on crucial issues, and could not or chose not to answer many of our questions. They then promised to follow up with letters, which—unsurprisingly—failed to address all of our questions. We are left in no doubt that this strategy was deliberate.

Existing UK regulators

31. In the UK, the main relevant regulators—Ofcom, the Advertising Standards Authority, the Information Commissioner's Office, the Electoral Commission and the Competition and Markets Authority—have specific responsibilities around the use of content, data and conduct. When Sharon White, the chief executive of Ofcom appeared in front of the Committee in October 2018, following the publication of our interim report, we asked her whether their experience as a broadcasting regulator could be of benefit when considering how to regulate content online. She said:

We have tried to look very carefully at where we think the synergies are. [...] It struck us that there are two or three areas that might be applicable online.

35 [Q4231](#)

36 [Q4337](#)

37 [Q4330](#)

38 [Uncorrected transcript of oral evidence](#), CMS Committee inquiry into phone hacking, 19 July 2011. In reference to international witnesses giving evidence before committees, Erskine May states: "Foreign or Commonwealth nationals are often invited to attend to give evidence before committees. Commissioners or officials of the European Commission, irrespective of nationality, have regularly given evidence. Select committees frequently obtain written information from overseas persons or representative bodies."

39 Anil Kashyap (who lives and works in Canada), External member of the Financial Policy Committee, Bank of England (16 January 2019); Benoit Rochet, Deputy CEO, Port of Calais (5 June 2018); and Joachim Coens, CEO, Port of Zeebrugge (5 June 2018).

[...] The fact that Parliament has set standards, set quite high level objectives, has felt to us very important but also very enduring with key objectives, whether that is around the protection of children or concerns about harm and offence. You can see that reading across to a democratic process about what are the harms that we believe as a society may be prevalent online. The other thing that is very important in the broadcasting code is that it sets out explicitly the fact that these things adapt over time as concerns about harm adapt and concerns among consumers adapt. It then delegates the job to an independent regulator to work through in practice how those so-called standards objectives are carried forward. There is transparency, the fact that we publish our decisions when we breach, and that is all very open to the public. There is scrutiny of our decisions and there is independence around the judgment.⁴⁰

32. She also added that the job of a regulator of online content could be to assess the effectiveness of the technology companies in acting against content which has been designated as harmful; “One approach would be to say do the companies have the systems and the processes and the governance in place with transparency that brings public accountability and accountability to Parliament, that the country could be satisfied of a duty of care or that the harms are being addressed in a consistent and effective manner”.⁴¹

33. However, should Ofcom be asked to take on the role of regulating the ability of social media companies, it would need to be given new investigatory powers. Sharon White told the committee that “It would be absolutely fundamental to have statutory information-gathering powers on a broad area”.⁴²

34. The UK Council for Internet Safety (UKCIS) is a new organisation, sponsored by the Department for Digital, Culture, Media and Sport, the Department for Education and the Home Office, bringing together more than 200 organisations with the intention of keeping children safe online. Its website states: “If it’s unacceptable offline, it’s unacceptable online”. Its focus will include online harms such as: cyberbullying and sexual exploitation; radicalisation and extremism; violence against women and girls; hate crime and hate speech; and forms of discrimination against groups protected under the Equality Act.⁴³ Guy Parker, CEO of the Advertising Standards Authority, told us that the Government could decide to include advertising harms within their definition of online harms.⁴⁴

35. We believe that the UK Council for Internet Safety should include within its remit “the risk to democracy” as identified in the Center for Human Technology’s “Ledger of Harms”, particularly in relation to deep fake films. We note that Facebook is included as a member of the UKCIS and, in view of its potential influence, understand why. However, given the conduct of Facebook in this inquiry, we have concerns about the good faith of the business and its capacity to participate in the work of UKCIS in the public interest, as opposed to its own interests.

36. When the Secretary of State for Digital, Culture, Media and Sport (DCMS), Rt Hon Jeremy Wright MP, was asked about formulating a spectrum of online harm, he gave a

40 [Q3781](#)

41 [Q3784](#)

42 [Q3785](#)

43 [UK Council for Internet Safety](#), gov.uk, July 2018.

44 [Q4115](#)

limited answer: “What we need to understand is the degree to which people are being misled or the degree to which elections are being improperly interfered with or influenced and, if they are [...] we need to come up with appropriate responses and defences. It is part of a much more holistic landscape and I do not think it is right to try to segment it out”.⁴⁵ However, having established the difficulties surrounding the definition, spread and responsibility of online harms, the Secretary of State was more forthcoming when asked about the regulation of social media companies, and said that the UK should be taking the lead:

My starting point is what are the harms, and what are the responsibilities that we can legitimately expect online entities to have for helping us to minimise, or preferably to eliminate, those harms. Then, once you have established those responsibilities, what systems should be in place to support the exercise of those responsibilities.⁴⁶

We hope that the Government’s White Paper will outline its view on suitable legislation to ensure there is proper, meaningful online safety and the role expected of the UKCIS.

37. *Our Interim Report recommended that clear legal liabilities should be established for tech companies to act against harmful or illegal content on their sites. There is now an urgent need to establish independent regulation. We believe that a compulsory Code of Ethics should be established, overseen by an independent regulator, setting out what constitutes harmful content. The independent regulator would have statutory powers to monitor relevant tech companies; this would create a regulatory system for online content that is as effective as that for offline content industries.*

38. *As we said in our Interim Report, such a Code of Ethics should be similar to the Broadcasting Code issued by Ofcom—which is based on the guidelines established in section 319 of the 2003 Communications Act. The Code of Ethics should be developed by technical experts and overseen by the independent regulator, in order to set down in writing what is and is not acceptable on social media. This should include harmful and illegal content that has been referred to the companies for removal by their users, or that should have been easy for tech companies themselves to identify.*

39. *The process should establish clear, legal liability for tech companies to act against agreed harmful and illegal content on their platform and such companies should have relevant systems in place to highlight and remove ‘types of harm’ and to ensure that cyber security structures are in place. If tech companies (including technical engineers involved in creating the software for the companies) are found to have failed to meet their obligations under such a Code, and not acted against the distribution of harmful and illegal content, the independent regulator should have the ability to launch legal proceedings against them, with the prospect of large fines being administered as the penalty for non-compliance with the Code.*

40. *This same public body should have statutory powers to obtain any information from social media companies that are relevant to its inquiries. This could include the capability to check what data is being held on an individual user, if a user requests such information. This body should also have access to tech companies’ security mechanisms*

45 [Q255](#)

46 [Q229](#) Evidence session, 24 October 2018, The Work of the Department for Digital, Culture, Media and Sport.

and algorithms, to ensure they are operating responsibly. This public body should be accessible to the public and be able to take up complaints from members of the public about social media companies. We ask the Government to put forward these proposals in its forthcoming White Paper.

Use of personal and inferred data

41. When Mark Zuckerberg gave evidence to Congress in April 2018, in the wake of the Cambridge Analytica scandal, he made the following claim: “You should have complete control over your data [...] If we’re not communicating this clearly, that’s a big thing we should work on”. When asked who owns “the virtual you”, Zuckerberg replied that people themselves own all the “content” they upload, and can delete it at will.⁴⁷ However, the advertising profile that Facebook builds up about users cannot be accessed, controlled or deleted by those users. It is difficult to reconcile this fact with the assertion that users own all “the content” they upload.

42. In the UK, the protection of user data is covered by the General Data Protection Regulation (GDPR).⁴⁸ However, ‘inferred’ data is not protected; this includes characteristics that may be inferred about a user not based on specific information they have shared, but through analysis of their data profile. This, for example, allows political parties to identify supporters on sites like Facebook, through the data profile matching and the ‘lookalike audience’ advertising targeting tool. According to Facebook’s own description of ‘lookalike audiences’, advertisers have the advantage of reaching new people on Facebook “who are likely to be interested in their business because they are similar to their existing customers”.⁴⁹

43. The ICO Report, published in July 2018, questions the presumption that political parties do not regard inferred data as personal information:

Our investigation found that political parties did not regard inferred data as personal information as it was not factual information. However, the ICO’s view is that as this information is based on assumptions about individuals’ interests and preferences and can be attributed to specific individuals, then it is personal information and the requirements of data protection law apply to it.⁵⁰

44. Inferred data is therefore regarded by the ICO as personal data, which becomes a problem when users are told that they can own their own data, and that they have power of where that data goes and what it is used for. Protecting our data helps us secure the past, but protecting inferences and uses of Artificial Intelligence (AI) is what we will need to protect our future.

45. The Information Commissioner, Elizabeth Denham, raised her concerns about the use of inferred data in political campaigns when she gave evidence to the Committee in November 2018, stating that there has been:

47 [Congress grills Facebook CEO over data misuse - as it happened](#), Julia Carrie Wong, The Guardian, 11 April 2018.

48 [California Privacy Act homepage](#), accessed 18 December 2018.

49 [Annex to letter from Rebecca Stimson, Facebook, to the Chair, 14 May 2018: Letter from Gareth Lambe, Facebook, to Louise Edwards, Electoral Commission, 14 May 2018.](#)

50 [Democracy disrupted?](#) ICO Report, November 2018, para 3.8.2.

A disturbing amount of disrespect for personal data of voters and prospective voters. What has happened here is that the model that is familiar to people in the commercial sector of behavioural targeting has been transferred—I think transformed—into the political arena. That is why I called for an ethical pause so that we can get this right. We do not want to use the same model that sells us holidays and shoes and cars to engage with people and voters. People expect more than that. This is a time for a pause to look at codes, to look at the practices of social media companies, to take action where they have broken the law. For us, the main purpose of this is to pull back the curtain and show the public what is happening with their personal data.⁵¹

46. With specific reference to the use of 'lookalike audiences' on Facebook, Elizabeth Denham told the Committee that they "should be made transparent to the individuals [users]. They would need to know that a political party or an MP is making use of lookalike audiences. The lack of transparency is problematic".⁵² When we asked the Information Commissioner whether she felt that the use of 'lookalike audiences' was legal under GDPR, she replied: "We have to look at it in detail under the GDPR, but I am suggesting that the public is uncomfortable with lookalike audiences and it needs to be transparent".⁵³ People need to be clear that information they give for a specific purpose is being used to infer information about them for another purpose.

47. The Secretary of State, Rt Hon Jeremy Wright MP, also told us that the ethical and regulatory framework surrounding AI should develop alongside the technology, not "run to catch up" with it, as has happened with other technologies in the past.⁵⁴ We shall be exploring the issues surrounding AI in greater detail, in our inquiry into immersive and addictive technologies, which was launched in December 2018.⁵⁵

48. We support the recommendation from the ICO that inferred data should be as protected under the law as personal information. Protections of privacy law should be extended beyond personal information to include models used to make inferences about an individual. We recommend that the Government studies the way in which the protections of privacy law can be expanded to include models that are used to make inferences about individuals, in particular during political campaigning. This will ensure that inferences about individuals are treated as importantly as individuals' personal information.

Enhanced role of the ICO and a levy on tech companies

49. In our Interim Report, we called for the ICO to have greater capacity to be both an effective "sheriff in the Wild West of the Internet" and to anticipate future technologies. The ICO needs to have the same if not more technical expert knowledge as those

51 [Q4011](#)

52 [Q4016](#)

53 [Q4018](#)

54 [Q226](#), Oral evidence, 24 October 2018, Work of the Department for Digital, Culture, Media and Sport.

55 [Immersive and addictive technologies inquiry website](#), DCMS Committee, launched 7 December 2018.

organisations under scrutiny.⁵⁶ We recommended that a levy could be placed on tech companies operating in the UK, to help pay for this work, in a similar vein to the way in which the banking sector pays for the operating costs of the Financial Conduct Authority.⁵⁷

50. When the Secretary of State was asked his thoughts about a levy, he replied, with regard to Facebook specifically: “The Committee has my reassurance that if Facebook says it does not want to pay a levy, that will not be the answer to the question of whether or not we should have a levy.⁵⁸ He also told us that “neither I, nor, I think, frankly, does the ICO, believe that it is underfunded for the job it needs to do now. [...] If we are going to carry out additional activity, whether that is because of additional regulation or because of additional education, for example, then it does have to be funded somehow. Therefore, I do think the levy is something that is worth considering”.⁵⁹

51. *In our Interim Report, we recommended a levy should be placed on tech companies operating in the UK to support the enhanced work of the ICO. We reiterate this recommendation. The Chancellor’s decision, in his 2018 Budget, to impose a new 2% digital services tax on UK revenues of big technology companies from April 2020, shows that the Government is open to the idea of a levy on tech companies. The Government’s response to our Interim Report implied that it would not be financially supporting the ICO any further, contrary to our recommendation. We urge the Government to reassess this position.*

52. *The new independent system and regulation that we recommend should be established must be adequately funded. We recommend that a levy is placed on tech companies operating in the UK to fund its work.*

56 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 36.

57 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 36.

58 [Q263](#)

59 [Q262](#)

3 Data use and data targeting

Introduction

53. The ICO published its report, “Investigation into the use of data analytics in political campaigns” on 6 November 2018, the same day that the Information Commissioner and the Deputy Information Commissioner appeared before the Committee. The report was an update on its investigation into the use of data analytics for political purposes, which started in May 2017. It states that it “had little idea of what was to come. Eighteen months later, multiple jurisdictions are struggling to retain fundamental democratic principles in the face of opaque digital technologies”⁶⁰ and the report went on to reveal the extent of the illegal practices that took place during this time:

We have uncovered a disturbing disregard for voters’ personal privacy. Social media platforms, political parties, data brokers and credit reference agencies have started to question their own processes—sending ripples through the big data eco-system. We have used the full range of our investigative powers and where there have been breaches of the law, we have acted. We have issued monetary penalties and enforcement notices ordering companies to comply with the law. We have instigated criminal proceedings and referred issues to other regulators and law enforcement agencies as appropriate. And, where we have found no evidence of illegality, we have shared those findings openly. Our investigation uncovered significant issues, negligence and contraventions of the law.

54. This Chapter will build on data issues explored in our Interim Report, updating on progress where there has been resolution, and making recommendations to the Government, to ensure that such malpractice is tackled effectively in the future. As Elizabeth Denham told us when she gave evidence in November 2018, “This is a time for a pause to look at codes, to look at the practices of social media companies, to take action where they have broken the law”.⁶¹

55. We shall also focus on the Facebook documents dated between 2011 and 2015, which were provided to a Californian court by Facebook, under seal, as part of a US app developer’s lawsuit. The Committee ordered the provision of these documents from an individual in the UK on 19 November 2018 and we published them, in part, on 5 December 2018. We took this unusual step because we believed this information to be in the public interest, including to regulators, which it proved to be.

The ICO’s fine of Facebook

56. The ICO wrote in its report of November 2018 that it is in the process of referring issues about Facebook’s targeting functions and techniques used “to monitor individuals’ browsing habits, interactions and behaviour across the internet and different devices to the Irish Data Protection Commission, as the lead supervisory authority for Facebook under the General Data Protection Regulation (GDPR).”⁶²

60 [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018.

61 [Q4011](#)

62 [Investigation into the use of data analytics in political campaigns](#), ICO, November 2018, p9.

57. On 25 October 2018, the ICO imposed the maximum penalty possible at the time—£500,000—on Facebook under the UK’s previous data protection law (prior to the introduction, in May 2018, of the GDPR), for lack of transparency and security issues relating to the harvesting of data, in contravention of the first and seventh data protection principles of the Data Protection Act 1998.⁶³ Facebook has since appealed against the fine on the grounds that the ICO had not found evidence that UK users’ personal data had actually been shared. However, the Information Commissioner told us that the ICO’s fine was *not* about whether UK users’ data was shared. Instead:

We fined Facebook because it allowed applications and application developers to harvest the personal information of its customers who had not given their informed consent—think of friends, and friends of friends—and then Facebook failed to keep the information safe. [...] It is not a case of no harm, no foul. Companies are responsible for proactively protecting personal information and that’s been the case in the UK for thirty years. [...] Facebook broke data protection law, and it is disingenuous for Facebook to compare that to email forwarding, because that is not what it is about; it is about the release of users’ profile information without their knowledge and consent.⁶⁴

58. Elizabeth Denham told the Committee that the ICO “found their business practices and the way applications interact with data on the platform to have contravened data protection law. That is a big statement and a big finding”.⁶⁵ In oral evidence, Elizabeth Denham said that Facebook does not view the rulings from the federal privacy commissioner in Canada or the Irish ICO as anything more than advice.⁶⁶ She said that, from the evidence that Richard Allan, Vice President of Policy Solutions at Facebook, had given, she thought “that unless there is a legal order compelling a change in their business model and their practice, they are not going to do it”.⁶⁷

59. GDPR fines, introduced on 25 May 2018, are much higher than the £500,000 maximum specified in the Data Protection Act 1998. The new regulation includes provision for administrative fines of up to 4% of annual global turnover or €20 million, whichever is the greater.⁶⁸ In the fourth quarter of 2018, Facebook’s revenue rose 30% from a year earlier to \$16.9 billion and its profits increased by 61% to \$6.9 billion, showing the scope for much greater fines in the future.⁶⁹

The ICO, SCL Group and Cambridge Analytica

60. Our Interim Report described the “complex web of relationships” within what started out as the SCL (Strategic Communications Laboratories) group of companies, of which

63 Same as above.

64 [Q4284](#)

65 [Q4294](#)

66 [Q4284](#)

67 [Q4284](#)

68 [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016](#) Article 83, Chapter VIII.

69 [Facebook’s profits and revenue climb as it gains more users Mike Isaac](#), The New York Times, 30 January 2019.

Cambridge Analytica was a part.⁷⁰ The SCL Group went into administration in April 2018. The ICO's latest Report, published in November 2018, commented on its investigation into Cambridge Analytica. At that stage, the ICO had:

- issued an enforcement notice requiring Cambridge Analytica to deal with Professor David Carroll's Subject Access Request;⁷¹
- pursued a criminal prosecution for failing to deal properly with the enforcement notice;
- identified "serious breaches of data protection principles and would have issued a substantial fine if the company was not in administration";
- referred Cambridge Analytica to the Insolvency Service.⁷²

61. On 9 January 2019, SCL Elections Ltd was fined £15,000 for failing to comply with the enforcement notice issued by the ICO in May 2018, relating to David Carroll's Subject Access Request. The company pleaded guilty, through its administrators, to breaching Section 47(1) of the Data Protection Act 1998 (again, the fine was under the old legislation, not under the GDPR). Hendon Magistrates' Court also ordered the company to pay £6,000 costs and a victim surcharge of £170. In reaction, the Information Commissioner, Elizabeth Denham, made the following public statement:

This prosecution, the first against Cambridge Analytica, is a warning that there are consequences for ignoring the law. Wherever you live in the world, if your data is being processed by a UK company, UK data protection laws apply. Organisations that handle personal data must respect people's legal privacy rights. Where that does not happen and companies ignore ICO enforcement notices, we will take action.⁷³

62. We were keen to know when and which people working at Facebook first knew about the GSR/Cambridge Analytica breach. The ICO confirmed, in correspondence with the Committee, that three "senior managers" were involved in email exchanges earlier in 2015 concerning the GSR breach before December 2015, when it was first reported by The Guardian.⁷⁴ At the request of the ICO, we have agreed to keep the names confidential, but it would seem that this important information was not shared with the most senior executives at Facebook, leading us to ask why this was the case.

63. The scale and importance of the GSR/Cambridge Analytica breach was such that its occurrence should have been referred to Mark Zuckerberg as its CEO immediately. The fact that it was not is evidence that Facebook did not treat the breach with the seriousness it merited. It was a profound failure of governance within Facebook that its CEO did not

70 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 124.

71 For more information about Professor David Carroll's Subject Access Request, please see para 100 of [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19.

72 [Investigation into the use of data analytics in political campaigns](#), A report to Parliament, Information Commissioner's Office, 6 November 2018, page 8.

73 [SCL Elections prosecuted for failing to comply with enforcement notice](#), ICO website, 9 January 2019.

74 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.

know what was going on, the company now maintains, until the issue became public to us all in 2018. The incident displays the fundamental weakness of Facebook in managing its responsibilities to the people whose data is used for its own commercial interests.

Facebook and the Federal Trade Commission Consent Decree 2011

64. When Richard Allan, Vice President of Policy Solutions at Facebook, gave evidence in November 2018, he told us that “our intention is that you should not be surprised by the way your data is used [...] It is not a good outcome for us if you are”.⁷⁵ Yet, time and again, this Committee and the general public have been surprised by the porous nature of Facebook data security protocols and the extent to which users’ personal data has been shared in the past and continues to be shared today. The scale of this data sharing risks being massively increased, given the news that, by early 2020, Facebook is planning to integrate the technical infrastructure of Messenger, Instagram and WhatsApp, which, between them, have more than 2.6 billion users.⁷⁶

65. The Federal Trade Commission Consent Decree of 2011 is an example of the way in which Facebook’s security protocols and practices do not always align. In November 2009, Facebook users had a ‘central privacy page’, with the Facebook text stating: “Control who can see your profile and personal information”. A user’s profile and personal information might include: name; gender; email address; birthday; profile picture; hometown; relationship information; political and religious views; likes and interests; education and work; a Friends list; photos and videos; and messages.⁷⁷

66. In November 2011, the US Federal Trade Commission (FTC) made a complaint against Facebook on the basis that Facebook had, from May 2007 to July 2010, allowed external app developers unrestricted access information about Facebook users’ personal profile and related information, despite the fact that Facebook had informed users that platform apps “will access only the profile information these applications need to operate”.⁷⁸ The FTC complaint lists several examples of Facebook making promises to its users that were not kept:

- In December 2009, Facebook changed its website so that certain information that users may have designated as private—such as their Friends List—was made public. They did not warn users that this change was coming, or get their approval in advance;
- Facebook stated that third-party apps that users installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users’ personal data;
- Facebook told users they could restrict the sharing of their data to limited audiences—for example with “Friends Only.” In fact, selecting “Friends Only” did not prevent their information from being shared with third-party apps that their friends used;

75 [Q4188](#)

76 [Zuckerberg plans to integrate WhatsApp, Instagram, and Facebook Messenger](#), Mike Isaac, The New York Times, 25 January 2019.

77 [USA Trade Federal Commission, in the matter of Facebook Inc](#), DOCKET NO. C-4365, July 2012, p2.

78 As above, Para 30.

- Facebook had a “Verified Apps” option, which was supposed to certify the security of participating apps, but did not;
- Despite promising users that it would not share their personal information with advertisers, Facebook did share such information;
- Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible, but this content was still accessible;
- Facebook claimed that it complied with the US/EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union, but it did not.⁷⁹

67. Under the settlement, Facebook agreed to obtain consent from users before sharing their data with third parties. The settlement also required Facebook to establish a “comprehensive privacy program” to protect users’ data and to have independent, third-party audits every two years for the following 20 years to certify that it has a privacy programme that meets or exceeds the requirement of the FTC order.

68. When Richard Allan was asked at what point Facebook had made such changes to its own systems, to prevent developers from receiving information (which resulted in circumventing Facebook users’ own privacy settings), he replied that the change had happened in 2014:

The FTC objected to the idea that data may have been accessed from Facebook without consent and without permission. We were confident that the controls we implemented constituted consent and permission—others would contest that, but we believed we had controls in place that did that and that covered us for that period up to 2014”.⁸⁰

Richard Allan was referring here to the change from Version 1 of Facebook’s Application Programming Interface (API) to its more restrictive Version 2.

69. In reply to a question as to whether CEO Mark Zuckerberg knew that Facebook continued to allow developers access to that information, after the agreement, Richard Allan replied that Mr Zuckerberg and “all of us” knew that the platform continued to allow access to information. As to whether that was in violation of the FTC Consent Decree (and over two years after Facebook had agreed to it), he told us that “as long as we had the correct controls in place, that was not seen as being anything that was inconsistent with the FTC consent order”.⁸¹

70. Richard Allan was referring to Count 1 of the Federal Trade Commission’s complaint of 2011, which states that Facebook’s claim that the correct controls were in place was misleading:

Facebook has represented, expressly or by implication, that, through their Profile Privacy Settings, users can restrict access to their profile information to specific groups, such as “Only Friends” or “Friends of Friends.” In truth and in fact, in many instances, users could not restrict access to their

79 [Facebook settles FTC charges that it deceived consumers by failing to keep privacy promised](#), FTC, 29 November 2011.

80 [Q4178](#)

81 [Q4184](#)

profile information to specific groups, such as “Only Friends” or “Friends of Friends” through their Profile Privacy Settings. Instead, such information could be accessed by Platform Applications that their Friends used.⁸²

71. Richard Allan’s argument was that, while Facebook continued to allow the same data access—highlighted in the first count of the FTC’s complaint and of which the CEO, Mark Zuckerberg, was also aware—that was acceptable due to the fact that Facebook had supposedly put “controls” in place that constituted consent and permission.

72. Ashkan Soltani, an independent researcher and consultant, was then a primary technologist at the Federal Trade Commission, worked on the Facebook investigation in 2010 to 2011 and became the Chief Technologist at the FTC in 2014. Before our Committee, he questioned Richard Allan’s evidence:

Mr Allan corrected one of the comments from you all, specifically that apps in Version 1 of the API did not have unfiltered access to personal information. In fact, that is false. In the 2011 FTC settlement, the FTC alleged that if a user had an app installed, it had access to nearly all of the user’s profile information, even if that information was set to private. I think there is some sleight of hand with regards to V1, but this was early V1 and I believe it was only addressed after the settlement.⁸³

73. Mr Soltani clarified the timeline of events:

The timelines vary, but this—in my opinion—was V1, if they are considering the changes in 2014 as V2.⁸⁴ In short, I found that time and time again Facebook allows developers to access personal information of users and their friends, in contrast to their privacy settings and their policy statements.⁸⁵

74. Richard Allan did not specify what controls had been put in place by Facebook, but they did not prevent app developers, who were not authorised by a user, from accessing data that the user had specified should not to be shared (beyond a small group of friends on the privacy settings page). The FTC complaint took issue with both the fact that apps had unfettered access to users’ information, and that the privacy controls that Facebook represented as allowing users to control who saw their personal information were, in fact, inconsequential with regards to information to which the apps had access.

75. There was public outcry in March 2018, when the Cambridge Analytica data scandal was revealed and the vast majority of Facebook users had no idea that their data was able to be accessed by developers unknown to them, despite the fact that they had set privacy settings, specifically disallowing the practice.⁸⁶ Richard Allan also admitted to us that people might indeed take issue with Facebook’s position: “we were confident that the controls we implemented constituted consent and permission—others would

82 [USA Trade Federal Commission, in the matter of Facebook Inc](#), DOCKET NO. C-4365, July 2012.

83 [Q4327](#)

84 Facebook’s APIs were released as follows: V1.0 was introduced in April 2010, V2.0–2.12 was introduced in April 2014, and V3.0–3.2 was introduced in April 2018. V2 limited Facebook developers’ industrial-level access to users’ information, but the same day that Facebook launched V2, it announced its largest tracking and ad targeting initiative to date: the Facebook Audience Network, extending the company’s data profiling and ad-targeting from its own apps and services to the rest of the Internet.

85 [Q4327](#)

86 Para 102 to 110 of [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19.

contest that”.⁸⁷ He seemed to justify Facebook’s continued allowance of data access by app developers, by stating that the users had given their consent to this data access. The fact that Facebook continued to allow this access after the Consent Decree is not new information; the new information is the admission by Richard Allan that the CEO and senior management— “all of us”—knew that Facebook was continuing to allow the practice to occur, despite the public statements about its change of policy. That, people might well contest, constituted deceit and we would agree with them.⁸⁸ Ashkan Soltani told us that he believed that Facebook is in violation of the Consent Decree and the FTC has publicly confirmed that it is investigating the company.⁸⁹

76. The Cambridge Analytica scandal was facilitated by Facebook’s policies. If it had fully complied with the FTC settlement, it would not have happened. The US Federal Trade Commission (FTC) Complaint of 2011 ruled against Facebook—for not protecting users’ data and for letting app developers gain as much access to user data as they liked, without restraint—and stated that Facebook built their company in a way that made data abuses easy. When asked about Facebook’s failure to act on the FTC’s complaint, Elizabeth Denham, the Information Commissioner, told us: “I am very disappointed that Facebook, being such an innovative company, could not have put more focus, attention and resources into protecting people’s data”.⁹⁰ We are equally disappointed.

Facebook and the Six4Three case

77. A current court case at the San Mateo Superior Court in California also concerns Facebook’s data practices. It is alleged that Facebook violated the privacy of US citizens by actively exploiting its privacy policy, and that Mark Zuckerberg constructed a revenue-maximising and competition-suppressing scheme in mid-2012, in discussions with Chris Cox, Javier Oliván, Sheryl Sandberg, Dan Rose and Sam Lessin, and other senior Facebook colleagues, in its attempts to move Facebook’s business from a games and apps-driven desktop model to an advertising business model, delivered via smartphones.⁹¹

78. The published ‘corrected memorandum of points and authorities to defendants’ special motions to strike’, by the complainant in the case, the US-based app developer Six4Three, describes the allegations against Facebook; that Facebook used its users’ data to persuade app developers to create platforms on its system, by promising access to users’ data, including access to data of users’ friends.⁹² The case also alleges that those developers that became successful were targeted and ordered to pay money to Facebook. If apps became too successful, Facebook is alleged to have removed the access of data to those apps, thereby starving them of the information they needed to succeed. Six4Three lodged its original case in 2015, after Facebook removed developers’ access to friends’ data, including its own.

79. The DCMS Committee took the unusual, but lawful, step of obtaining these documents, which spanned between 2012 and 2014, even though they were sealed under

87 [Q4178](#)

88 [Q4184](#)

89 [Q4340](#)

90 [Q4316](#)

91 Facebook’s old model was taking a percentage of online payments made to Facebook apps (such as free-to-play games) that ran on desktop, but would not run on smartphones.

92 [The superior court of California, County of San Mateo](#) website.

a court order at the San Mateo Court, as we believed strongly that the documents related specifically to the serious issues of data privacy that we have been exploring for the past 18 months. The Committee received the documents after issuing an order for their delivery to Ted Kramer, the founder of Six4Three, whilst he was visiting London on a business trip in November 2018. Mr Kramer complied with the Committee's order, rather than risk being found to be in contempt of Parliament. Since we published these sealed documents, on 14 January 2019 another court agreed to unseal 135 pages of internal Facebook memos, strategies and employee emails from between 2012 and 2014, connected with Facebook's inappropriate profiting from business transactions with children.⁹³ A *New York Times* investigation published in December 2018 based on internal Facebook documents also revealed that the company had offered preferential access to users data to other major technology companies, including Microsoft, Amazon and Spotify.⁹⁴

80. We believed that our publishing the documents was in the public interest and would also be of interest to regulatory bodies, in particular the ICO and the FTC. In evidence, indeed, both the UK Information Commissioner and Ashkan Soltani, formerly of the FTC, said it would be. We published 250 pages of evidence selected from the documents on 5 December 2018 and at the same time as this Report's publication, we shall be publishing more evidence. The documents highlight Facebook's aggressive action against certain apps, including denying them access to data that they were originally promised. They highlight the link between friends' data and the financial value of the developers' relationship with Facebook. The main issues concern: 'white lists'; the value of friends' data; reciprocity; the sharing of data of users owning Android phones; and Facebook's targeting of competition.⁹⁵

White Lists

81. Facebook entered into 'whitelisting agreements' with certain companies, which meant that, after the platform changes in 2014/15, those companies maintained full access to friends' data. It is not fully clear that there was any user consent for this, nor precisely how Facebook decided which companies should be whitelisted or not.⁹⁶

82. When asked about user privacy settings and data access, Richard Allan consistently said that there were controls in place to limit data access, and that people were aware of how the data was being used. He said that Facebook was confident that the controls implemented constituted consent and permission.⁹⁷ He did admit that "there are very valid questions about how well people understand the controls and whether they are too complex," but said that privacy settings could not be overridden.⁹⁸ Finally, he stated that:

93 [Judge unseals trove of internal Facebook documents following our legal action](#), Nathan Halverson, Reveal, 17 January 2019; [Facebook knowingly duped game-playing kids and their parents out of money](#), Nathan Halverson, 24 January 2019.

94 [As Facebook raised a privacy wall, it carved an opening for tech giants](#), Gabriel J.X.Dance, Michael LaForgia and Nicholas Confessore, The New York Times, 18 December 2018.

95 The specific terms will be explained below.

96 In [the Six4Three documents](#), exhibits 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 94 and 95 include discussions on whitelisting businesses.

97 [Q4178](#)

98 Same as above.

“Our intention is that you should not be surprised by the way your data is used. Our intention is that it is clear and that you are not surprised. It is not a good outcome for us if you are”.⁹⁹

83. Ashkan Soltani rejected this claim, saying that up until 2012, platform controls did not exist, and privacy controls did not apply to apps. So even if a user set their profile to private, installed apps would still be able to access information. After 2012, Facebook added platform controls and made privacy controls applicable to apps. However, there were ‘whitelisted’ apps that could still access user data without permission and which, according to Ashkan Soltani, could access friends’ data for nearly a decade before that time.¹⁰⁰ Apps were able to circumvent users’ privacy of platform settings and access friends’ information, even when the user disabled the Platform.¹⁰¹ This was an example of Facebook’s business model driving privacy violations.

84. Expanding the whitelisting scheme resulted in a large number of companies striking special deals with Facebook. A November 2013 email discussion reveals that Facebook was managing 5,200 whitelisted apps.¹⁰² From the documents we received, the following well-known apps were among those whitelisted:

- **The Taxi app, Lyft:** Konstantinos Papamiltiadis at Facebook wrote to Lyft on 30 March 2015: “As far as I can tell, the app ID below have been whitelisted for all Mutual Friends access”;¹⁰³
- **AirBnB:** Mr Papamiltiadis wrote to Airbnb on 18 March 2015: “As promised, please find attached the docs for Hashed Friends API that can be used for social ranking. Let us know if this would be of interest to you, as we will need to sign an agreement that would allow you access to this API”;¹⁰⁴
- **Netflix:** Chris Barbour and Mr Papamiltiadis at Facebook wrote to Netflix on 17 February 2015, and Netflix wrote on 13 February, “we will be whitelisted for getting all friends, not just connected friends”;¹⁰⁵

85. All whitelisted companies used a standard form agreement called a “Private Extended API Addendum,” which reads in part:

Access to the Private Extended APIs. Subject to the terms of the Agreement, FB may, in its sole discretion, make specific Private Extended APIs available to Developer for use in connection with Developer Applications. FB may terminate such access for convenience at any time. The Private Extended APIs and the Private Extended API Guidelines will be deemed to be a part of the Platform and the Platform Policies, respectively, for purposes of the Agreement.... ‘Private Extended APIs’ means a set of APIs and services provided by FB to Developer that enables Developer to retrieve data or

99 [Q4188](#)

100 [Q4343](#)

101 [Q4327](#), Ashkan Soltani.

102 [Exhibit 100](#)

103 [Exhibit 87](#)

104 [Exhibit 91](#)

105 [Exhibit 92](#)

functionality relating to Facebook that is not generally available under Platform, which may include persistent authentication, photo upload, video upload, messaging and phonebook connectivity.¹⁰⁶

86. From the documents, it is also clear that whitelisting had been under consideration for quite some time in the run-up to all these special permissions being granted. There was an internal Facebook discussion, for instance, about the whitelisting process in an email sent on 5 September 2013: **“We need to build collective experience on how to review the access that’s been granted, and how to make decisions about keep/kill/contract”**.¹⁰⁷

Value of friends’ data

87. It is clear that increasing revenues from major app developers was one of the key drivers behind the policy changes made by Facebook. The idea of linking access to friends’ data to the financial value of the developers’ relationship with Facebook was a recurring feature of the documents.

88. The FTC had found that Facebook misrepresented its claims regarding their app oversight programme, specifically the ‘verified apps programme’, which was a review allegedly designed to give users additional assurances and help them identify trustworthy applications. The review was non-existent and there was no oversight of those apps. Some preinstalled apps were able to circumvent users’ privacy settings or platform settings, and to access friends’ information as well as users’ information, such as birthdays and political affiliation, even when the user disabled the platform. For example, Yelp and Rotten Tomatoes would automatically get access to users’ personal information.

89. Mr. Soltani told the Committee:

In short, I found that time and time again Facebook allows developers to access personal information of users and their friends, in contrast to their privacy settings and their policy statements. This architecture means that if a bad actor gets a hold of these tokens [...] there is very little the user can do to prevent their information from being accessed. Facebook prioritises these developers over their users.¹⁰⁸

90. As an example of the value Facebook’s customers placed on access to friends data, there is a long internal Facebook discussion in the documents we have published—again, dating back to 2013—around the Royal Bank of Canada’s ‘Neko’ spend, alongside whether they should also be whitelisted. ‘Neko’ was Facebook’s internal name for its new mobile advertising product, Mobile App Install Ads.

91. In an email from Sachin Monga at Facebook to Jackie Chang at Facebook, on 20 August 2013, at 10.38am, the negative impact of the platform changes on Royal Bank of Canada was discussed: “Without the ability to access non-app friends, the Messages API becomes drastically less useful”.

106 [Exhibit 93](#) - not published yet

107 ‘Gks’ and ‘Sitevars’ refer to internal Facebook terms. (own emphasis added).

108 [Q4327](#)

92. In reply, minutes later, Sachin Monga wrote back:

What would be really helpful for us is if you can provide the below details first:

2/ did they sign an extended api agreement when you whitelisted them for this api?

3/ who internally gave you approval to extend them whitelist access? Can you send me email or permalink from the Platform Whitelist Approval Group.

4/ Is there budget tied specifically to this integration? How much? We need the above info foremost and we understand the context below.'

93. The next email was from Sachin Monga to Jackie Chang, 10.58am, 20 August 2013:

Thanks for the quick response. Answers below:

2/ They did not sign an extended API agreement. Should they have? I didn't know about this...

3/ Doug gave the approval...

4/ There is budget tied specifically to this app update (all mobile app install ads to existing RBC customers, via custom audiences). I believe it will be one of the biggest neko campaigns ever run in Canada.¹⁰⁹

94. The internal discussions about Royal Bank of Canada continued into the autumn, citing precedents Facebook had already used in its whitelisting extended access process. Simon Cross wrote to Jackie Chang, Sachin Monga, Bryan Hurren (Facebook), 25 October 2013: "+ bryan who recently whitelisted Netflix for the messages API—he will have a better idea of what agreements we need to give them to access to this API". On the same day, Bryan Hurren then responded to Sachin Monga, Jackie Chang and Simon Cross: "From a PR perspective, the story is about the app, not the API, so the fact that it uses Titan isn't a big deal. From a legal perspective, they need an "Extended API agreement" (we used with Netflix) which governs use going forward and should provide us with the freedom to make the changes that Simon mentions below (without being too explicit)". Jackie Chang then wrote to the Facebook group, on 28 October 2013, stating "Bryan—can you take the lead on getting this agreement written up?"

95. These exchanges about just one major country customer, the Royal Bank of Canada, demonstrate the interlinkages between the value of access to friends' data to advertising spending, and Facebook's preferential whitelisting process, which we now consider further.

The linking of data access with spending on advertising at Facebook

96. From the Six4Three case documents, it is clear that spending substantial sums with Facebook, as a condition of maintaining preferential access to personal data, was part and parcel of the company's strategy of platform development as it embraced the mobile advertising world. And that this approach was driven from the highest level.

109 [Exhibit 83](#)

97. Included in the documents is an email between Mike Vernal, then Vice-President of Search, Local, and Developer Products at Facebook, and Mark Zuckerberg, Chris Daniels, Dan Rose, and Douglas Pardy, dated 7 October 2012. It discusses the link of data with revenue:

Mark Zuckerberg:

I've been thinking about platform business model a lot this weekend [...] if we make it so devs can generate revenue for us in different ways, then it makes it more acceptable for us to charge them quite a bit more for using platform. The basic idea is that any other revenue you generate for us earns you a credit towards whatever fees you own us for using platform. For most developers this would probably cover cost completely. So instead of everyone paying us directly, they'd just use our payments or ads products.

A basic model could be:

- Login with Facebook is always free;
- Pushing content to Facebook is always free;
- Reading anything, including friends, costs a lot of money. Perhaps on the order of \$0.10/user each year.

For the money that you owe, you can cover it in any of the following ways:

- Buys ads from us in neko or another system;
- Run our ads in your app or website (canvas apps already do this; Use our payments;
- Sell your items in our Karma store.

Or if the revenue we get from those doesn't add up to more than the fees you owe us, then you just pay us the fee directly.¹¹⁰

98. On 27 October 2012, Mark Zuckerberg sent an internal email to Sam Lessin, discussing linking data to revenue, highlighting the fact that users' data was valuable and that he was sceptical about the risk of such data leaking from developer to developer, which is, of course, exactly what happened during the Cambridge Analytica scandal. The following quotation illustrates this:

There's a big question on where we get the revenue from. Do we make it easy for devs to use our payments/ad network but not require them? Do we require them? Do we just charge a rev share directly and let devs who use them get a credit against what they owe us? It's not at all clear to me here that we have a model that will actually make us the revenue we want at scale.

I'm getting more on board with locking down some parts of platform, including friends data and potentially email addresses for mobile apps.

'I'm generally sceptical that there is as much data leak strategic risk as you think. I agree there is clear risk on the advertiser side, but I haven't figured out how that connects to the rest of the platform. **I think we leak info to developers, but I just can't think if any instances where that data has leaked from developer to developer and caused a real issue for us.** Do you have examples of this?¹¹¹

[...]

Without limiting distribution or access to friends who use this app, I don't think we have any way to get developers to pay us at all besides offering payments and ad networks.¹¹²

99. By the following year, Facebook's new approach, accompanying the launch of Neko in the mobile advertising world was clearly paying off handsomely. An email exchange on 20 June 2013 from Sam Lessin to Deborah Lin, copying in Mike Vernal and Douglas Purdy, shows the rapid growth of revenues from Neko advertising: "The nekk [sic.] growth is just freaking awesome. Completely exceeding my expectations re what is possible re ramping up paid products".¹¹³

100. By the autumn of 2013, at least, the substantial revenue link from Facebook customers to gain preferential access to personal data was set in stone. The following internal Facebook email from Konstantinos Papamiltiadis to Ime Archibong, on 18 September 2013, discussed slides prepared for a talk to the 'DevOps' the following day, highlighting the need for app developers to spend \$250,000 per year to maintain access to their current Facebook data: "Key points: 1/ Find out what other apps like Refresh are out that we don't want to share data with and figure out if they spend on NEKO. Communicate in one-go to all apps that don't spend that those permission will be revoked. Communicate to the rest that they need to spend on NEKO \$250k a year to maintain access to the data".¹¹⁴

101. The Six4Three documents also show that Facebook not only considered hard cash as a condition of preferential access, but also app developers' property, such as tradenames. For example, the term 'Moments' was already protected by Tinder. This email from 11 March 2015 highlights a discussion about giving Tinder whitelisted access to restricted APIs in return for Facebook using the term 'Moments':

I was not sure there was not a question about compensation, apologies; in my mind we have been working collaboratively with Sean and the team in good faith for the past 16 or so months. He's a member of a trusted group of advisers for our platform (Developer Advisory Board) and based on our commitment to provide a great and safe experience for the Tinder users, we have developed two new APIs that effectively allow Tinder to maintain parity of the product in the new API world.¹¹⁵

111 Our emphasis added.

112 [Exhibit 38](#)

113 [Exhibit 158](#)

114 [Exhibit 79](#)

115 [Exhibit 97](#)

Another email from Konstantinos Papamiltiadis to Tinder sent the next day states: “We have been working with Sean and his team in true partnership spirit all this time, delivering value that we think is far greater than this trademark.” Facebook then launched a photo-sharing app under the name of ‘Moments’ in June 2015.¹¹⁶

102. We discuss, under ‘Facebook’s targeting of competition’ at the end of this Chapter, more examples of Facebook’s use of its position in the social media world to enhance its dominance and the issues this raises for the public, the industry and regulators alike.

Facebook’s sharing of data with developers

103. ‘Data reciprocity’ is the exchange of data between Facebook and apps, and then allowing the apps’ users to share their data with Facebook. As Ashkan Soltani told us, Facebook’s business model is “to monetise data”,¹¹⁷ which evolved into Facebook paying app developers to build apps, using the personal information of Facebook’s users. To Mr Soltani, Facebook was and is still making the following invitation: “Developers, please come and spend your engineering hours and time in exchange for access to user data”.¹¹⁸

104. Data reciprocity between Facebook and app developers was a central feature in the discussions about the re-launch of its platform. The following email exchange on 30 October 2012 highlights this issue:

Mike Vernal: On Data Reciprocity—in practice I think this will be one of those rights that we reserve. [...] We’ll pay closest attention to strategic partners where we want to make sure the value exchange is reciprocal.

Greg Schechter: Seems like Data Reciprocity is going to require a new level of subjective evaluation of apps that our platform ops folks will need to step up to—evaluating whether the reciprocity UI/action importers are sufficiently reciprocal.’

Mike Vernal: As many of you know, we’ve been having a series of conversations w/Mark for months about the Platform Business Model. [...] We are going to require that all platform partners agree to data reciprocity. If you access a certain type of data (e.g. music listens), you must allow the user to publish back that same kind of data. Users must be able to easily turn this on both within your own app as well as from Facebook (via action importers).¹¹⁹

105. Mark Zuckerberg wrote a long email entitled “Platform Model Thoughts,” sent on 19 November 2012 to senior executives Sheryl Sandberg, Mark Vernal, Douglas Purdy, Javier Olivan, Alex Schultz, Ed Baker, Chris Cox, Mike Schroepfer (who gave evidence to the DCMS Committee in April 2018), Dan Rose, Chris Daniels, David Ebersman, Vladimir Fedrov, Cory Ondrejka and Greg Badros. He discusses the concept of reciprocity and data value, and also refers to “pulling non-app friends out of friends.get”, thereby prioritising developer access to data from users who had not granted data permission to the developer:

116 [Introducing Moments: a private way to share photos with friends](#), Facebook newsroom, 15 June 2015.

117 [Q4358](#)

118 [Q4327](#)

119 [Exhibit 45](#)

After thinking about platform business for a long time, I wanted to send out a note explaining where I'm leaning on this. This isn't final and we'll have a chance to discuss this in person before we decide this for sure, but since this is complex, I wanted to write out my thoughts. This is long, but hopefully helpful.

The quick summary is that I think we should go with full reciprocity and access to app friends for no charge. Full reciprocity means that apps are required to give any user who connects to FB a prominent option to share all of their social content within that service back [...]to Facebook.

[...]

We're trying to enable people to share everything they want, and to do it on Facebook. Sometimes the best way to enable people to share something is to have a developer build a special purpose app or network for that type of content and to make that app social by having Facebook plug into it. **However, that may be good for the world but it's not good for us unless people also share back to Facebook and that content increases the value of our network.**¹²⁰ So ultimately, I think the purpose of platform—even the read side—is to increase sharing back into Facebook.'

[...]

It seems like we need some way to fast app switch to the FB app to show a dialog on our side that lets you select which of your friends you want to invite to an app. We need to make sure this experience actually is possible to build and make as good as we want, especially on iOS where we're more constrained. We also need to figure out how we're going to charge for it. **I want to make sure this is explicitly tied to pulling non-app friends out of friends.get.**¹²¹ (friends information)

[...]

What I'm assuming we'll do here is have a few basic thresholds of API usage and once you pass a threshold you either need to pay us some fixed amount to get to the next threshold or you get rate limited at the lower threshold.

[...]

Overall, I feel good about this direction. The purpose of platform is to tie the universe of all the social apps together so we can enable a lot more sharing and still remain the central social hub. **I think this finds the right balance between ubiquity, reciprocity and profit.**¹²² On 19 November 2012, Sheryl Sandberg replied to this email from Mark Zuckerberg, stating, "I like full reciprocity and this is the heart of why".¹²³

120 Our emphasis added.

121 Our emphasis added.

122 [Exhibit 48](#) (Our emphasis added).

123 [Exhibit 48](#)

106. The use of 'reciprocity' highlights the outlook and the business model of Facebook. 'Reciprocity' agreements with certain apps enabled Facebook to gain as much information as possible, by requiring apps that used data from Facebook to allow their users to share of their data back to Facebook (with scant regard to users' privacy). Facebook's business interests were and are based on balancing the needs of developers to work with Facebook by giving them access to users' data, while supposedly protecting users' privacy. By logging into an app such as Tinder, for instance, the user would not have realised they were giving away all their information on Facebook. Facebook's business interest is to gather as much information from users as possible, both directly and from app developers on the Platform.

Facebook collecting data from Android customers

107. Paul-Olivier Dehaye and Christopher Wylie described the way in which the Facebook app collects users' data from other apps on Android phones.¹²⁴ In fact, Facebook's was one of millions of Android apps having potential access to users' calls and messages in the Android operating system, dating back to 2008.¹²⁵ The Six4Three documents reveal discussions about how Facebook could obtain such information. Facebook knew that the changes to its policies on the Android mobile phone system, which enabled the Facebook app to collect a record of calls and texts sent by the user, would be controversial. To mitigate any bad PR, Facebook planned to make it as hard of possible for users to know that this was one of the underlying features of the upgrade of their app.

108. The following email exchange, sent on 4 February 2015, from Michael LeBeau to colleagues, highlight the changing of 'read call log' permissions on Android and a disregard for users' privacy:

Michael LeBeau – 'Hi guys, as you know all the growth team is planning on shipping a permissions update on Android at the end of this month. They are going to include the 'read call log' permission, which will trigger the Android permissions dialog on update, requiring users to accept the update. They will then provide an in-app opt in NUX for a feature that lets you continuously upload your SMS and call log history to Facebook to be used for improving things like PYMK, coefficient calculation, feed ranking etc. **This is a pretty high-risk thing to do from a PR perspective but it appears that the growth team will charge ahead and do it.**¹²⁶

109. On 25 March 2018, Facebook issued a statement about the logging of people's call and text history, without their permission:

Call and text history logging is part of an opt-in feature for people using Messenger or Facebook Lite on Android. This helps you find and stay connected with the people you care about, and provides you with a better experience across Facebook. [...] Contact importers are fairly common among social apps and services as a way to more easily find the people you want to connect with.¹²⁷

124 [Q1396](#)

125 As of October 2017, there were 3.3 million apps, [statista.com](http://www.statista.com).

126 Footnote needed (our emphasis added).

127 [Exhibit 172](#)

This positive spin on the logging of people's data may have been accurate, but it failed to highlight the huge financial advantage to Facebook of collecting extensive data from its users' daily interactions.

Facebook's monitoring of app usage

110. Onavo was an Israeli company that built a VPN app, which could hide users' IP addresses so that third parties could not track the websites or apps used. Facebook bought Onavo in 2013, promoting it to customers "to keep you and your data safe when you go online by blocking potentially harmful websites and securing your personal information".¹²⁸ However, Facebook used Onavo to collect app usage data from its customers to assess not only how many people had downloaded apps, but how often they used them. This fact was included in the 'Read More' button in the App Store description of Onavo: "Onavo collects your mobile data traffic [...] Because we're part of Facebook, we also use this info to improve Facebook products and services, **gain insights into the products and services people value, and build better experiences**".¹²⁹

111. This knowledge helped them to decide which companies were performing well and therefore gave them invaluable data on possible competitors. They could then acquire those companies, or shut down those they judged to be a threat. Facebook acquired and used this app, giving the impression that users had greater privacy, when in fact it was being used by Facebook to spy on those users.¹³⁰

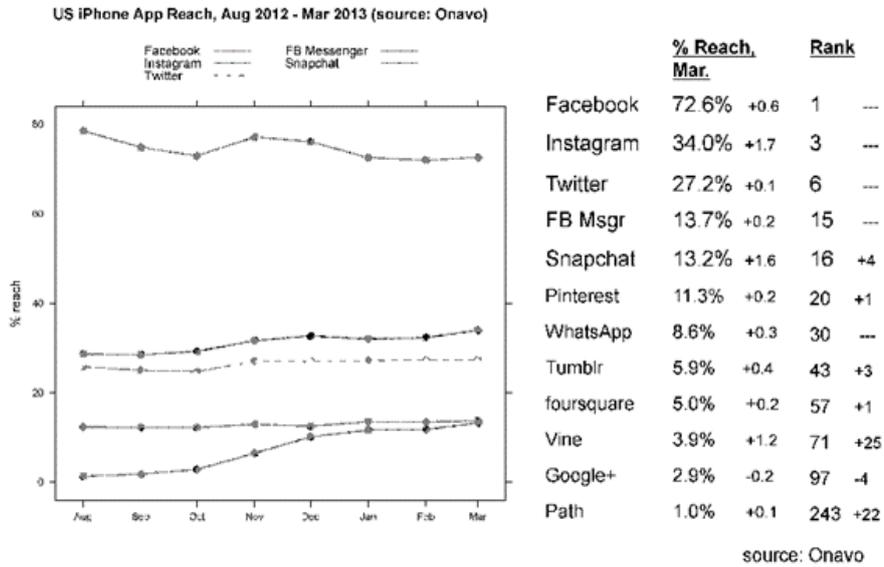
112. The following slides are from a presentation, titled "Industry Update", given on 26 April 2013, showing market analysis driven by Onavo data, comparing data about apps on users' phones and mining that data to analyse Facebook's competitors.

113. The following slide illustrates statistics collected from different popular apps, such as Vine, Twitter, Path and Tumblr:

128 Onavo promotional information.

129 [People are furious about Onavo, a Facebook-owned VPN that sends your app usage habits back to Facebook](#), Rachel Sandler, Business Insider, 14 February 2018 (our emphasis added)

130 [Apple removed Facebook's Onavo from the App Store for gathering app data](#), Taylor Hatmaker Techcrunch.com, 22 August 2018.



HIGHLY CONFIDENTIAL

FB-01367813

“Industry Update” Facebook presentation, given on 26 April 2013

114. In August 2018, Apple discovered that Facebook had breached its terms and conditions and removed Onavo from its App Store, stating:

We work hard to protect user privacy and data security throughout the Apple ecosystem. With the latest update to our guidelines, we made it explicitly clear that apps should not collect information about which other apps are installed on a user’s device for the purposes of analytics or advertising/marketing and must make it clear what user data will be collected and how it will be used.¹³¹

115. Since 2016, Facebook has undertaken similar practices in relation to its ‘Facebook Research’ app, which violated Apple’s rules surrounding the internal distribution of apps within an organisation. Facebook secretly paid users, aged between 13 and 25, up to \$20 in gift cards per month to sell their phone and website activity, by installing the Android ‘Facebook Research’ app. Apple blocked Facebook’s Research app in January 2019, when it realised that Facebook had violated Apple’s terms and conditions. The app will continue, however, to run on Android.¹³² An Apple spokesman stated:

Facebook has been using their membership to distribute a data-collecting app to consumers, which is a clear breach of their agreement with Apple. Any developer using their enterprise certificates to distribute apps to consumers will have their certificates revoked, which is what we did in this case to protect our users and their data.¹³³

131 [Facebook pulls Onavo Protect from App store after Apple finds it violates privacy policy, Mikey Campbell, appleinsider, 22 August 2018.](#)

132 [Facebook pays teens to install VPM that spied on them, Josh Constine, Techncrunch.com, 29 January 2019.](#)

133 [Apple banned Facebook app that spied on kids as young as 13, Charlotte Henry, the Mac Observer, 30 January, 2019.](#)

Facebook targeting competitor apps

116. Since inception, Facebook has made multiple acquisitions, including Instagram in 2012 and WhatsApp in 2014. The Six4Three files show evidence of Facebook taking aggressive positions against certain apps, especially against direct competitors, which resulted in their being denied access to data. This inevitably led to the failure of those businesses, including Six4Three. An email sent on 24 January 2013 from Justin Osofsky to Mike Vernal, Mark Zuckerberg, Kevin Systrom, Douglas Purdy and Dan Rose describes the targeting of Twitter's Vine app, a direct competitor to Instagram, by shutting down its use of Facebook's Friends API:

Justin Osofsky – **Twitter launched Vine today** which lets you shoot multiple short video segments to make one single, 6-second video. As part of their NUX,¹³⁴ you can find friends via FB. **Unless anyone raises objections, we will shut down their friends API access today.** We've prepared reactive PR, and I will let Jana know our decision.

MZ – **Yup, go for it.**¹³⁵

117. Instagram Video, also created in 2013, enabled users to upload 15-second videos to their profile. From the email exchange above, it is clear that Mark Zuckerberg personally approved the decision to deny access to data for Vine. In October 2016, Vine announced that Twitter would be discontinuing the Vine mobile app, in part due to the fact that they could not grow their user base.¹³⁶ On the same day that we published the Six4Three documents in December 2018, the co-founder of Vine, Rus Yusupov, tweeted "I remember that day like it was yesterday".¹³⁷

Facebook's response to the publication of the Six4Three documents

118. We published a small proportion of the evidence obtained from the Six4Three court case. For over a year, on multiple occasions, Mark Zuckerberg has refused to give evidence to the DCMS Committee. Yet within four hours of the Six4Three evidence being published on the DCMS Committee website, he responded, with the following post on his Facebook page:

This week a British Parliament committee published some internal Facebook emails, which mostly include internal discussions leading up to changes we made to our developer platform to shut down abusive apps in 2014–15. Since these emails were only part of our discussions, I want to share some more context around the decisions that were made.

We launched the Facebook Platform in 2007 with the idea that more apps should be social. For example, your calendar should show your friends' birthdays and your address book should have your friends' photos. Many new companies and great experiences were built on this platform, but at

134 A NUX is a toolkit, used to create user interfaces.

135 [Exhibit 44](#) (our emphasis added).

136 [Mark Zuckerberg gave the order to kneecap Vine, emails show](#), Rachel Kraus, MashableUK, 5 December 2018.

137 Same as above.

the same time, some developers built shady apps that abused people's data. In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the data apps could access.

This change meant that a lot of sketchy apps—like the quiz app that sold data to Cambridge Analytica—could no longer operate on our platform. Some of the developers whose sketchy apps were kicked off our platform sued us to reverse the change and give them more access to people's data. We're confident this change was the right thing to do and that we'll win these lawsuits.¹³⁸

119. The “sketchy apps” that Mr Zuckerberg referred to—‘the quiz app that sold data to Cambridge Analytica’—was the ‘thisisyourdigitallife’ app, owned by GSR, which brings us back full circle to the starting point of our inquiries into the corporate methods and practices of Facebook.

120. One of the co-founders of GSR was Joseph Chancellor, who was employed, until recently, at Facebook, as a quantitative researcher on the User Experience Research team, only two months after leaving GSR. Facebook has provided us with no explanation for its recruitment of Mr Chancellor, after what Facebook now presents as a very serious breach of its terms and conditions. We believe the truth of the matter is contained in the evidence of Mr Chancellor's co-founder Aleksandr Kogan.

121. When Richard Allan was asked why Joseph Chancellor was employed by Facebook, he replied that “Mr. Chancellor, as I understand it, is somebody who had a track record as an academic working on relevant areas”. He acknowledged that Mr Chancellor was involved with the source of the breach to Cambridge Analytica and that Facebook had not had any action taken against him.¹³⁹

122. When Aleksandr Kogan gave evidence to the DCMS Committee in April 2018, he was asked why Joseph Chancellor had been employed by Facebook, given the circumstances of his involvement with GSR. As to whether it seemed strange, Dr Kogan replied: “The reason I don't think it's odd is because, in my view, Facebook's comments are PR crisis mode. I don't believe they actually think these things, because I think they realise that the platform has been mined left and right by thousands of others”.¹⁴⁰

123. Dr Kogan's interpretation of what happened seems to be supported by the Six4Three evidence. Facebook was violating user privacy because, from the beginning, its Platform had been designed in that way. Facebook fostered a tension between developer access to data and user privacy; it designed its Platform to apply privacy settings for Facebook apps only, but applied different and varying settings for data passed through the Platform's APIs. For example, an email exchange between Mr Papamiltiadis and colleagues reveal that over 40,000 apps that had requested access to APIs were categorised based on: those that may cause negative press; those providing strategic value, by driving value to

138 Mark Zuckerberg post on Facebook, around 6.30pm, accessed 7.40pm, 5 December 2018.

139 [Qs 4144–4149](#)

140 Dr Kogan's evidence, requested by Ian Lucas MP, in the 'International Grand Committee' oral evidence session, [Q4152](#).

Facebook; those that are competitive, driving little value to Facebook; and those that will cause a business disruption. Mr. Lessin responds that all lifestyle apps should have their access removed “because we are ultimately competitive with all of them”.¹⁴¹

124. Another document supplied to the committee by Six4Three shows concerns being raised by Facebook staff in 2011 about apps being removed from the platform that were not necessarily ‘spammy’ or ‘sketchy’ to use Mark Zuckerberg’s terminology. In an internal email Mike Vernal from Facebook wrote that “It’s very, very bad when we disable a legitimate application. It erodes trust in the platform, because it makes developers think that their entire business could disappear at any second.”¹⁴² This is indeed the grievance that developers have tried to take up against Facebook and is at the heart of Six4Three’s complaint against the company.

125. Facebook has continually hidden behind obfuscation. The sealed documents contained internal emails, revealing the fact that Facebook’s profit comes before anything else. When they are exposed, Facebook “is always sorry, they are always on a journey”, as Charlie Angus, MP (Vice-Chair of the Canadian Standing Committee on Access to Information, Privacy and Ethics, and member of the ‘International Grand Committee’) described them.¹⁴³ Facebook continues to choose profit over data security, taking risks in order to prioritise their aim of making money from user data.

Facebook’s business model and further challenges for regulators

126. Facebook has recently turned 15 years old, which makes it a relatively young company. What started as a seemingly innocuous way of sharing information with friends and family has turned into a global phenomenon, influencing political events. Theresa Hong, a member of the Trump digital election campaign described ‘Project Alamo’, which involved staff working for the then presidential candidate Donald Trump, Cambridge Analytica staff and Facebook staff all working together with the Cambridge Analytica data sets, targeting specific states and specific voters. The project spent \$85 million on Facebook adverts and Ms Hong said that “without Facebook we wouldn’t have won”.¹⁴⁴

127. Facebook has grown exponentially, buying up competitors such as WhatsApp and Instagram. As Charlie Angus said to Richard Allan: “Facebook has broken so much trust that to allow you to simply gobble up every form of competition is probably not in the public interest. [...] The problem is the unprecedented economic control of every form of social discourse and communication by Facebook”.¹⁴⁵

128. In portraying itself as a free service, Facebook gives only half the story. As Ashkan Soltani, former Chief Technologist to the Federal Trade Commission of the United States of America, told us:

141 [Exhibit 75](#)

142 [Exhibit 19](#).

143 [Q4131](#)

144 [@Stephaniefishm4 Tweet](#), 21 August 2017.

145 [Q4273](#)

It is either free—there is an exchange of information that is non-monetary— or it is an exchange of personal information that is given to the platform, mined, and then resold to or reused by third-party developers to develop apps, or resold to advertisers to advertise with.¹⁴⁶

129. The documents that we received highlighted the fact that Facebook wanted to maximise revenues at all cost, and in doing so favoured those app developers who were willing to pay a lot of money for adverts and targeted those apps that were in direct or potential future competition—and in certain notable instances acquired them.

130. Facebook's behaviour clearly poses challenges for competition regulators. A joint HM Treasury and Department for Business, Energy and Industrial Strategy (BEIS) initiative has commissioned an expert panel, chaired by Professor Jason Furman, to consider the potential opportunities and challenges that the digital economy may pose for competition and pro-competition policy, and to make recommendations on any changes needed. The consultation period ended in early December 2018, and the panel is due to report in early 2019. We hope it will consider the evidence we have taken.

131. Since our publication of a selection of the Six4Three case documents, they have clearly been available to regulators, including the UK's Information Commissioner and the US Federal Trade Commission to assist in their ongoing work. In March 2018, following the revelations over Cambridge Analytica, the FTC said it was launching a further investigation into Facebook's data practices, the outcome of which—including the possibility of substantial fines—is still awaited.

132. When asked whether it was fair to think of Facebook as possibly falling foul of the US Racketeer Influenced and Corrupt Organisations Act, in its alleged conspiracy to damage others' businesses, Richard Allan disagreed, describing the company as “a group of people who I have worked with closely over many years who want to build a successful business”.¹⁴⁷ We received evidence that showed that Facebook not only targeted developers to increase revenue, but also sought to switch off apps where it considered them to be in competition or operating in a lucrative areas of its platform and vulnerable to takeover. Since 1970, the US has possessed high-profile federal legislation, the Racketeer Influenced and Corrupt Organizations Act (RICO); and many individual states have since adopted similar laws. Originally aimed at tackling organised crime syndicates, it has also been used in business cases and has provisions for civil action for damages in RICO-covered offences.

133. We believe that Mark Zuckerberg's response to the publication of the Six4Three evidence was, similarly, to use Dr. Kogan's description, “PR crisis mode”. Far from Facebook acting against “sketchy” or “abusive” apps, of which action it has produced no evidence at all, it, in fact, worked with such apps as an intrinsic part of its business model. This explains why it recruited the people who created them, such as Joseph Chancellor. Nothing in Facebook's actions supports the statements of Mark Zuckerberg who, we believe, lapsed into “PR crisis mode”, when its real business model was exposed. This is just one example of the bad faith which we believe justifies governments holding a business such as Facebook at arms' length. It seems clear to us that Facebook acts only when serious breaches become public. This is what happened in 2015 and 2018.

146 [Q4370](#)

147 [Q4213](#)

134. Despite specific requests, Facebook has not provided us with one example of a business excluded from its platform because of serious data breaches. We believe that is because it only ever takes action when breaches become public. We consider that data transfer for value is Facebook's business model and that Mark Zuckerberg's statement that "we've never sold anyone's data" is simply untrue."

135. **The evidence that we obtained from the Six4Three court documents indicates that Facebook was willing to override its users' privacy settings in order to transfer data to some app developers, to charge high prices in advertising to some developers, for the exchange of that data, and to starve some developers—such as Six4Three—of that data, thereby causing them to lose their business. It seems clear that Facebook was, at the very least, in violation of its Federal Trade Commission settlement.**

136. *The Information Commissioner told the Committee that Facebook needs to significantly change its business model and its practices to maintain trust. From the documents we received from Six4Three, it is evident that Facebook intentionally and knowingly violated both data privacy and anti-competition laws. The ICO should carry out a detailed investigation into the practices of the Facebook Platform, its use of users' and users' friends' data, and the use of 'reciprocity' of the sharing of data.*

137. Ireland is the lead authority for Facebook, under GDPR, and we hope that these documents will provide useful evidence for Helen Dixon, the Irish Data Protection Commissioner, in her current investigations into the way in which Facebook targeted, monitored, and monetised its users.

138. *In our Interim Report, we stated that the dominance of a handful of powerful tech companies has resulted in their behaving as if they were monopolies in their specific area, and that there are considerations around the data on which those services are based. Facebook, in particular, is unwilling to be accountable to regulators around the world. The Government should consider the impact of such monopolies on the political world and on democracy.*

139. *The Competitions and Market Authority (CMA) should conduct a comprehensive audit of the operation of the advertising market on social media. The Committee made this recommendation its interim report, and we are pleased that it has also been supported in the independent Cairncross Report commissioned by the government and published in February 2019. Given the contents of the Six4Three documents that we have published, it should also investigate whether Facebook specifically has been involved in any anti-competitive practices and conduct a review of Facebook's business practices towards other developers, to decide whether Facebook is unfairly using its dominant market position in social media to decide which businesses should succeed or fail. We hope that the Government will include these considerations when it reviews the UK's competition powers in April 2019, as stated in the Government response to our Interim Report. Companies like Facebook should not be allowed to behave like 'digital gangsters' in the online world, considering themselves to be ahead of and beyond the law.*

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

140. Our Interim Report highlighted the methods by which Arron Banks campaigned during the Referendum, which, in his own words, involved creating 'bush fires' and then "putting a big fan on and making the fan blow".¹⁴⁸ He described the issue of immigration as one that set "the wild fires burning".¹⁴⁹ Evidence we received indicated that data had been shared between the Leave.EU campaign—with its strapline of 'leaving the EU out of the UK'¹⁵⁰—and Arron Banks' insurance company, Eldon Insurance Ltd.¹⁵¹ When we asked Mr Banks whether staff from Eldon Insurance had also worked on campaigning for LeaveEU, Mr Banks responded that such an allegation was "a flat lie".¹⁵²

141. The allegation of the sharing of people's data during a referendum campaign is a matter both for the Information Commissioner's Office (as it relates to the alleged unauthorised sharing of data, in contravention of the Privacy and Electronic Communication Regulations 2003)¹⁵³ and for the Electoral Commission (as it relates to alleged breaches of rules relating to spending limits during a referendum).

142. Since we published our Interim Report, the ICO published the findings of its investigations into these issues.¹⁵⁴ Its report states that Leave.EU and Eldon Insurance are closely linked, with both organisations sharing at least three directors, with further sharing of employees and projects.¹⁵⁵ The ICO found evidence to show that Eldon Insurance customers' personal data, in the form of email addresses, was accessed by staff working for Leave.EU and was used unlawfully to send political marketing messages:

- Leave.EU sent 1,069,852 emails to subscribers who had consented to receive email information from Leave.EU between 25 February and 31 July 2017, but which also included marketing for GoSkippy services and a discount offer for Leave.EU supporters, for which Leave.EU did not have consent; and
- Leave.EU sent a single email to over 49,000 email addresses on 23 August 2016, announcing a 'sponsorship' deal with GoSkippy.¹⁵⁶

143. The ICO's report highlighted its notice of intent to fine the following companies:

- Both Leave.EU and Eldon Insurance (trading as GoSkippy) £60,000 each for serious breaches of the Privacy and Electronic Communications Regulations (PECR) 2003; and

148 [Q3609](#)

149 [Q3609](#)

150 [Leave.EU website](#), accessed 29 November 2018.

151 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, paras 151 to 159.

152 [Q3619](#)

153 As above, para 155.

154 [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018.

155 As above, p45.

156 [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018, p47.

- Leave.EU £15,000 for a separate breach of PECR regulation 22, after almost 300,000 emails were sent to Eldon Insurance customers that contained a Leave.EU newsletter.¹⁵⁷

144. The Information Commissioner gave evidence to us on the day of publication of her report, and described to us the “failure to keep separate the data of insurance clients of Eldon and marketing and messaging to potential supporters and voters and Leave.EU data. We have issued notices of intent under the electronic marketing regulation, but also our work on the data protection side, to look deeply into the policies or the disregard for separation of the data. That is going to be looked at through an audit”.¹⁵⁸ The ICO issued a preliminary enforcement notice on Eldon Insurance, requiring immediate action to ensure that the company is compliant with data protection law.¹⁵⁹

145. On 1 February 2019, after considering the companies’ representations, the ICO issued the fines, confirming a change to one amount, with the other two remaining unchanged (the fine for Leave.EU’s marketing campaign was £15,000 less than the ICO’s original notice of intention). The Information Commissioner has also issued two assessment notices to Leave.EU and Eldon Insurance, to inform both organisations that they will be audited.¹⁶⁰

146. From the evidence we received, which has been supported by the findings of both the ICO and the Electoral Commission, it is clear that a porous relationship existed between Eldon Insurance and Leave.EU, with staff and data from one organisation augmenting the work of the other. There was no attempt to create a strict division between the two organisations, in breach of current laws. We look forward to hearing the findings of the ICO’s audits into the two organisations.

147. As set out in our Interim Report, Arron Banks and Andy Wigmore showed complete disregard and disdain for the parliamentary process when they appeared before us in June 2018. It is now evident that they gave misleading evidence to us, too, about the working relationship between Eldon Insurance and Leave.EU. They are individuals, clearly, who have less than a passing regard for the truth.

157 As above, p9.

158 [Q3894](#)

159 ICO Report, p47.

160 [ICO to audit data protection practices at Leave.EU and Eldon Insurance after fining both companies for unlawful marketing messages](#), ICO, 1 February 2019.

4 Aggregate IQ

Introduction

148. Aggregate IQ is a Canadian digital advertising web and software development company incorporated in 2012 by its owners Jeff Silvester and Zack Massingham. Jeff Silvester told us that he had known Christopher Wylie, the Cambridge Analytica whistleblower, since 2005, and met Alexander Nix, the then SCO of Cambridge Analytica, “around the beginning of 2014.”¹⁶¹

149. AIQ worked for SCL to “create a political customer relationship management software tool” for the Trinidad and Tobago election campaign in 2014, and then went on to develop a software tool—the Ripon tool—commissioned and owned by SCL.¹⁶² According to the ICO, in early 2014, SCL Elections approached AIQ to “help it build a new political Customer Relations Management (CRM) tool for use during the American 2014 midterm elections”.¹⁶³ The AIQ repository files contain a substantial amount of development work, with vast amounts of personal data, in plain text, of the residents of Trinidad and Tobago.

150. The Ripon tool was described by Jeff Silvester as “a political customer relationship management tool focused on the US market”¹⁶⁴ and it was described by Christopher Wylie as “the software that utilised the algorithms from the Facebook data”.¹⁶⁵ As a result of developing the Ripon tool, so that voters could be sent micro-targetted adverts, AIQ also worked on political campaigns in the US.¹⁶⁶ This work was still ongoing when they also got involved in Brexit-related campaigns in the UK’s EU Referendum. According to Facebook, “AIQ ran 1,390 ads on behalf of the pages linked to the referendum campaign between February 2016 and 23 June 2016 inclusive”.¹⁶⁷

151. Chris Vickery, Director, Cyber Risk Research, at the UpGuard consultancy, works as a data breach hunter, locating exposed data and finding common threads. After *The Observer*, Channel 4 and *New York Times* coverage of Cambridge Analytica (and associated companies), Upguard published four papers that explained connections between AIQ, Cambridge Analytica, and SCL, and AIQ’s work during the UK Referendum.¹⁶⁸ These papers were based on the data that Chris Vickery had found through the insecure AIQ website. When he appeared before the Committee, he presented Gitlab¹⁶⁹ data containing over 20,000 folders and 113,000 files, which he had downloaded from the insecure AIQ website.¹⁷⁰ The Committee has made the full data set available to the ICO.

161 [Q2765](#) and [Q2771](#)

162 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 117.

163 [Investigation into the use of data analytics in political campaigns](#), A report to Parliament, ICO, 6 November 2018.

164 [Q2776](#)

165 [Q1299](#)

166 [Q2784](#). As we said in para 110 of the Interim Report, 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.

167 [Letter from Rebecca Stimson, Facebook to Louise Edwards, The Electoral Commission](#), 14 May 2018, p1.

168 The Aggregate IQ Files: [Part one: How a political engineering firm exposed their code base](#), UpGuard, 30 April 2018; [Part two: The Brexit Connection](#), UpGuard, 30 April 2018; [Part three: A Monarch, a Peasant, and a Saga](#), 30 April 2018; [Part Four: Northwest passage](#), 1 November 2018

169 Gitlab is an online platform on which developers write and share code.

170 [Chris Vickery oral evidence session](#), 2 May 2018.

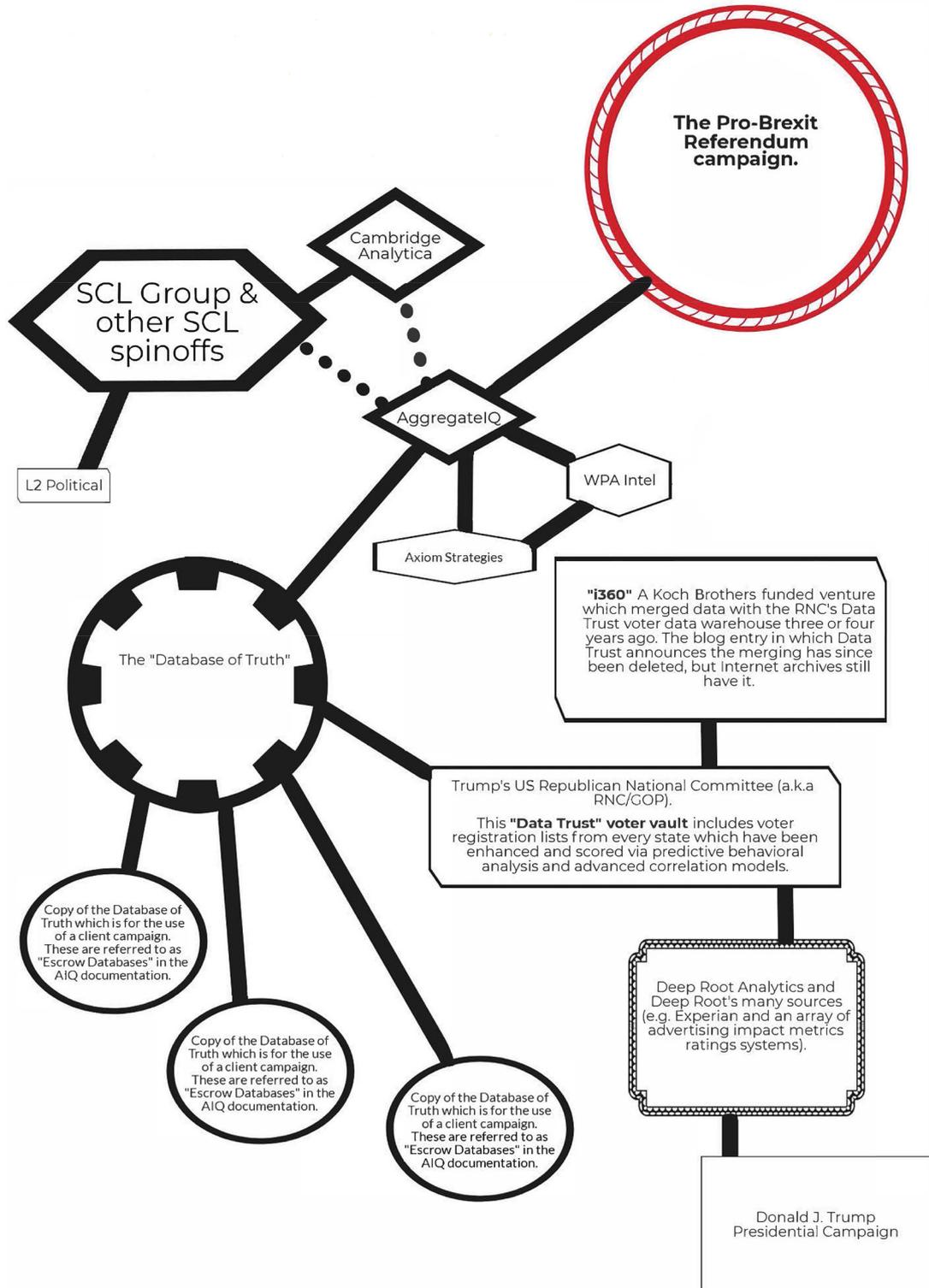
152. Mr Vickery described the evidence that he submitted to the inquiry:

This repository is a set of sophisticated applications, data management programs, advertising trackers, and information databases that collectively could be used to target and influence individuals through a variety of methods, including automated phone calls, emails, political websites, volunteer canvassing, and Facebook ads.¹⁷¹

153. The following chart supplied in evidence by Chris Vickery highlights the relationship that AIQ had between Cambridge Analytica, SCL and other clients. The full list of AIQ-repository-present projects known to involve UK entities is:

- “Client-VoteLeave-Gove”
- “Client-VoteLeave-MyPollingStation”
- “Client-VoteLeave-PlatformSync”
- “Client-DUP-ActionSite”
- “Client-VeteransForBritain-Site”
- “Client-CountrysideAlliance-Action”
- “Client-ChangeBritain-MailSend”
- “Client-ChangeBritain-Site”
- “Client-S8-Action” (Save the 8th)

154. According to Chris Vickery, “the 15 nodes shown below are corroborated with documentation and credible testimony. This is not an exhaustive list of every data gateway and relevant flow, but I do remain confident in stating that this is a reasonable depiction of what has transpired”:¹⁷²



Source: Chris Vickery¹⁷³

172 FKN0125

173 FKN 0125

155. In its July 2018 report, the ICO confirmed that AIQ had access to the personal data of UK voters, given by the Vote Leave campaign, and that AIQ “held UK data that they should not have continued to hold”.¹⁷⁴ This Chapter will explore the AIQ unsecured data discovered by Chris Vickery, studying: the relationship between AIQ, SCL and Cambridge Analytica; the work that AIQ carried out for the EU referendum; and the capabilities that were open to AIQ, by the types of tools that were exposed in the repository. We commissioned the communications agency, 89up,¹⁷⁵ to carry out analysis of this data and have also used the expertise of Chris Vickery in our work.

Relationship between AIQ and SCL/Cambridge Analytica before the UK’s EU referendum

156. According to Jeff Silvester, CEO of AggregateIQ, roughly 80% of AIQ’s revenue came from SCL, from 2013 until mid-2015.¹⁷⁶ It would appear from Chris Vickery’s files that, where AIQ and SCL worked together, staff had mutual access to some of the same databases.¹⁷⁷ Alexander Nix told us that “after they had built the software platform for us, AIQ continued to work with us as consultants, not least to help some of our clients to interface with the product that they had built and to teach them how to use it”.¹⁷⁸

157. In our Interim Report, we described the Ripon software—a political customer relationship management software tool—developed by AIQ, which was commissioned and owned by SCL.¹⁷⁹ The files obtained by Chris Vickery illustrate clear collaboration between Cambridge Analytica and AIQ, with the importing of the original Ripon development project from a Cambridge Analytica-controlled domain to the AIQ repository. AIQ’s involvement with the Ripon software came from a source repository located at “scl.ripon.us”. The domain was registered to the then CEO of Cambridge Analytica, Alexander Nix. The ICO discovered financial transactions and contacts between the organisations, and also concluded that it was purely a contractual relationship:

We found no evidence of unlawful activity in relation to the personal data of UK citizens and AIQ’s work with SCLE. To date, we have no evidence that SCLE [SCL Elections] and CA [Cambridge Analytica] were involved in any data analytics work with the EU Referendum campaigns.¹⁸⁰

158. AIQ’s lawyers, Borden Ladner Gervais, wrote to the Committee to state: “AggregateIQ is not an associated company of Cambridge Analytica, SCL, or any other company for that matter. AggregateIQ is 100% Canadian owned and operated. AggregateIQ wrote software for SCL. AggregateIQ did not manipulate micro-targeting, nor facilitate its manipulation.”¹⁸¹

159. According to the files we obtained, there was certainly data exchanged between both AIQ and SCL, as well as between AIQ and Cambridge Analytica. The repository files include stray ‘debug’ logs, which document the importing of data, including OCEAN

174 [Investigation into data analytics for political purposes: investigation update, ICO, July 2018, p4.](#)

175 [89up website.](#)

176 [Q2964](#)

177 [Q3270](#), Damian Collins MP.

178 [Q3270](#)

179 [Disinformation and ‘fake news’: Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, para 117.

180 As above, p42.

181 [Letter from Borden Ladner Gervais LLP to Damian Collins MP](#), 20 September 2018.

psychographic scores, which Jeff Silvester openly stated, in his second appearance before the Canadian Parliament, had come from Cambridge Analytica and had been used in the AIQ-developed side of the Ripon software.¹⁸² After being asked by Nathaniel Erskine-Smith MP, Vice-Chair of the Canadian Standing Committee on Access to Information, Privacy and Ethics, and member of the 'International Grand Committee', whether AIQ should have exercised more due diligence in taking information from SCL and converting it into advertising and targeting, Jeff Silvester said:

We did ask questions about where it came from, but the information we got was that it was from public data sources, and there are tons of them in the United States. We were unaware they were obtaining information improperly at the time. [...] With respect to everything that's transpired after having worked with SCL, would I do it again? I probably wouldn't.¹⁸³

160. Mr Vickery was able to find AIQ's repository only after a SCL developer left a software script open on his own private Github account.¹⁸⁴ The script file has a header stating that it originated from an AIQ developer. SCL staff had access to AIQ data and the two businesses seemed unusually closely linked. According to Chris Vickery, the available evidence would weigh heavily towards there being more to the AIQ, Cambridge Analytica, SCL relationship than is usually seen in an arm's length relationship.

161. Within the AIQ repository are references to the "The Database of Truth", a system that obtains and integrates data from disparate sources, collating information from hundreds of thousands, and potentially millions, of voters.¹⁸⁵ Some of this came from the RNC database—the Republican National Committee Data Trust is the Republican party's primary voter file provider—and some came from the Ted Cruz campaign. This database can be interrogated using a number of parameters, including, but not limited to: first name, last name, birth year, age, age range, registration address, whether they were Trump supporters and whether they would vote.

162. The full voter data stores were held elsewhere from the code repository, although the repository did include the means through which anyone could have accessed the full voter data stores. The information included in the 'Database of Truth' could have been used to target specific users on Facebook, using its demographic targeting feature when creating adverts on the Facebook platform. According to Chris Vickery, the credentials contained within the 'Database of Truth' could have been used by anyone finding them. In other words, anyone could find exposed passwords on the site and then access millions of individuals' private details.

163. References in the repository explain how the 'Database of Truth' was used by WPAi, a company which describes itself as "a leading provider of political intelligence for campaigns from President to Governor and U.S. Senate to Mayor and City Council in all 50 states and several foreign countries".¹⁸⁶ The repository also shows that WPAi worked with AIQ for the Osnova party in Ukraine.¹⁸⁷ WPAi was described as a partner of AIQ.

182 [Evidence on Tuesday 12 June 2018](#), Standing Committee on access to information, privacy and ethics, Parliament of Canada, Q1045.

183 Same as above.

184 Github is a web-based hosting service.

185 In the repository, there is access to the search results only, so the number of users is unknown.

186 [WPAi website](#), accessed 1 February 2019.

187 The Osnova party will be discussed further in Chapter 7.

164. With detailed information about voters available to AIQ, the company would have been able to create highly targeted ads on Facebook to reach potential voters. More specifically, they would have been able to use this information to target users by: age; gender; location, within a designated one-mile radius (using Facebook's hyperlocal targeting); and race (in 2018, Facebook removed over 5,000 options that could have been used to exclude certain religious and ethnic minority groups).¹⁸⁸

165. Chris Vickery uncovered a "config" file, which illustrated the interplay between AIQ, Cambridge Analytica, and right-wing news website Breitbart, run by the ultra-conservative campaigner Steve Bannon. A config file is a collection of settings that software refers to during execution, in order to fill in variables. It is a file that describes the preferences of the user on how a programme should run, but it can only ask for things that the programme knows how to do. As we said in the Interim Report, Steve Bannon served as White House chief strategist at the start of President Trump's term, having previously served as Chief Executive of Trump's election campaign. He was the Executive Chairman of Breitbart News, a website he described as 'the platform of the alt-right'. He was also the former Vice President of Cambridge Analytica.¹⁸⁹

166. There is clear evidence that there was a close working relationship between Cambridge Analytica, SCL and AIQ. There was certainly a contractual relationship, but we believe that the information revealed from the repository would imply something closer, with data exchanged between both AIQ and SCL, as well as between AIQ and Cambridge Analytica.

AIQ work related to the EU Referendum

167. AIQ carried out online advertising work for Brexit-supporting organisations Vote Leave, Veterans for Britain, Be Leave and DUP Vote to Leave, who all, according to Jeff Silvester, approached AIQ independently of each other.¹⁹⁰ The majority of the adverts—2,529 out of a total of 2,823—were created by AIQ on behalf of Vote Leave.¹⁹¹ The value of this advertising carried out by and paid to AIQ for the Brexit campaigns included:

- £2.9 million for Vote Leave;
- £625,000 for BeLeave;
- £100,000 for Veterans for Britain; and
- £32,000 for the DUP.¹⁹²

168. AIQ written evidence denies the fact that AIQ held individuals' information relating to the EU referendum:

The information accessed by the security researcher is primarily software code, but also included contact information for supporters and voters

188 [Keeping advertising safe and civil](#), Facebook blog post, 21 August 2018.

189 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, para 96.

190 [Q2986](#)

191 [Investigation into the use of data analytics in political campaigns, a report to Parliament](#), 6 November 2018, para 3.6.

192 [Q3000](#)

from a few of our past clients. None of these files contained any individual financial, password or other sensitive information, and none of the personal information came from the Brexit campaign.¹⁹³

169. This concurs with the work of the Federal Office of the Privacy Commissioner of Canada (OPC) and the Office of the Information and Privacy Commissioner of British Columbia (OIPC), which are conducting a joint investigation and, according to the ICO “have not yet made findings. [...] they have advised us that they have not located any UK personal data, other than that identified within the scope of our enforcement notice.”¹⁹⁴

170. We believe that AIQ handled, collected, stored and shared UK citizen data, in the context of their work on the EU referendum. There is an entire AIQ project area—“Brexit Sync”—devoted to synchronising UK and Brexit-relevant data, including personal individuals’ information, from multiple pro-Brexit client entities. The processing scripts contained in the AIQ repository also show that Facebook Account IDs were being harvested and attached to voter profiles for people living in the UK.

171. Mr Vickery told us that:

In the time since my testimony before the Committee, I have located a spreadsheet in the AIQ repository files containing the first name, last name, and email addresses for 1,438 apparently UK citizens. I am making the nationality assumption based upon the email address domain names (examples: yahoo.co.uk, btinternet.com, hotmail.co.uk, sky.com).¹⁹⁵

172. As we stated previously, AIQ used data scraped by Aleksandr Kogan to target voters in the US election. Therefore, AIQ had the capability to email potential voters during the EU referendum and also to target people via Facebook. By uploading the emails to Facebook to a “custom audience”, all the users whose emails were uploaded and matched the emails used to register accounts on Facebook could be precisely targeted via the platform.

173. In response to the Electoral Commission’s request for information concerning Vote Leave, Darren Grimes and Veterans for Britain, Facebook told the Electoral Commission in May 2018 that AIQ had made use of data file custom audiences—enabling AIQ to reach existing customers on Facebook or to reach users on Facebook who were not existing customers—website custom audiences and lookalike audiences.¹⁹⁶ AIQ stated that it was an administrative error, which was quickly corrected.¹⁹⁷

174. Furthermore, Facebook wrote to the Electoral Commission in May 2018, in response to a request for information connected with pro-Brexit campaign groups. The letter states that “SCL Elections is listed as the contact for at least one AIQ Facebook ad account”. The provided email address belongs to an SCL employee.¹⁹⁸ No explanation has been given to why this should be the case.

193 [FKN0086](#)

194 [ICO, p42.](#)

195 Correspondence between the Committee and Chris Vickery, 22 January 2019.

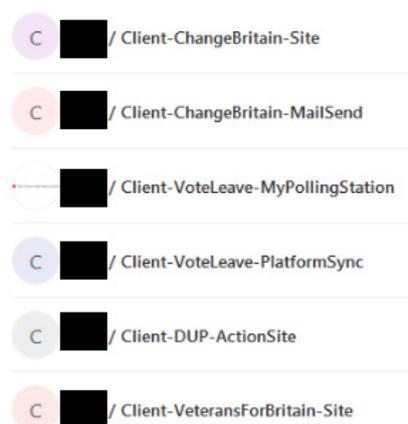
196 Facebook’s explanations of the different custom audiences can be found here: [Letter from Rebecca Stimson, Facebook to Louise Edwards, The Electoral Commission, 14 May 2018, p2.](#)

197 [Letter from Borden Ladner Gervais to the Committee, re testimony of AggregateIQ Data Services Limited before the DCMS Committee, 20 September 2018.](#)

198 [Letter from Rebecca Stimson, Facebook to Louise Edwards, The Electoral Commission, 14 May 2018, p4.](#)

175. James Dipple-Johnstone, Deputy Information Commissioner, told us that the email addresses in the repository “came from other work that the company had done for UK companies and organisations and it had been retained by them following those other contracts that it had”.¹⁹⁹ In July 2018, the ICO confirmed that AIQ had access to the personal data of UK voters, given by the Vote Leave campaign and have established “that [AIQ] hold UK data which they should not continue to hold.”²⁰⁰ This data was discovered in the AIQ Gitlab repository that was presented to the ICO by the Committee. In October 2018, issued an Enforcement Notice, stating that “the Commissioner is satisfied that the controller has failed to comply with Articles 5(1)(a)-(c) and Article 6 of the GDPR”.²⁰¹ Mr Dipple-Johnstone told us that the ICO “have asked them to delete that data as part of the enforcement notice”.²⁰² **AIQ had the capability to use the data scraped by Dr. Kogan. We know that they did this during the US elections in 2014. Dr Kogan’s data also included UK citizens’ data and the question arises whether this was used during the EU referendum. We know from Facebook that data matching Dr Kogan’s was found in the data used by AIQ’s leave campaign audience files. Facebook believe that this is a coincidence, or, in the words of Mike Schroepfer, CTO of Facebook, an “effectively random chance”.²⁰³ It is not known whether the Kogan data was destroyed by AIQ.**

176. Among the AggregateIQ repositories exposed are those relating to four pro-leave EU referendum campaign groups: ChangeBritain; Vote Leave; DUP; and VeteransForBritain.²⁰⁴



In July 2018, the Committee published Facebook adverts that had been run by AIQ during the EU referendum, which illustrates the fact that multiple adverts were being run and targeted by AIQ for different audiences. The series of PDFs highlighted adverts run by AIQ during the referendum on behalf of Vote Leave and the ‘50 Million’ prediction competition.

Facebook and the Vote Leave £50 million prediction competition

177. The £50 million competition was a data-harvesting initiative run for Vote Leave, which offered football fans the chance to win £50m. To enter the competition, fans had

199 [Q3941](#)

200 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 119.

201 [AIQ enforcement notice, 24 October 2018](#), ICO.

202 [Q3943](#)

203 [Q2497](#)

204 Change Britain was founded as a successor to the Vote Leave campaign.

to input their name, address, email and telephone number, and also how they intended to vote in the Referendum. But working out what message to send to which audience was absolutely crucial. Screenshots published on our website prove that AIQ processed all the data from the £50 million football predicted contest that they hosted, and harvested Facebook IDs and emails from signups for the contest.²⁰⁵

178. Furthermore, a blog written by Dominic Cummings admitted that the competition was a data-harvesting exercise: “Data flowed in on the ground and was then analysed by the data science team and integrated with all the other data streaming in. This was the point of our £50m prize for predicting the results of the European football championships, which gathered data from people who usually ignore politics.”²⁰⁶ If people engaged with the quiz, their data was harvested. There is no evidence to show that this was fraudulent, but one could question whether data gathered in this way was ethical. Furthermore, the odds of winning the £50 million prize were estimated as one in 9.2 quintillion (billion, billion).²⁰⁷

AIQ's Capabilities

179. The repository data submitted by Chris Vickery highlight the capabilities that AIQ had built, in obtaining and using people's personal data. It is unclear whether these tools were actually used, but they were obviously developed with the potential to extract and manipulate data. The inclusion of debugging logs within the repository show that the tools were used. The entire extent of their use is not known.

Artificial intelligence

180. Three machine learning pipelines were used to process both text and images. The software could be used to read photographs of people on websites, match them to their Facebook profiles, and then target advertising at these individual profiles.

Facebook Pixels

181. The Facebook Pixel is a piece of code placed on websites. The Pixel can be used to register when Facebook users visit the site. Facebook can use the information gathered by the Pixel to allow advertisers to target Facebook users who had visited that given site. AIQ definitely utilized Pixels and other tools to help in data collection and targeting efforts.

205 [Relevant screenshots of AIQ repository](#), submitted by Chris Vickery

206 [Dominic Cummings's blog](#)

207 [Vote Leave launches £50m football prediction competition](#), Andrew Sparrow, The Guardian, 27 May 2016.

182. For example, if a user visited a website during the referendum campaign that was using a Facebook tracking pixel, placed there by Vote Leave/AIQ, then those users could be unknowingly served adverts by that campaign through Facebook. Those users could be served adverts by other leave campaigns if they had access to the same pixel data. This would be possible if all social adverts were being managed by the same entity for all campaigns (it is easy to share pixel information between different Facebook advertising campaigns). From the repository, it is clear that AIQ staff had access to more than one campaign.

183. Chris Vickery, based on his analysis of the contents of the Gitlab repository, believes that AIQ's capabilities went much further:

“AIQ harvested, and attached to profiles, the Facebook IDs of registered UK voters who had a Facebook account. This data was all synchronized (matched together from many data sources) and collected through the platform offered by Nationbuilder.com. [...] I have the synchronization scripts showing the aggregation on that platform as well as the names of databases controlled directly by AggregateIQ containing this data (along with the usernames and passwords to access the databases)”²⁰⁸

184. Facebook told us of the number of different tools that it provides that third parties can choose to integrate into their websites or other products. We asked Mike Schroepfer, Chief Technology Officer for Facebook, for the percentage of sites on the internet on which Facebook tracks users.²⁰⁹ He did not provide an adequate answer, so we asked again in writing.

185. In its subsequent letter, Facebook again failed to give a figure, but did give examples of other tools that it uses to track users, for example, social plugins (software that enables a customised service) such as the Like button and Share button. Facebook told us that these plugins “enrich users’ experience of Facebook by allowing them to see what their Facebook friends have liked, shared, or commented on across the Web”.²¹⁰ Such plugins also benefit Facebook, as it receives information when a site with the plugin is visited. Its servers log: that a device visited a website or app; and any additional information about the person’s activities on that site that the website chooses to share with Facebook. Facebook told us that, between 9 April and 16 April 2018, the Facebook Like button appeared on 8.4 million websites, the Share button appeared on 931k websites, and there were 2.2 million Facebook Pixels installed on websites.²¹¹

186. Given the fact that AIQ maintained several British interests websites, it would have been easy to install the Facebook pixels on each of the sites that AIQ built and then to share the information from one campaign with another. As well as building websites for UK-based campaigns, there is evidence of wider campaign tool building and deployment targeting of UK voters. For example, a folder called ‘ChangeBritain-MailSend-master’ contains a library of applications as well as a folder called ‘test’. Within this folder is a document that appears to be a template letter for voters to send to their MPs, encouraging them to vote for the triggering of Article 50 if there were a parliamentary vote.

208 [Written evidence](#), submitted by Chris Vickery

209 [Qq 2104 – 2108](#)

210 [Letter from Rebecca Stimson, Facebook, to Damian Collins MP](#), 14 May 2018.

211 Same as above.

LinkedIn profile scraper

187. There is a data scraper tool, within the repository, which has the capacity to extract data from LinkedIn. There is a folder called 'LinkedIn-person-fondler-master', which is an application that scrapes LinkedIn user data. Within the repository is a file containing information on 92,000 individuals on LinkedIn. These names could then have been used to gather the user's location, position and place of work via the LinkedIn scraper tool. Using Facebook's ad targeting, AIQ would then have been able to reach these users via targeting of locations, place of work and job positions.

188. The '[LInbot.py](#)' (LinkedIn bot) script contains commentary from whoever wrote it explaining that it scrapes LinkedIn accounts. There is even a stray log in the same directory suggesting that this bot was run at least from October 8th, 2017 to October 19th, 2017. Scraping data from LinkedIn in this manner violates LinkedIn's terms of User Agreement, which states: "we don't permit the use of any third party software, including "crawlers", bots, browser plug-ins, or browser extensions (also called "add-ons"), that scrape".²¹²

189. AIQ's lawyers, Borden Ladner Gervais, wrote to the Committee on 20 September 2019, stating that "AggregateIQ developed a tool to search for users on LinkedIn and open their profile in such a way as to appear as though a candidate in their local election looked at their profile. This was not a scraping tool. This tool was never deployed".²¹³

190. However, according to Chris Vickery, the commentary within the tool explicitly claims to scrape data, "It is not even nuanced". Sophisticated data matching between LinkedIn and Facebook, when combined with a detailed databased of scraped contacts, could have been used by AIQ to give their political clients a major edge in running high-targeted political adverts, when the target of those adverts had not consented to their data being used in this way. We believe that AIQ certainly developed a tool on LinkedIn that was intended to scrape data from the social network.

Conclusion

191. The ICO Report, "Investigation into the use of data analytics in political campaigns" highlighted its work on investigating the relationship between Cambridge Analytica, SCLE and AIQ,²¹⁴ describing "a permeability" between the companies above and beyond what would normally be expected to be seen".²¹⁵ The ICO states that broader concerns about the close collaboration of the companies are understandable and cites the following financial transactions and contacts:

On 24 October 2014, SCLE Elections Limited made payments to Facebook of approximately \$270,000 for an AIQ ad account; on 4 November 2014, SCLE made a payment of \$14,000 for the same AIQ ad account; A refund for unused AIQ ads was later made to SCLE, with the explanation that SCLE had made pre-payments for its campaigns under AIQ. SCLE was listed as

212 [Prohibitive software and extensions](#), LinkedIn's terms of agreement, accessed 2 December 2018.

213 [Letter from Borden Ladner Gervais LLP to Damian Collins MP](#), 20 September 2018.

214 [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018, p40-43.

215 [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018, p40.

one of the main contacts for at least one of the AIQ. Facebook accounts, and the email address for that contact belonged to an SCLE employee who was also involved in a number of payments.²¹⁶

However, the ICO's investigations showed that, while there was a close working relationship, "we have no evidence that AIQ has been anything other than a separate legal entity".²¹⁷

192. From the files obtained by Chris Vickery, and from evidence we received, there seems to be more to the AIQ/Cambridge Analytica/SCL relationship than is usually seen in a strictly contractual relationship. **AIQ worked on both the US Presidential primaries and for Brexit-related organisations, including the designated Vote Leave group, during the EU Referendum. The work of AIQ highlights the fact that data has been and is still being used extensively by private companies to target people, often in a political context, in order to influence their decisions. It is far more common than people think. The next chapter highlights the widespread nature of this targeting.**

216 Same as above, p41.

217 [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018, p41.

5 Advertising and political campaigning

Introduction

193. The ICO's investigation into the use of data analytics in political campaigns uncovered "a disturbing disregard for voters' personal privacy".²¹⁸ The ICO makes the forceful point that "citizens can only make truly informed choices about who to vote for if they are sure that those decisions have not been unduly influenced".²¹⁹ For that reason, when personal data is used to target political messages, that use should be both transparent and lawful.

194. The Electoral Commission's Report, "Digital Campaigning: increasing transparency for voters", published in June 2018, recommends that the law needs to change to ensure "more clarity over who is spending what, and where and how, and bigger sanctions for those who break the rules. Funding of online campaigning is already covered by the laws on election spending and donations. But the laws need to ensure more clarity about who is spending what, and where and how, and bigger sanctions for those who break the rules".²²⁰ This chapter will highlight the difference between general advertising and political advertising and the steps which are being taken to increase transparency in relation to political advertising. It should be read in conjunction with the recommendations in these respects in our Interim Report.

Online adverts

195. Non-political advertising in the UK is regulated by the Advertising Standards Authority (ASA) through a system of self-regulation and co-regulation, funded by the advertising industry. Guy Parker, CEO of the ASA, told us that "the standards we apply through our advertising codes are, almost without exception, the same for broadcast advertising and for non-broadcast advertising including online".²²¹

196. All non-broadcast advertising, including websites, emails and social media is covered by self-regulation. Co-regulation is the ASA's shared duty with Ofcom, the communications regulator and broadcast licensing authority. Under this arrangement, the ASA regulates broadcast TV and radio advertising on behalf of, and according to, Ofcom's broadcasting regulations.²²²

197. Advertisers that do not comply with ASA standards are subject to sanction. However, the ASA does not have the authority to bring legal action against advertisers who refuse to comply with the Codes. As well as adjudicating on complaints, pressure can be brought to bear by the ASA on companies in the advertising industry which recognise its Codes, and the media, contractors and service providers may decide to withhold services or deny access to space, with the accompanying adverse publicity.²²³

218 [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018, p6.

219 Same as above.

220 [Digital Campaigning: increasing transparency for votes](#), Electoral Commission, June 2018, p3.

221 [Q4101](#)

222 [ASA website](#), accessed 5 February 2019.

223 [Self-regulation and co-regulation, ASA website](#), accessed 5 February 2019.

198. Due to the fact that the ASA is the UK advertising regulator, Guy Parker told us that only UK adverts are under their control, defining a UK advert as “an ad that is targeted at UK consumers”. However, he said that the ASA would “take into account the country of origin of the company that has delivered the ad, for example with direct mailings. It may entail us working with our equivalent in that country if we have a cross-border complaints arrangement with them.”²²⁴ There are obvious difficulties connected with that definition, given the fact that such adverts might originate from abroad, or that their origin is unknown.

199. Guy Parker said that Facebook, Google, and other digital companies that make money out of online adverts should be working on removing misleading and fraudulent adverts, and should be contributing financially to the ASA, to improve the systems and processes of regulating online advertising.²²⁵

Online political adverts

200. The Electoral Reform Society has recently published “Reining in the political ‘wild west’: campaign rules for the 21st century”, coinciding with the 15th anniversary of Facebook’s launch, and—19 years since the main election rules were created—it has made proposals to ensure proper transparency in campaigning: “the ability to rapidly transmit disinformation and channel millions of pounds into campaigns without scrutiny was far more difficult. So much has changed—yet our campaign rules have remained in the analogue age”.²²⁶ The report describes the increase in political parties’ spending on Facebook adverts in the past two general elections: in 2015, it was around £1.3 million; in 2017, it had grown to around £3.2 million.²²⁷ This was national expenditure and excluded local constituency expenditure.

201. In June 2018, the Electoral Commission published a chart, highlighting the proportion of money that campaigners have reported spending on digital advertising as a percentage of total advertising spend.²²⁸ They explained that the chart does not show the full picture of digital advertising in elections and referenda: “It only contains spending data for the most well-known digital platforms, which registered campaigners have reported to us”. As well as paid digital advertisers, campaigners can also ‘like’, ‘share’, and ‘post’ messages for free, with the potential to reach wider audiences.²²⁹

224 [Q4108](#)

225 [Q4112](#)

226 [Reining in the political ‘wild west’: campaign rules for the 21st century](#), foreword Rt Hon Dame Cheryl Gillan MP, Electoral Reform Society (ERS) 4 February 2019.

227 Same as above, Dr Jess Garland, Director of Policy and Research, ERS.

228 [Digital campaigning: increasing transparency for voters](#), The Electoral Commission, June 2018, p4.

229 As above.

202. Political advertising on television is subject to strict regulation and political parties or organisations cannot hold a broadcast licence, or run a broadcaster or channel. Party political broadcasts have clear rules and regulations, which are overseen by Ofcom, during election periods.²³⁰ Non-broadcast political advertising remains unregulated and, as we said in our Interim Report, the ability of social media companies to target content to individuals, and in private, is a new phenomenon, which creates issues in relation to the regulation of elections.²³¹

203. The Electoral Commission described the pernicious nature of micro-targeted political adverts: “Only the voter, the campaigner and the platform know who has been targeted with which messages. Only the company and the campaigner know why a voter was targeted and how much was spent on a particular campaign”.²³² Guy Parker, CEO of the ASA, clarified the position surrounding the regulation of such online political advertising:

We do not cover political advertising, which we define as advertising whenever it appears—it does not have to appear in an election period—whose principal purpose is to influence voters in an election or referendum. [...] Our system of regulation relies on a substantial proportion of the people we are regulating buying into our regulation. The political parties and big campaign groups have never agreed to comply with our advertising codes.²³³

204. It is important to recognise the fact that not all political adverts are run by political parties; they can be distributed through groups and through personal contacts, some of which are not paid. Facebook Groups are where people and organisations can share their interests and express an opinion and can be: public, where anyone can see who the Group members and what has been posted; closed, where only those invited to join the Group can see and share the content; or secret, where nobody on Facebook knows the Group's existence, other than those in the Group. Facebook Pages are always public, created by organisations to engage with their audience and post content, but only administrators of the Pages can post to the account.²³⁴

205. On 5 February 2019, Facebook banned four Facebook Groups in Burma, designating them as ‘dangerous organisations’: the Arakan Army, the Myanmar National Democratic Alliance Army, Kachin Independence Army, and the Ta'ang national Liberation Army. They will also ban “all related praise, support and representation” as soon as they “become aware of it”.²³⁵

206. Written evidence from Dr Kate Dommett, University of Sheffield, recommends a public register of all political advertising, differentiating between formally-affiliated campaigns (a political party and the companies that are paying to carry out digital advertising) and information campaigns, operating without direct influence of the party. This would “build understanding of the political landscape”.²³⁶

230 [Q3790](#), Sharon White, CEO, Ofcom.

231 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 137.

232 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 140.

233 [Q4102](#)

234 [Using Facebook Groups](#), Tiffany Black, lifewire, 16 December 2018.

235 [Banning more dangerous organizations from Facebook in Myanmar](#), Facebook newsroom, 5 February 2019.

236 [FKN0104](#)

207. Our Interim Report supported 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.²³⁷ These recommendations were similar to those made by the Committee on Standards in Public Life.²³⁸

208. It is especially important to know the origin of political adverts when considering the issue of overseas interference in elections. The geographical source of an advert should be apparent. There is also the need for swift action during the short period of a campaign when false, misleading or illegal political advertising takes place. Delay in taking action increases the possibility of disinformation influencing an outcome.

209. The Coalition for Reform in Political Advertising, which includes representation from the Incorporated Society of British Advertisers (ISBA), the Internet Commission and Econsultancy, has developed a four-point plan for the future of political adverts. The plan recommends that: all factual claims used in political ads be pre-cleared; an existing or new body should have the power to regulate political advertising content; all paid-for political adverts should be available for public view, on a single searchable website; and political advertisements should carry an imprint or watermarks to show the sponsor of the advert.²³⁹

210. We repeat the recommendation from our Interim Report, that the Government should look at the ways in which the UK law should define digital campaigning, including having agreed definitions of what constitutes online political advertising, such as agreed types of words that continually arise in adverts that are not sponsored by a specific political party. There also needs to be an acknowledgement of the role and power of unpaid campaigns and Facebook Groups that influence elections and referendums (both inside and outside the designated period).

211. Electoral law is not fit for purpose and needs to be changed to reflect changes in campaigning techniques, and the move from physical leaflets and billboards to online, microtargeted political campaigning. There needs to be: absolute transparency of online political campaigning, including clear, persistent banners on all paid-for political adverts and videos, indicating the source and the advertiser; a category introduced for digital spending on campaigns; and explicit rules surrounding designated campaigners' role and responsibilities.

212. We would expect that the Cabinet Office's consultation will result in the Government concluding that paid-for political advertising should be publicly accessible, clear and easily recognisable. Recipients should be able to identify the source, who uploaded it, who sponsored it, and its country of origin.

213. The Government should 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; defining what constitutes political campaigning; and reducing the time for spending returns to be sent to the Electoral Commission.

237 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 41.

238 [Intimidation in Public Life: a review by the Committee on Standards in Public Life](#), December 2017.

239 [The Coalition for Reform in Political Advertising blog](#), accessed 3 February 2019.

214. *The Government should explore ways in which the Electoral Commission can be given more powers to carry out its work comprehensively, including the following measures:*

- *the legal right to compel organisations that they do not currently regulate, including social media companies, to provide information relevant to their inquiries;*
- *The Electoral Commission's current maximum fine limit of £20,000 should be increased, and changed to a fine based on a fixed percentage of turnover, in line with powers already conferred on other statutory regulators;*
- *The ability for the Electoral Commission to petition against an election due to illegal actions, which currently can only be brought by an individual;*
- *The ability for the Electoral Commission to intervene or stop someone acting illegally in a campaign if they live outside the UK.*

215. *Political advertising items should be publicly accessible in a searchable repository—who is paying for the ads, which organisations are sponsoring the ad, who is being targeted by the ads—so that members of the public can understand the behaviour of individual advertisers. It should be run independently of the advertising industry and of political parties. This recommendation builds on paragraph 144 of our Interim Report.*

216. *We agree with the ICO's proposal that a Code of Practice, which highlights the use of personal information in political campaigning and applying to all data controllers who process personal data for the purpose of political campaigning, should be underpinned by primary legislation. We urge the Government to act on the ICO's recommendation and bring forward primary legislation to place these Codes of Practice into statute.*

217. *We support the ICO's recommendation that all political parties should work with the ICO, the Cabinet Office and the Electoral Commission, to identify and implement a cross-party solution to improve transparency over the use of commonly-held data. This would be a practical solution to ensure that the use of data during elections and referenda is treated lawfully. We hope that the Government will work towards making this collaboration happen. We hope that the Government will address all of these issues when it responds to its consultation, "Protecting the Debate: Intimidating, Influence, and Information" and to the Electoral Commission's report, "Digital Campaigning: increasing transparency for voters". A crucial aspect of political advertising and influence is that of foreign interference in elections, which we hope it will also strongly address.*

Facebook and Mainstream Network

218. Facebook and Twitter claim to have tightened up on the dissemination of disinformation on their sites. However, during the course of our inquiry, when we commissioned work from 89up, they also looked into the work of 'Mainstream Network', a sophisticated, pro-Brexit website, promoted on Facebook, with an advertising spend estimated at £257,000 in just over 10 months during 2018.²⁴⁰ Using Facebook's tools to access adverts, 89up found over 70 adverts that the site was running at one time. They discovered that Mainstream Network were targeting adverts to specific constituents, encouraging them to send standard emails to their MP. Examples of the adverts including one dismissing the Prime Minister's 'Chequers deal'. Whenever a user emails their MP from the site, Mainstream Network puts its own email into the BCC field. This would mean that the user's data was being stored by the site owner, and could be used for marketing purposes, using Facebook's 'Custom Audience' feature.²⁴¹

219. In their evidence, 89up reported that Mainstream Network content had reached 10.9 million users on Facebook alone:

The website is highly misleading and contains no information on the authors of the content, nor any legally required information for GDPR compliance. With the level of spending estimated, it is possible this website is in breach of both GDPR and also Electoral Commission rules on non-party campaigners.²⁴²

220. It is concerning that such a site is run anonymously, so there is no ability to check the origins of the organisation, who is paying for the adverts and in what currency, and why political campaigns are being undertaken without any transparency about who is running them. Facebook requires political campaigning in the US and in India to be registered as running "ads related to politics or of issues of national importance", but this is not the case in the UK.²⁴³ The ICO is currently looking into the activities of Mainstream Network and whether there was a contravention of the GDPR, in distributing such communications.²⁴⁴

221. In October 2018, Facebook announced new requirements for organisations and individuals placing an advert that features political figures and parties, elections, legislation before Parliament or past referendums. These requirements introduced a verification process, whereby people placing political adverts must prove their identity (by a passport, driving licence, or residence permit), which will be checked by a third-party organisation. Political adverts suspected of promoting misinformation or disinformation can be reported and, if the advert contains 'falsehoods', it can be taken down.

222. When Richard Allan, Vice President for Public Policy EMEA at Facebook, was asked about Mainstream Network, during the 'International Grand Committee' oral evidence session in November 2018, he said that there was nothing illegal about a website running such adverts, but that Facebook's changed policy now means that "any organisation that wants to run ads like that will have to authorise. We will collect their identifying

240 [Written evidence on Mainstream network.co.uk](#) submitted by 89up, October 2018.

241 Facebook's 'Custom Audiences' was explained in Chapter 4.

242 89up evidence, October 2018.

243 [Written evidence on Mainstreamnetwork.co.uk](#), submitted by 89up, 20 October 2018.

244 [Q3913](#), Elizabeth Denham.

information. They will have to put on an accurate disclaimer. Their ads will go in the archive". When asked who was behind the Mainstream Network account, Richard Allan said:

We would know whose Facebook account it was, and if there were an investigation by an entity that can legally require information, we would provide information in line with normal procedures.²⁴⁵

Our own investigations have shown that Mainstream Network is now no longer running political adverts on Facebook. There is, however, also no access to any adverts that they ran prior to 16 October 2018, as political adverts that ran prior to this date are not viewable. Richard Allan was asked whether he would provide the Committee with details of who was behind the account or, if not, provide us with the reasons why they cannot.²⁴⁶ **Mainstream Network is yet another, more recent example of an online organisation seeking to influence political debate using methods similar to those which caused concern over the EU Referendum and there is no good case for Mainstream Network to hide behind anonymity. We look forward to receiving information from Facebook about the origins of Mainstream Network, which—to date—we have not received, despite promises from Richard Allan that he would provide the information. We consider Facebook's response generally to be disingenuous and another example of Facebook's bad faith. The Information Commissioner has confirmed that it is currently investigating this website's activities and Facebook will, in any event, have to co-operate with the ICO.**

223. Tech companies must address the issue of shell companies and other professional attempts to hide identity in advert purchasing, especially around political advertising—both within and outside campaigning periods. There should be full disclosure of the targeting used as part of advertising transparency. The Government should explore ways of regulating the use of external targeting on social media platforms, such as Facebook's Custom Audiences.

224. The rapid rise of new populist, right-wing news sites is pushing conspiratorial, anti-establishment content outside the channels of traditional media. This can be seen in the success, for example, of PoliticalUK.co.uk, which works within a network of sites, social media pages and video accounts. Since its inception at the end of April 2018, according to Tom McTague, PoliticalUK has gained more than 3 million interactions on social media, with an average of 5,000 'engagements' for each story published.²⁴⁷

225. McTague noted in his investigation that PoliticalUK.co.uk's report 'Media Silence as tens of thousands protest against Brexit betrayal', about a rally in Westminster in December 2018 led by the far-right activist Stephen Yaxley-Lennon, also known as Tommy Robinson, received 20,351 interactions on Facebook compared to a more critical report about the same event by the Daily Mail which received just 3,481 interactions. Content from PoliticalUK.co.uk is being promoted by Facebook groups including 'EU-I Voted Leave' which is followed by more than 220,000 people. Robinson himself has over 1 million followers on Facebook, making him the second most popular British political figure on the site, after the Labour Party leader, Jeremy Corbyn.

245 [Q4218](#)

246 [Q4219](#)

247 [How Britain grapples with nationalist dark web](#), Tom McTague, Politico, 17 December 2018, [The man to 'make the British establishment's head blow off](#), Tom McTague, Politico, 21 December 2018.

226. However, tools that let the public see the way in which Facebook users are being targeted by advertisers have recently been blocked by Facebook. Evidence we received from Who Targets Me? puts Facebook's desire for more transparency on its site into question. Who Targets Me? was established in 2017 to help the public understand how they were being targeted with online adverts during the general election. It explains its work, in collaboration with the London School of Economics, the Oxford Internet Institute and Sheffield University:

Our tool can be installed as a browser extension, it then collects data from Facebook users and shows them personalised statistics of how many adverts they have seen. The data is also collated into a master database, that is shared exclusively with researchers and journalists interested in exposing misinformation, election overspending and microtargeting, among other issues. Our tool can be installed as a browser extension, it then collects data from Facebook users and shows them personalised statistics of how many adverts they have seen. The data is also collated into a master database, that is shared exclusively with researchers and journalists interested in exposing misinformation, election overspending and microtargeting, among other issues.²⁴⁸

227. On January 9th, 2014, Who Targets Me? and all other organisations operating in this space, including ProPublica and Mozilla, lost access to this data. Facebook made this change with the purpose of blocking tools that operate to highlight the content and targeting of Facebook adverts. There is now no practical way for researchers to audit Facebook advertising.²⁴⁹

228. The ICO has called for a Code of Practice to be placed in statute, to highlight the use of personal information in political campaigning—following the same codes set out in the Data Protection Act²⁵⁰—including an age-appropriate design code and a data protection and journalism code.²⁵¹ The ICO anticipates that such codes would apply to all data controllers who process personal data for the purpose of political campaign. The ICO has existing powers under the General Data Protection Regulation (GDPR) to produce codes of practice relating to the Commissioner's functions, which they intend to do before the next general election.²⁵² But the ICO also feels that such codes should have a statutory underpinning in primary legislation and a consultation on this proposal closed on 21 December 2018. We agree; only by placing such codes of practice on a statutory footing will the processing of personal data be taken seriously.

Constitutional Research Council (CRC)

229. This lack of transparency in political advertising was illustrated by the Constitutional Research Council's donation during the EU Referendum. The CRC is an unincorporated funding organisation based in Scotland, which contributed to the Democratic Unionist Party's Leave campaign in Northern Ireland and in England, during the EU referendum. It donated £435,000 to the DUP, the biggest political donation in Northern Ireland's history,

248 [FKN0123](#)

249 Same as above.

250 [Data Protection Act 2018](#), Schedules 121 to 124.

251 [Call for views: Code of Practice for the use of personal information in political campaigns](#), 6 November 2018.

252 [Article 57 1.\(d\) of the GDPR](#), Official Journal of the European Union, L119/68.

of which £425,000 was spent on advertising in the referendum campaign. Its sole named office holder is its Chairman, Richard Cook. There have been claims that Vote Leave and the DUP were part of a co-ordinated campaign in the EU Referendum, and allegations that Richard Cook's financial affairs involved fraud relating to waste management.²⁵³ The Committee twice wrote to Richard Cook asking him for the source of the £435,000 donation and how it was presumed the money would be spent. We received one reply on 5 November 2018 in which Mr. Cook claimed to be "greatly amused" by the Committee's letter before accusing us of spreading "fake news and disinformation" about him. He declined however to reveal the source of the money or to say how the Constitutional Research Council believed it was going to be spent.²⁵⁴

230. The Electoral Commission gave evidence on 6 November 2018, and were asked about this donation from the CRC. The then CEO, Claire Bassett, explained that "we are restricted by law on what we can say about any donations made before 2017" and it is a situation "that we do not really want to be in, and it is deeply regrettable".²⁵⁵ Donations made to political parties in Northern Ireland before July 2017 are protected, namely, from disclosure, under Section 71E of the Political Parties, Elections and Referendums Act 2000. Louise Edwards, Head of Regulations at the Electoral Commission, explained the position:

The Democratic Unionist Party as a registered party in Northern Ireland needed to continue to supply quarterly donation reports to us throughout the referendum period, which it did. We are under a duty to verify the contents of donation reports for Northern Ireland parties and that is a duty we take very seriously and we do it. If we discover that a donation in one of those reports is in fact impermissible, the restrictions [...] are lifted and we can talk about that donation. We cannot talk about donations to the DUP from that period because, having verified those reports, the donors on them were permissible²⁵⁶

253 [Electoral Commission Freedom of Information response](#), to a request made on 5 August, in reference to the Spotlight BBC programme, 25 September 2018, Electoral Commission website. The exchange of internal emails highlights the issues.

254 [Correspondence between Damian Collins MP and Richard Cook, Constitutional Research Council.](#)

255 [Q4068](#)

256 [Q4068](#)

231. When asked whether there was a common plan between the Constitutional Research Council donating £435,000 to the DUP and booking an advert for £280,000 in the Metro newspaper, in London, on behalf of Vote Leave (within days of the vote), Louise Edwards replied, “There is not a way for me to answer that question that does not put me in breach of the law, I am afraid”.²⁵⁷ When asked whether the money from the CRC donated to the DUP was from the UK, and not of foreign origin (which would make it impermissible in UK law), Claire Bassett replied that “we were satisfied that the donors were permissible”.²⁵⁸ When asked whether they had been told the origin of the money, Louise Edwards and Claire Bassett said, “we are not able to discuss it any further”²⁵⁹ and “we were satisfied that the donors were permissible in UK law”,²⁶⁰ from information verified by “a range of sources”.²⁶¹ They were also unable, by law, to confirm whether they knew the identity of the person who donated the money.²⁶²

232. Donations made to political parties in Northern Ireland before July 2017 are protected from disclosure, under Section 71E of the Political Parties, Elections and Referendums Act 2000. This prevents the Electoral Commission from disclosing any information relating to such donations before July 2017. We concur with the Electoral Commission that it is “deeply regrettable” that they are unable, by law, to tell Members of Parliament and the public about details surrounding the source of the £435,000 donation that was given by the Constitutional Research Council (CRC) to the DUP or the due diligence that was followed. Because of the law as it currently stands, this Committee and the wider public have no way of investigating the source of the £435,000 donation to the DUP made on behalf of the CRC and are prevented from even knowing whether it came from an organisation, whose membership had either sanctioned the donation or not, or from a wealthy individual.

233. There is an absence of transparency surrounding the relationship between the Constitutional Research Council, the DUP and Vote Leave. We believe that, in order to avoid having to disclose the source of this £435,000 donation, the CRC, deliberately and knowingly, exploited a loophole in the electoral law to funnel money to the Democratic Unionist Party in Northern Ireland. That money was used to fund pro-Brexit newspaper advertising outside Northern Ireland and to pay the Canadian-based data analytics company, Aggregate IQ.

234. We support the Electoral Commission in its request that the Government extend the transparency rules around donations made to political parties in Northern Ireland from 2014. This period of time would cover two UK general elections, two Northern Ireland Assembly elections, the Scottish independence referendum, the EU referendum, and EU and local government elections. We urge the Government to make this change in the law as soon as is practicable to ensure full transparency over these elections and referendums.

257 [Q4081](#), Louise Edwards

258 [Q4069](#), Claire Bassett

259 [Q4070](#), Louise Edwards

260 [Q4069](#), Louise Edwards

261 [Q4072](#), Louise Edwards

262 [Q4075](#), Claire Bassett

The Cairncross Review: a sustainable future for journalism

235. As we said in our Interim Report, the then Secretary of State, Rt Hon Matthew Hancock MP, told us that the Cairncross Review would be looking at the role of the digital advertising supply chain, within the broader context of the future of the UK press, at how fair and transparent it is, and whether it “incentivises the proliferation of inaccurate and/or misleading news.” The consultation closed in September 2018²⁶³ and the Cairncross Report was published on 12 February 2019.

236. We welcome Dame Frances Cairncross’s report on safeguarding the future of journalism, and the establishment of a code of conduct to rebalance the relationship between news providers and social media platforms. In particular, we welcome the recommendation that online digital newspapers and magazines should be zero rated for VAT, as is the case for printed versions. This would remove the false incentive for news companies against developing more paid-for digital services. We support the recommendation that chimes with our own on investigating online advertising, in particular focussing on the major search and social media companies, by the Competitions and Markets Authority.

263 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 53.

6 Foreign influence in political campaigns

Introduction

237. The speed of technological development has coincided with a crisis of confidence in institutions and the media in the West. This has enabled foreign countries intent on destabilising democratic institutions to take advantage of this crisis. There has been clear and proven Russian influence in foreign elections, and we highlighted evidence in our Interim Report of such attempts in the EU Referendum.²⁶⁴

238. It is interesting to note that, as of 30 November 2018, the online Government response to our Report received a total of 1,290 unique page views and the PDF has been visited 396 unique times from the website.²⁶⁵ In the month following its publication, over 63% of views of the report online were from foreign IP addresses (whereas, on average, 80% of viewers of Reports are UK-based), and of these, over half were from Russia. Furthermore, two-thirds of viewers were new visitors, meaning they had not visited the parliament.uk website before (in comparison with the majority of Reports, where only around 30% are new visitors). The following table shows the unique page views by city, illustrating this high proportion from Russia:

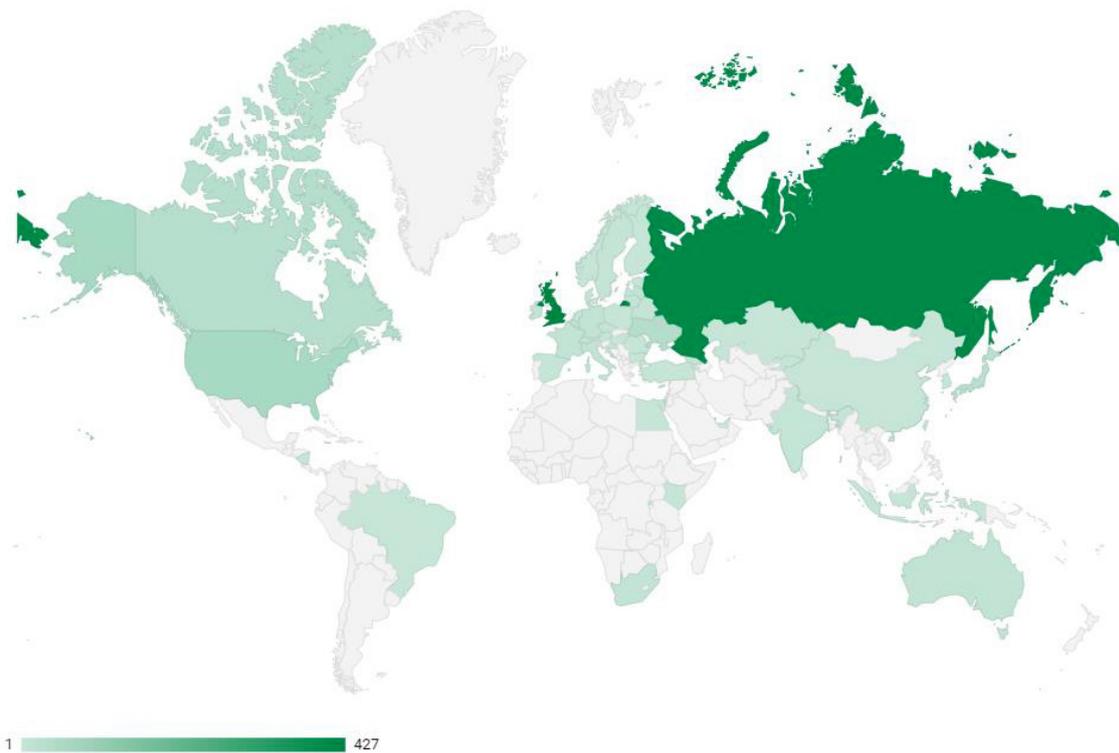
	City	Unique Pageviews ▾
1.	Moscow	19.79%
2.	London	17.8%
3.	Saint Petersburg	2.94%
4.	Cambridge	2.25%
5.	Kyiv	1.9%
6.	Sheffield	1.56%
7.	Bristol	1.38%
8.	Edinburgh	1.38%
9.	Novosibirsk	1.21%
10.	Ottawa	1.21%

Source: Web and publications Unit, House of Commons

The following map shows the concentration of those readers of the Government Response to the Interim Report, by country:

264 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, Chapter 5.

265 These statistics have been supplied by the Web and Publications Unit, House of Commons. 'Unique' means that if the same person visited a HTML page/PDF multiple times in one session it would count as one view only). It is not possible to log any reads of the PDF which have not come from the Parliament.uk website (for example, when the link to the PDF is shared on Twitter) so this statistic is deceptively low.



Source: Web and Publications Unit, House of Commons

This itself demonstrates the very clear interest from Russia in what we have had to say about their activities in overseas political campaigns.

239. In this Chapter, we will update the information we set down in our Interim Report, including Facebook's knowledge about Russian interference in its data. We shall also build on our previous recommendations.

Russian interference in UK elections

240. As we said in our Interim Report, Prime Minister Theresa May accused Russia of meddling in elections and planting disinformation, in an attempt to 'weaponise information' and sow discord in the West.²⁶⁶ In its response to the Report, the Government stated that, following the nerve agent attack in Salisbury in March 2018, the Government had "judged the Russian state promulgated at least 38 false disinformation narratives around this criminal act".²⁶⁷ However, the Government made it clear that "it has not seen evidence of successful use of disinformation by foreign actors, including Russia, to influence UK democratic processes".²⁶⁸

266 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 41.

267 [Disinformation and 'fake news': Government Response to the Committee's Fifth Report of Session 2017–19](#), 23 October 2018, HC 1630 Government response to Interim Report, page 16.

268 Same as above.

241. When the Secretary of State was questioned in oral evidence over what constitutes “successful”, Rt Hon Jeremy Wright MP, responded: “We have seen nothing that persuades us that Russian interference has had a material impact on the way in which people choose to vote in elections. It is not that they have not tried, but we have not seen evidence of that material impact”.²⁶⁹ It is surely a sufficient matter of concern that the Government has acknowledged that interference has occurred, irrespective of the lack of evidence of impact. The Government should be conducting analysis to understand the extent of Russian targeting of voters during elections.

242. The Government also cannot state definitively that there was “no evidence of successful interference” in our democratic processes, as the term “successful” is impossible to define in retrospect. There is, however, strong evidence that points to hostile state actors influencing democratic processes. Cardiff University and the Digital Forensics Lab of the Atlantic Council have both detailed ways in which the Kremlin attempted to influence attitudes in UK politics.²⁷⁰

243. Kremlin-aligned media published significant numbers of unique articles about the EU referendum. 89 Up researchers analysed the most shared of the articles, and identified 261 with a clear anti-EU bias to the reporting. The two main outlets were RT and Sputnik, with video produced by Ruptly.²⁷¹ The articles that went most viral had the heaviest anti-EU bias.²⁷² The social reach of these anti-EU articles published by the Kremlin-owned channels was 134 million potential impressions, in comparison with a total reach of just 33 million and 11 million potential impressions for all content shared from the Vote Leave website and [Leave.EU](#) website respectively.²⁷³ The value for a comparable paid social media campaign would be between £1.4 and 4.14 million.

244. On 17 January 2019, Facebook removed 289 Pages and 75 accounts from its site, accounts that had about 790,000 followers and had spent around \$135,000 on ads between October 2013 and January 2019. The sites had been run by employees at the Russian state-owned news agency Sputnik, who represented themselves as independent news or general interest Pages. Around 190 events were hosted by these Pages (the first was scheduled for August 2015 and the most recent was scheduled for January 2019).²⁷⁴

245. Nathaniel Gleicher, Facebook’s head of cybersecurity policy, wrote: “Despite their misrepresentations of their identities, we found that these Pages and accounts were linked to employees of Sputnik, a news agency based in Moscow, and that some of the Pages frequently posted about topics like anti-NATO sentiment, protest movements, and anti-corruption.”²⁷⁵ Facebook also removed 107 Pages, groups and accounts that were designed to look as if they were run from Ukraine, but were part of a network that originated in Russia.

269 [Q211 Evidence session, 24 October 2018, The Work of the Department for Digital, Culture, Media and Sport.](#)

270 [Russian influence and interference measures following the 2017 UK terrorist attacks](#), Cardiff University Crime and Security Research Institute, funded by Centre for Research and Evidence on Security Threats (CREST), 18 December 2017; [#Election Watch: Scottish vote, pro-Kremlin trolls: how pro-Russian accounts boosted claims of election fraud at Scotland’s independence referendum](#), DFRLab, 12 December 2017.

271 Ruptly GmbH is a video news agency that is owned by the RT televised news network.

272 [89up releases report on Russian influence in the EU referendum](#), 89up, 2 October 2018, slide 10.

273 [89up releases report on Russian influence in the EU referendum](#), 89up, 2 October 2018.

274 [Removing coordinated inauthentic behavior from Russia](#), Facebook newsroom, 17 January 2019.

275 Same as above.

246. Ben Nimmo, from the Digital Forensics Lab of the Atlantic Council, has detailed attempts to influence attitudes to the Scottish Referendum, for instance, which included a Russian election observer calling the referendum not in line with international standards, and Twitter accounts calling into question its legitimacy. The behaviour of these accounts, Mr Nimmo argues, is pro-Kremlin, and consistent with the behaviour of accounts known to be run by the so-called “troll factory” in St. Petersburg, Russia, during the United States 2016 presidential election and beyond. However, it is not possible to determine from open sources whether some or all of the accounts are independent actors, or linked to Russian information operations.²⁷⁶

247. As the Secretary of State said, Russia also used malign digital influence campaigns to undermine the Government’s communication of evidence in the aftermath of the poisoning of the Skripals.²⁷⁷ Research by the Centre for Research and Evidence on Security Threats at Cardiff University showed how ‘sock puppet’ Twitter accounts,²⁷⁸ controlled by the St Petersburg-based ‘Internet Research Agency’, tried to fuel social divisions, including religious tensions, in the aftermath of the Westminster, Manchester, London Bridge and Finsbury Park terror attacks.²⁷⁹ Furthermore, the methods through which malign influence can be deployed are also constantly being expanded. While Twitter has been responsive in shutting down abusive and fake accounts, Facebook remains reluctant to do so. Research by the Institute for Strategic Dialogue and the LSE Arena Program into the German 2017 elections discovered Facebook Groups created by unverifiable administrators, directing Russian state-backed media during the election period, with regularity, across social media.²⁸⁰

248. The Government has been very ready to accept the evidence of Russian activity in the Skripal case, an acceptance justified by the evidence. However, it is reluctant to accept evidence of interference in the 2016 Referendum in the UK. If the Government wishes the public to treat its statements on these important matters of national security and democracy seriously, it must report the position impartially, uninfluenced by the political implications of any such report.

249. In common with other countries, the UK is clearly vulnerable to covert digital influence campaigns and the Government should be conducting analysis to understand the extent of the targeting of voters, by foreign players, during past elections. We ask the Government whether current legislation to protect the electoral process from malign influence is sufficient. Legislation should be in line with the latest technological developments, and should be explicit on the illegal influencing of the democratic process by foreign players. We urge the Government to look into this issue and to respond in its White Paper.

276 [Russians ‘tried to discredit 2014 Scots independence vote’](#), Chris Marshall, 13 December 2017; [#Election Watch: Scottish Vote, Pro-Kremlin Trolls](#), medium, 13 December 2017

277 [Q215 Rt Hon Jeremy Wright QC MP evidence session](#), 24 October 2018, The Work of the Department for Digital, Culture, Media and Sport, HC 361

278 A sockpuppet is an online identity used for purposes of deception.

279 [Russian influence and interference measures following the 2017 UK terrorist attacks](#), Cardiff University Crime and Security Research Institute, funded by Centre for Research and Evidence on Security Threats (CREST), 18 December 2017.

280 [“Make Germany great again”: Kremlin, alt-right and international influences in the 2017 German elections](#), Institute for Strategic Dialogue and the Institute of Global Affairs, December 2017.

Facebook and Russian disinformation

250. The Committee has repeatedly asked Facebook, in written correspondence and in oral evidence, about Russian activity on Facebook and, in particular, about knowledge of the Russian adverts that ran during the presidential election in America in 2016. According to a New York Times article published in November 2018,²⁸¹ Facebook had discovered suspicious Russia-linked activity on its site in early 2016, in an attempt to disrupt the presidential election. In September 2017, Alex Stamos, the then Chief Security Officer, told the members of Facebook's Executive Board that that Russian activity was still not under control. The article claimed that Facebook executives, including Mark Zuckerberg and Sheryl Sandberg, attempted to deflect attention from their own company to other tech companies, by hiring a political consultancy, Definers Public Affairs, allegedly to spread anti-semitic information about George Soros and his campaigning activities, after Mr Soros called Facebook "a menace to society" in early 2018.²⁸²

251. When Simon Milner, Policy Director UK, Middle East and Africa, at Facebook, gave evidence to us in February 2018, he was asked specifically about whether Facebook had experienced people from one country seeking to place political adverts in another country. He replied:

We have not seen in the last general election, during the Brexit vote or during the 2015 general election, investigative journalism, for instance, that has led to the suggestion that lots of campaigns are going on, funded by outsiders. [...] There is no suggestion that this is going on.²⁸³

252. Given the information contained in the New York Times article and the information we have received from Six4Three, we believe that Facebook knew that there was evidence of overseas interference and that Mr Milner misled us when he gave evidence in February 2018. Facebook's Chief Technology Officer, Mike Schroepfer, also told the Committee, with regards to the company's knowledge of Russian interference in the 2016 presidential election, by targeting user accounts on the site: "We were slow to understand the impact of this at the time".²⁸⁴ Again, this would appear to be a misleading answer based on what senior executives at Facebook knew in 2016. We now know that this statement was simply not true. **We are left with the impression that either Simon Milner and Mike Schroepfer deliberately misled the Committee or they were deliberately not briefed by senior executives at Facebook about the extent of Russian interference in foreign elections.**

Russian IP addresses at Facebook

253. The Six4Three documents revealed that "an engineer at Facebook notified the company in October 2014 that entities with Russian IP addresses had been using a Pinterest API key to pull over 3 billion data points a day through the ordered friends API. This activity was not reported to any external body at the time".²⁸⁵

281 [Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis](#), Sheera Frenkel, Nicholas Confessore, Cecilia Kang, Matthew Rosenberg and Jack Nicas, The New York Times, 14 November 2018.

282 Charlie Angus, [Q4131](#).

283 [Q424 to 425](#)

284 [Q2122](#)

285 [Q4168](#), the Chair, Damian Collins MP.

254. When questioned about these emails, Richard Allan refused to answer, stating that that information was based on emails that were “unverified, partial accounts from a source who has a particular angle”.²⁸⁶ However, on the same evening of 27 November 2018, Facebook itself chose to send the very same emails to a CNN Reporter, despite Richard Allan’s description of them.²⁸⁷ Facebook wanted to show that the investigation had proved that there had been no Russian interference. However, the email exchange shows that the engineer’s reassurance of there being no Russian interference was given within an hour, and it is questionable whether Facebook engineers would have been able to satisfy themselves within that short time that Russian interference had not occurred.

Facebook data owned by the Cambridge University Psychometrics Centre and shared with Russian APIs

255. The ICO has been investigating how far data was shared between GSR—the company set up by Dr. Kogan, in advance of his work involving the ‘thisisyourdigitallife’ app—Cambridge University, and Russian APIs.²⁸⁸ When asked whether the ICO was still investigating whether Dr Kogan’s data had been accessed by people in Russia, the Information Commissioner, Elizabeth Denham replied:

It is an active line of investigation. What we said in July was that there were some IP addresses that were found in that data and that server associated with Aleksandr Kogan that resolved to Russia and associated states. That is information that we have passed on to the authorities. It is not in our remit to investigate any further than that, but we have passed that on to the relevant authorities.²⁸⁹

She later told us that the ICO had referred the issue to the National Crime Agency.²⁹⁰

256. Further clarification from the Deputy Information Commissioner, James Dipple-Johnston, highlighted the fact that IP addresses originating from Russia were connected to an earlier app at the Cambridge University Psychometrics Centre. The IP addresses were also linked to alleged cyber attacks in the past and to a “Tor entry point”—a device for people to hide their identity online.²⁹¹

Russian interference through other social media platforms

257. Russian meddling in elections overseas has, clearly, not been limited to just Facebook. In October 2018, Twitter released an archive of tweets that had been shared by accounts from the Internet Research Agency, with the goal of “encouraging open research and investigation of these behaviors from researchers and academics around the world”.²⁹² The datasets comprised of 3,841 accounts that were affiliated with the Internet Research Agency and originated from Russia, and 770 other accounts, “potentially originating in

286 [Q4169](#)

287 [Donie O’Sullivan Twitter account \(@donie\)](#), incorporating the redacted Facebook emails, 27 November 2018.

288 [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018.

289 [Q3967](#)

290 [Q4308](#)

291 [Qs 3968 and 3969](#)

292 [Enabling further research on information operations on Twitter](#), Vijaya Gadde and Yoel Roth, Twitter website, 17 October 2018.

Iran". The accounts included more than 10 million tweets and more than 2 million images.²⁹³ The Twitter accounts were used to influence the 2016 US presidential election, as well as elections and referenda in several other countries, including the UK. The accounts were also used to influence public sentiment around several issues of national importance in other countries, including Ukraine.

258. The Oxford Internet Institute and the Senate Select Committee on Intelligence worked together to inquire into the activities of the Internet Research Agency (IRA), by studying data that had been provided by the tech companies in the summer of 2017.²⁹⁴ The investigations revealed that: the Russian campaign to polarise the US electorate and destabilise trust in the media started in 2013, which is earlier than previously thought; and the IRA subsequently accelerated content production across a full set of social media companies, with parallel trends across Twitter, Facebook, Instagram and YouTube.

259. We note as well the comments made by Vladislav Surkov, a senior advisor to President Putin, in an article published in the Russian daily *Nezavisimaya Gazeta*, on 11 February 2019. He said that "Foreign politicians blame Russia for meddling in elections and referenda all over the planet. In fact, it's even more serious than that: Russia is meddling in their brains and they don't know what to do with their changed consciousness."²⁹⁵

Leave.EU, Arron Banks, the US and Russia

260. Our Interim Report highlighted the fact that Arron Banks is, to date, the person who has, allegedly, given the largest donation to a political campaign in British history, reported to be £8.4 million, but that questions still remain over both the sources of that donation and the extent of Mr Banks' wealth.²⁹⁶

261. The Report recorded the fact that Arron Banks discussed business ventures within Russia and beyond, 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. [...] It is unclear whether Mr. Banks profited from business deals arising from meetings arranged by Russian officials.²⁹⁷

262. Our Interim Report recommended that the Electoral Commission pursue investigations into donations that Arron Banks made to the Leave campaign, to verify that that money was not sourced from abroad, and that "should there be any doubt, the matter should be referred to the National Crime Agency".²⁹⁸ On 1 November 2018, the Electoral Commission referred the following organisations and individuals to the National

293 Same as above.

294 [The IRA, Social Media, and Political Polarization in the United States, 2012–2018](#), Philip N.Howard, Bharath Ganesh, Dimitra Liosiou, University of Oxford, and John Kelly, Camille Francois, Graphika, 18 December 2018.

295 [Official: Russia's political system a good model for others](#), Vladimir Isachenkov, The Washington Post, 11 February 2019.

296 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 28 July 2018, paras 187 to 188.

297 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 28 July 2018, paras 185 and 186.

298 Same as above, para 191.

Crime Agency: Better for the Country (the company that ran the Leave.EU referendum campaign); Arron Banks; Leave.EU; Elizabeth Bilney; and other associated companies and individuals. The Electoral Commission's investigation focused on £2m reported to have been loaned to Better for the Country by Arron Banks and his group of insurance companies and a further £6m reported to have been given to the organisation, on behalf of Leave.EU, by Arron Banks alone.²⁹⁹ The NCA has now launched a criminal investigation.

263. We asked the National Crime Agency for an update on their investigations and they replied:

The NCA has initiated an investigation concerning the entities Better for the Country (BFTC) and Leave.EU; as well as Arron Banks, Elizabeth Bilney and other individuals. This follows our acceptance of a referral of material from the Electoral Commission. This is now a live investigation, and we are unable to discuss any operational detail.³⁰⁰

264. In the spring of 2018, we heard that Steve Bannon had introduced Arron Banks to Cambridge Analytica.³⁰¹ In November 2018, we received evidence to show that there was a relationship between Leave.EU and Steve Bannon in 2015, highlighted in an email from Arron Banks to Andy Wigmore, copying in Steve Bannon and Elizabeth Bilney, showing that Leave.EU wanted Cambridge Analytica to set up a funding strategy in the US:

We would like Cambridge Analytica to come up with a strategy for fundraising in the States [...] and how we could connect to people with family ties in the UK and raise money and create SM [social media] activity.³⁰²

Arron Banks and Leave.EU had not only Russia, but the US, in their sights.

265. The Electoral Commission's paper, "Digital Campaigning", published in June 2018, highlights the fact that the current rules on spending were established in a pre-digital time:

The UK's rules set minimum amounts for campaign spending before people or organisations have to register as a non-party campaigner. This means that a foreign individual or organisation that spends under these amounts would not have broken any specific electoral laws in the UK. [...] Had not seen potential for foreign sources to direct purchase campaign advertising in the UK".³⁰³

266. We are pleased that our recommendation set out in the Interim Report in July 2018, concerning Arron Banks and his donation, has been acted on by both the Electoral Commission—which has concerns that Banks is not the 'true source' of the donation—and by the National Crime Agency, which is currently investigating the source of the donation.

299 [Report on investigation into payments made to Better for the Country and Leave.EU](#), Electoral Commission, 1 November 2018.

300 Email sent to the Committee, 16 November 2018.

301 [Q1506](#), Brittany Kaiser.

302 [FKN0109](#)

303 [Digital campaigning: increasing transparency for voters](#), The Electoral Commission, June 2018, para 86.

267. *There is a general principle that, subject to certain spending limits, funding from abroad is not allowed in UK elections. However, as the Electoral Commission has made clear, the current rules do not explicitly ban overseas spending. We recommend that, at the earliest opportunity, the Government reviews the current rules on overseas involvement in our UK elections to ensure that foreign interference in UK elections, in the form of donations, cannot happen. We also need to be clear that Facebook, and all platforms, have a responsibility to comply with the law and not to facilitate illegal activity.*

Further ongoing investigations and criminal complaints

268. We have recently been told by Clint Watts, an expert whom we first met in New York in February 2018, that Twitter accounts monitored during 2015 were discussing both Brexit and the US Presidential campaign influence.³⁰⁴ Furthermore, in the same month that Twitter released its archive of tweets shared by accounts from the Internet Research Agency, the US Department of Justice filed criminal charges against a Russian national, Elena Alekseevna Khusyaynova, for alleged crimes relating to interference between the period of the 2016 US presidential election and the 2018 mid-term elections.³⁰⁵

269. The FBI also filed a Criminal Complaint on 28 September 2018. It described the work of 'Project Lakhta', in which individuals have allegedly "engaged in political and electoral interference operations targeting populations within the Russian Federation and in various other countries, including, but not limited to, the United States, members of the European Union, and Ukraine".³⁰⁶ Since at least May 2014, Project Lakhta's stated goal in the United States was to spread distrust towards candidates for political office and the political system in general.³⁰⁷ The complaint also listed 14 companies—believed to be shell companies—involved in the conspiracy.³⁰⁸

270. As recently as 31 January 2018, Facebook announced the suspension of a network of accounts—783 pages, groups, and accounts—that it said were engaged in coordinated inauthentic behaviour on Facebook and Instagram that was "directed from Iran." Almost simultaneously, Twitter announced that it had suspended networks of accounts that it termed "foreign information operations", potentially connected to Iran, Venezuela and Russia.³⁰⁹

271. Information operations are part of a complex, interrelated group of actions that promote confusion and unrest through information systems, such as social media companies. These firms, in particular Facebook, need to take action against untransparent administrators of groups, which are being used for political campaigns. They also need to impose much more stringent punishment on users who abuse the system. Merely having a fake disinformation account shut down, but being able to open another one the next moment, is hardly a deterrent.

304 Private conversation with Clint Watts, Distinguished Research Fellow at the Foreign Policy Research Institute.

305 [Criminal complaint, USA v Elena Alekseevna Khusyaynova, case No. 1:18-MJ-464](#), District Court Alexandria, Virginia, 28 September 2018.

306 [Criminal complaint, USA v Elena Alekseevna Khusyaynova, case No. 1:18-MJ-464](#), District Court Alexandria, Virginia, 28 September 2018.

307 Same as above.

308 Same as above.

309 [Facebook and Twitter remove thousands of fake accounts tied to Russia](#), Venezuela and Iran, Donie O'Sullivan, CNN Business, 31 January 2019.

272. The Government should put pressure on social media companies to publicise any instances of disinformation. The Government needs to ensure that social media companies share information they have about foreign interference on their sites—including who has paid for political adverts, who has seen the adverts, and who has clicked on the adverts—with the threat of financial liability if such information is not forthcoming. Security certificates, authenticating social media accounts, would ensure that a real person was behind the views expressed on the account.

273. We repeat our call to the Government to make a statement about how many investigations are currently being carried out into Russian interference in UK politics. We further recommend that the Government launches an independent investigation into past elections—including the UK election of 2017, the UK Referendum of 2016, and the Scottish Referendum of 2014—to explore what actually happened with regard to foreign influence, disinformation, funding, voter manipulation, and the sharing of data, so that appropriate changes to the law can be made and lessons can be learnt for future elections and referenda.

7 SCL influence in foreign elections

Introduction

274. Data analytics firms have played a key role in elections around the world. Strategic communications companies frequently run campaigns internationally, which are financed by less than transparent means and employ legally dubious methods. As we wrote in our Interim Report, we raised concerns about the complex web of relationships between the SCL (Strategic Communications Laboratories) group of companies, and “these concerns have been heightened by Alexander Nix and SCL’s own links with organisations involved in the military, defence, intelligence and security realms”.³¹⁰

275. We highlighted the following election and referendum campaigns that SCL Elections and associated companies had been involved in: Australia; Brazil; Czech Republic; France; Gambia; Germany; Ghana (2013); Guyana; India; Indonesia; Italy; Kenya (Kenyatta campaigns of 2013 and 2017); Kosovo; Malaysia; Mexico; Mongolia; Niger; Nigeria; Pakistan; Peru; Philippines; Slovakia; St Kitts and Nevis; St Lucia; St Vincent and the Grenadines; Thailand; Trinidad and Tobago; and the UK. We also received testimony that SCL may also have worked on the Mayoral election campaign in Buenos Aires in 2015 for Mauricio Macri.³¹¹

276. Following publication of our Interim Report, both the High Commissioner of Malta and the Chelgate PR company wrote to the Committee, denying statements in the Interim Report that the Malta Labour Party had had dealings with the SCL Group “for several years before the 2013 elections”. We understand, however, that SCL certainly had meetings in Malta, that Christian Kalin of Henley & Partners was introduced by SCL to Joseph Muscat in 2011, and that Christian Kalin met with both political parties before 2013.³¹²

Further information regarding the work of SCL

277. As we said in our Interim Report, SCL Elections and its associated companies, including Cambridge Analytica, worked on campaigns that were not financed in a transparent way, overstepping legal and ethical boundaries.

278. Our Interim Report described the relationship between SCL Elections’ campaigning work and Christian Kalin, Chairman of Henley & Partners:

We were told that, behind much of SCL Elections’ campaigning work was the hidden hand of Christian Kalin, Chairman of Henley & 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 & Partners would gain exclusive passport rights for that country, under a citizenship-by-investment (CBI) programme. Alexander Nix and Christian Kalin have

310 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 123.

311 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 210; Leopoldo Moreau, Chair, Freedom of Expression Commission, Chamber of Deputies, Argentina ([FNW0117](#)).

312 Confidential evidence shown to the Committee.

been described as having a 'Faustian pact'. With the exclusive passport rights came a government that would be conducive to Mr. Kalin and his clients.³¹³

Citizenship-by-investment schemes

279. Henley & Partners currently manages 'citizenship-by-investment' schemes in several countries, including Malta, Moldova, St Lucia, St Kitts and Nevis, and Grenada. Caribbean passports allow visa-free access to travel to 130 countries, including the UK and many European states. Passports issued from Malta allow access to all European countries—Malta's Individual Investor Programme (IIP) was introduced at the beginning of 2014, the first of its kind to be recognised by the European Commission.³¹⁴ Many such passports are issued to residents from Russia, China and the Middle East. A recent Guardian article described the work of Henley & Partners, describing the way in which foreign nationals can become citizens of a country in which they have never lived, in exchange for donations to a national trust fund:

Henley has made tens of millions of dollars from this trade, and its first big client was the government of St Kitts. And while Nix's star has fallen, Kalin and his industry are on the up—and finding themselves increasingly under scrutiny. [...] For a few hundred thousand dollars, the right passport, from the right place, can get its owner into almost any country. A sum worth paying for legitimate traders. But also, police fear, for criminals and sanctions-busting businessmen.³¹⁵

280. There has been renewed pressure from the European Union to regulate the schemes of residence-by-investment (described as 'golden visas') and citizenship-by-investment (described as 'golden passports'). The granting of residence rights to foreign investors, in return for passports, is open to "security risks, risks of money laundering and corruption and tax evasion. Such risks are exacerbated by the cross-border rights associated with citizenship of the Union".³¹⁶ In January 2019, the European Commission published a report, "Investor Citizenship and Residence Schemes in the European Union", raising such concerns.³¹⁷

281. In our Interim Report, we highlighted the work carried out by SCL to win the 2010 general election in St Kitts and Nevis, which included a sting operation, with the Opposition Leader, Lindsay Grant, being offered a bribe by an undercover operative posing as a real-estate investor. Alexander Nix told us that Christian Kalin was also running a citizenship-by-investment programme in St Kitts and Nevis at the time.³¹⁸

313 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 211.

314 [Citizenship by Investment Malta](#), Maltalmmigration.com, accessed 3 February 2019.

315 [The passport king who markets citizenship for cash](#), Juliette Garside and Hilary Osborne, The Guardian, 16 October 2018.

316 [EU fact sheet, questions and answers on the report on investor citizenship and residence schemes in the EU](#), Brussels, 23 January 2019.

317 [Investor Citizenship and Residence Schemes in the European Union](#), Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 23 January 2019.

318 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 214.

282. In 2014, the UK issued a warning that 'illicit actors' were buying passports "for the purposes of evading US or international sanctions or engaging in other financial crime".³¹⁹ This was, in part, due to the fact that St Kitts and Nevis had removed 'Place of Birth' on its passport, and the US was concerned about the scheme. The following people are among those who have acquired St Kitts and Nevis passports:

- Ali Sadr Hasheminejad: Iranian, acquired SKN passport via application managed by Henley & Partners in 2009; arrested by the US in March 2017 for money laundering sanctions violations and was bailed in May; currently subject to electronic monitoring and curfew; his Maltese bank, Pilatus, had its licence withdrawn in October 2018, for money laundering;³²⁰
- Houshang Hosseinpour, Houshang Farsoudeh and Pourya Nayebi: Iranian, acquired SKN passports in November 2011, December 2011, and November 2012 respectively; they used their SKN passports to acquire a bank in Georgia; all three men were sanctioned in 2014 by the US;³²¹
- Ren Biao: a Chinese national, who obtained his SKN passport in September 2013; he moved to SKN with his family in 2014, after China issued an Interpol red notice. He was wanted for allegedly acquiring \$100m by defrauding state institutions;³²²
- John Babikian, fled Canada in 2012 in the wake of tax evasion charges, holder of an SKN passport, prosecuted by the US Securities and Exchange Commission (SEC) in 2014 for stock fraud, and fined \$3m.³²³

283. Henley & Partners was involved in both helping to finance elections in St Kitts and Nevis, by offering and paying for SCL's services and in running that Government's economic citizenship partnership.³²⁴ SCL was part of the package, which was being offered by Henley & Partners, which calls into question whether the UK Bribery Act is enough of a regulatory brake on bad behaviour abroad. According to a senior source from the St Kitts and Nevis Labour Party, Mr. Nix has claimed that, although the company SCL has gone into administration, the people who work there are the same and so they were available to provide services to campaign management.³²⁵

284. Henley & Partners denies directly funding any election campaigns in the Caribbean on citizenship-by-investment at the same time that SCL was active in the region. A letter from Global Citizens, on behalf of Henley & Partners, was sent to the Committee

319 [Abuse of the Citizenship-by-Investment Program Sponsored by the Federation of St. Kitts and Nevis](#), Financial Crimes Enforcement Network, 20 May 2014.

320 [Malta's Pilatus Bank had European licence withdrawn](#), Hilary Osborne, The Guardian, 5 November 2018; [US arrests Iranian over alleged \\$115 million sanctions evasion scheme](#), Nate Raymond, Reuters, 20 March 2018.

321 [Case study: US man indicted in larger Iranian financial sanctions busting scheme](#), Andrea Stricker, Institute for science and international security, 3 May 2017.

322 <https://www.stabroeknews.com/2017/news/regional/05/12/controversy-rocks-st-kitts-chinese-citizen-wanted-beijing-fraud/>

323 [US Securities and Exchange Commission, SEC v John Babikian](#), 20 September 2018.

324 [Q3389](#), Jo Stevens MP and Alexander Nix, interim Report.

325 [Former Cambridge Analytica used N-word to describe Barbados PM](#), Juliette Garside and Hilary Osborne, The Guardian, 8 October 2018.

in December 2018, stating: “It is natural that there would have been a certain amount of interaction among the numerous advisors and consultants. It is entirely incorrect, however, to suggest that Henley & Partners was a formal partner to SCL in any way”.³²⁶

285. As of the end of July, 2018 when we published our Interim Report, Alexander Nix had resigned as a director within the SCL/Cambridge Analytica group of companies, which themselves had gone into administration in the UK and Chapter 7 bankruptcy in the US.

286. Alexander Nix remains, however, a shareholder of their UK parent Emerdata—formed in August, 2017, as part of a group re-organisation. Emerdata did not go into administration, continues to be an active company and has a wide shareholder base. According to the latest records, it is in turn majority owned by Cambridge Analytica Holdings LLC, a Delaware-based company.³²⁷

287. Little substantial new information has emerged from the insolvency process, save that—following the scandal—the administrators have been unable to rescue the UK companies as going concerns. Emerdata remains by far the largest creditor, sits in pole position on the official creditors committee and has been paying the substantial administration costs.³²⁸

288. Similarly, little new information has surfaced from the Chapter 7 proceedings involving the former US operating companies. A group of Facebook users have since taken legal action in a putative class action suit over privacy breaches and, in January this year, a New York court ordered Julian Wheatland—the SCL group’s former Chairman and Emerdata’s current Chief Operating Officer—to hand over corporate documents that they had requested in their case.³²⁹

289. As well as Emerdata (and its Delaware parent), one former SCL group company in the UK—SCL Insight Limited—also remains active. Based in London, it is owned by the group’s co-founder Nigel Oakes and was spun off separately during the re-organisation in 2017.

290. Following the instruction by the Secretary of State for Business, Energy and Industrial Strategy (BEIS), the Insolvency Service is currently investigating the conduct of the directors of SCL Elections Ltd, SCL Group Ltd, SCL Analytics Ltd, SCL Commercial Ltd, SCL Social Ltd and Cambridge Analytica (UK) Ltd under the provisions of the 1986 Company Directors Disqualification Act.

326 Letter from Dr Juerg Steffen CEO, The Firm of Global Citizens to Damian Collins MP, 20 December 2018.

327 Filings at Companies House for Emerdata Limited. The company’s current directors are US-based Jennifer and Rebekah Mercer (daughters of financier Robert Mercer, who is active in conservative US political circles), Hong-Kong based Gary Ka Chun Tiu and UK-based Julian Wheatland. As of 10th August, 2018, the shareholders were Cambridge Analytica Holding LLC; Alexander Tayler; Julian Wheatley; trusts for the benefit of Rebekah, Jennifer and Heather Mercer; Alexander and Catherine Nix; Jonathan, Domenica, Allegra, Marcus and Hugo Marland; JP Marland & Sons Ltd; Henry and Roger Gabb; Nigel and Alexander Oakes; Reza Saddlou-Bundy; The Glendower Trust; Trinity Gate Ltd; Ample Victory Asia Ltd; Wealth Harvest Global Ltd; Metro Luck Ltd; Knight Glory Global Ltd; and Picton Properties Ltd.

328 Filings at Companies House for SCL Group Limited, SCL Elections Limited, SCL Social Limited, SCL Analysis Limited, SCL Commercial Limited and Cambridge Analytica (UK) Limited.

329 Court reports by legal news service, Law360. The US operating companies were SCL USA Inc. and Cambridge Analytica LLC (a different entity from the Delaware holding company, Cambridge Analytica Holdings LLC) and the class action also names Facebook, Aleksandr Kogan and his company Global Science Research Ltd (GSR).

Conflicts of interest

291. The problem with many strategic communication companies is the fact that they work on campaigns that are not only unethical and possibly illegal, but also that they work against the national and security interests of the UK with campaigns for private or hostile state actors, which are at odds with UK foreign policy. Evidence in the AIQ data submitted by Chris Vickery suggests that AIQ was either working with, or planning to work on a political campaign for the Osnova party in Ukraine. The Osnova Party was created by politician and businessman Serhiy Taruta. According to an Atlantic Council article, Mr Taruta has claimed that the majority of Ukrainians do not support NATO, contrary to other polling. The same article says that Osnova argues for making 'compromises' with Ukraine's neighbours.³³⁰

292. When we asked Jeff Silvester, CEO of AIQ, about Osnova and whether AIQ was working on the Ukrainian elections in 2019, Mr Silvester replied: "Osnova is a political party in the Ukraine. We have a client that we created an Android and IOS app for, and they are working with Osnova".³³¹ Ukraine is a country where the UK Ministry of Defence and the Foreign and Commonwealth Office have a deep interest in safeguarding its national security in the face of Russian aggression.

293. In our Interim Report, we stated:

Equally worrying is the fact that the SCL Group carried out work "for the British Government, the US Government and other allied Governments", 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. 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. 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".³³²

This raises the profound issue of whether companies working on election campaigns overseas in this way should also be winning projects from the UK Ministry of Defence and the Foreign and Commonwealth Office.

294. When Brittany Kaiser gave evidence to us in the spring of 2018, she discussed the porous nature between the commercial, the political and defence work of SCL, and that prior to 2015, the 'target audience analysis' (TAA) methodology was considered a weapon—"weapons grade communications tactics"—and the UK Government had to be told if it was going to be deployed in another country.³³³

330 [Serhiy Taruta: yet another champion of 'painful compromises'](#), Vitali Rybak, Atlantic Council, 25 September 2018.

331 [Q3130](#) and [Q3131](#).

332 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 228.

333 [Q1560](#)

295. Emma Briant, Senior Lecturer at the University of Essex, supports stricter regulation of strategic communications companies, with the establishment of professional licensing that can be revoked if necessary. Such licensing “would commercially protect the industry itself, creating a resulting ‘soft power’ economic benefit for industry and Western governments”.³³⁴ She gave two examples of Cambridge Analytica’s perceived conflicts of interests: Cambridge Analytica’s pitches to Lukoil, a Russian oil company with ubiquitous political connections, while at the same time the SCL Group was delivering counter-Russian propaganda training for NATO; and that “around the same time, Alexander Nix from Cambridge Analytica contacted Julian Assange at Wikileaks amplifying the release of damaging emails; Russia has been accused of the hacking of these, which it denies”.³³⁵

296. As we have stated, Emerdata is the major creditor of SCL Elections Ltd and has been paying the substantial administration costs.³³⁶ Given the fact that many senior personnel of SCL Elections Ltd/Cambridge Analytica are prominent in Emerdata, there is concern that the work of Cambridge Analytica is continuing, albeit under a different name. *We stated in our Interim Report that “SCL Group and associated companies have gone into administration, but other companies are carrying out similar work. Senior individuals involved in SCL and Cambridge Analytica appear to have moved onto new corporate vehicles.”*³³⁷ *We recommended that “the National Crime Agency, if it is not already, should investigate the connections between the company SCL Elections Ltd and Emerdata Ltd.”*³³⁸ *We repeat those recommendations in this Report.*

297. In October 2018, the Secretary of State for DCMS, Rt Hon Jeremy Wright MP, was asked by the Committee whether the current law in the UK relating to lobbying companies such as SCL was fit for purpose. He was not forthcoming in his response, stating that the ICO should investigate the work of the SCL “that will, I think, give us an indication of whether, first something has gone wrong in this case and, secondly, if it has, whether that indicates a structural weakness that we need to address”.³³⁹ He did not respond to the specific question about whether the law relating to lobbying companies such as SCL was fit for purpose. We believe that it is not fit for purpose; the current self-regulation of lobbying companies is not working.

298. *We recommend that the Government looks into ways that PR and strategic communications companies are audited, possibly by an independent body, to ensure that their campaigns do not conflict with the UK national interest and security concerns and do not obstruct the imposition of legitimate sanctions, as is the case currently with the legal selling of passports. Barriers need to be put in place to ensure that such companies cannot work on both sensitive UK Government projects and with clients whose intention might be to undermine those interests.*

299. *The transformation of Cambridge Analytica into Emerdata illustrates how easy it is for discredited companies to reinvent themselves and potentially use the same data and*

334 [FKN0099](#)

335 As above.

336 Filings at Companies House for SCL Group Limited, SCL Elections Limited, SCL Social Limited, SCL Analysis Limited, SCL Commercial Limited and Cambridge Analytica (UK) Limited.

337 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 135.

338 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, para 134.

339 [Q253](#) Oral evidence, 24 October 2018, Work of the Department for Digital, Culture, Media and Sport.

the same tactics to undermine governments, including in the UK. The industry needs cleaning up. As the SCL/Cambridge Analytica scandal shows, the sort of bad practices indulged in abroad or for foreign clients, risk making their way into UK politics. Currently the strategic communications industry is largely self-regulated. The UK Government should consider new regulations that curb bad behaviour in this industry.

300. *There needs to be transparency in these strategic communications companies, with a public record of all campaigns that they work on, both at home and abroad. They need to be held accountable for breaking laws during campaigns anywhere in the world, or working for financially non-transparent campaigns. We recommend that the Government addresses this issue, when it responds to its consultation, 'Protecting the Debate: Intimidating, Influence and Information'.*

301. *We recommend that the Government revisits the UK Bribery Act, to gauge whether the legislation is enough of a regulatory brake on bad behaviour abroad. We also look to the Government to explore the feasibility of adopting a UK version of the US Foreign Agents and Registration Act (FARA), which requires "persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationships with the foreign principal, as well as activities, receipts and disbursements in support of those activities".*

8 Digital literacy

Introduction

302. It is hard to differentiate on social media between content that is true, that is misleading, or that is false, especially when those messages are targeted at an individual level. Children and adults need to be equipped with the necessary information and critical analysis to understand content on social media, to work out what is accurate and trustworthy, and what is not. Furthermore, people need to be aware of the rights that they have over their own personal data, and what they should do when they want their data removed.

303. The majority of our witnesses stressed the need for greater digital literacy among users of social media. Ofcom has a statutory duty to promote media literacy, which it defines as “the ability to use, understand and create media and communications in a variety of contexts”. Sharon White told us that their focus on digital literacy is from a research base, “about how children use and understand the internet and similarly with adults”.³⁴⁰ We cannot stress highly enough the importance of greater public understanding of digital information—its use, scale, importance and influence.

304. Greater public understanding of what people read on social media has been helped by organisations working towards greater transparency on content. For example, journalists at the NewsGuard company apply nine criteria relating to credibility and transparency to news and information website—using ‘Nutrition Labels’, explaining each website’s history, ownership, financing and transparency. In January 2019, Microsoft integrated NewsGuard’s ratings into its Edge mobile browser.³⁴¹

305. We received evidence from the Disinformation Index, an organisation that assigns a rating to each outlet based on the probability of that outlet carrying disinformation: “In much the same way as credit rating agencies rate countries and financial products with AAA for low risk all the way to Junk status for the most risky investments, so the index will do for media outlets”.³⁴²

306. Facebook gives the impression of wanting to tackle disinformation on its site. In January 2019, Facebook employed Full Fact to review and rate the accuracy of news stories on Facebook—including the production of evaluation reports every three months—as part of its third-party factchecking programme, the first time that such an initiative has been operated in the UK.³⁴³ However, as we described in Chapter 5, Facebook has also recently blocked the work of organisations such as Who Targets Me? from helping the public to understand how and why they are being targeted with online adverts. **On the one hand, Facebook gives the impression of working towards transparency, with regard to the auditing of its news content; but on the other, there is considerable obfuscation concerning the auditing of its adverts, which provide Facebook with its ever-increasing revenue. To make informed judgments about the adverts presented to them on Facebook, users need to see the source and purpose behind the content.**

340 [Q3833](#)

341 [NewsGuard criteria for and explanation of ratings](#), NewsGuard website.

342 [FKN0058](#)

343 [Full fact to start checking Facebook content as third-party factchecking initiative reaches the UK](#), FullFact, 11 January 2019.

307. Elizabeth Denham described the ICO's "Your Data Matters" campaign, which has been running since April 2018: "It is an active campaign and I think that it has driven more people to file more complaints against companies as well as to us".³⁴⁴ She also stressed the need for the public to both understand their rights and also "make citizens more digitally literate so that they know how to navigate the internet and be able to exercise their rights". The Information Commissioner said that the ICO had a role to play in that, but did not necessarily have the resources.³⁴⁵

308. In our Interim Report, we recommended that the Government put forward proposals in its White Paper for an educational levy to be raised on social media companies, to finance a comprehensive framework based online, ensuring that digital literacy is treated as the fourth pillar of education, alongside reading, writing and maths.³⁴⁶ In its response, the Government stated that it was continuing to build an evidence base to inform its approach in regard to any social media levy, and that it would not want to impact on existing work done by charities and other organisations on tackling online harms. It did not agree that digital literacy should be the fourth pillar of education, since it "is already taught across the national school curriculum."³⁴⁷

Friction in the system

309. The term 'friction' represents anything that slows down a process or function. In 2011 Mark Zuckerberg announced that apps would no longer generate pop-up messages, asking users whether they wanted to publish their latest activity on their Facebook feed; instead Facebook created apps that would post directly onto users' feeds, without the need for permission. Mr Zuckerberg said, "from here on out, it's a frictionless experience".³⁴⁸

310. Some believe that friction should be reintroduced into the online experience, by both tech companies and by individual users themselves, in order to recognise the need to pause and think before generating or consuming content. There is a tendency to think of digital literacy as being the responsibility of those teaching and those learning it. However, algorithms can also play their part in digital literacy. 'Friction' can be incorporated into the system, to give people time to think about what they are writing and what they are sharing and to give them the ability to limit the time they spend online; there should be obstacles put in their place to make the process of posting or sharing more thoughtful or slower. For example, this additional friction could include: the ability to share a post or a comment, only if the sharer writes about the post; the option to share a post only when it has been read in its entirety; and a way of monitoring what is about to be sent, before it is sent.³⁴⁹

311. The Center for Humane Technology suggests simple methods for individuals themselves to adopt, to build friction into mobile devices, including: turning off all notifications, apart from people; changing the colour of the screen to 'grayscale', thereby

344 [Q3983](#)

345 [Q3983](#)

346 [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, 29 July 2018, p. 63.

347 [DCMS Committee, Disinformation and 'fake news': Interim Report: Government Response to the Committee's Fifth Report of Session 2017](#), p. 20.

348 [Is Tech too easy to use?](#) Kevin Roose, The New York Times, 12 December 2018.

349 [The Center for Humane Technology](#) website.

reducing the intensity and lure of bright colours; keeping home screen to tools only; launching apps by typing; charging devices outside people's bedrooms; removing social media from mobile devices; and telephoning instead of texting.³⁵⁰

Regulators and digital literacy

312. *As we wrote in our Interim Report, digital literacy should be a fourth pillar of education, alongside reading, writing and maths. In its response, the Government did not comment on our recommendation of a social media company levy, to be used, in part, to finance a comprehensive educational framework—developed by charities, NGOs, and the regulators themselves—and based online. Such a framework would inform people of the implications of sharing their data willingly, their rights over their data, and ways in which they can constructively engage and interact with social media sites. People need to be resilient about their relationship with such sites, particular around what they read and what they write. We reiterate this recommendation to the Government, and look forward to its response.*

313. *The public need to know more about their ability to report digital campaigning that they think is misleading and or unlawful. Ofcom, the ASA, the ICO and the Electoral Commission need to raise their profiles so that people know about their services and roles. The Government should take a leading role in co-ordinating this crucial service for the public. The Government must provide clarity for members of the public about their rights with regards to social media companies.*

314. *Social media users need online tools to help them distinguish between quality journalism, and stories coming from organisations that have been linked to disinformation or are regarded as being unreliable sources. The social media companies should be required to either develop tools like this for themselves, or work with existing providers, such as Newsguard, to make such services available for their users. The requirement for social media companies to introduce these measures could form part of a new system of content regulation, based on a statutory code, and overseen by an independent regulator, as we have discussed earlier in this report.*

315. *Social media companies need to be more transparent about their own sites, and how they work. Rather than hiding behind complex agreements, they should be informing users of how their sites work, including curation functions and the way in which algorithms are used to prioritise certain stories, news and videos, depending on each user's profile. The more people know how the sites work, and how the sites use individuals' data, the more informed we shall all be, which in turn will make choices about the use and privacy of sites easier to make.*

316. *Ofcom, the ICO, the Electoral Commission and the Advertising Standards Authority have all written separately about their role in promoting digital literacy. We recommend that the Government ensures that the four main regulators produce a more united strategy in relation to digital literacy. Included in this united approach should be a public discussion on how we, as individuals, are happy for our data to be used and shared. People need to know how their data is being used (building on recommendations we set out in Chapter Two of this Final Report). Users need to know how to set the boundaries that they want to, and how those boundaries should be set,*

350 Same as above.

with regard to their personal data. Included in this debate should be arguments around whether users want an agreed basic expectation of privacy, in a similar vein to a basic level of hygiene. Users could have the ability of opting out of such minimum thresholds, if they chose.

317. We recommend that participating in social media should allow more pause for thought. More obstacles or 'friction' should be both incorporated into social media platforms and into users' own activities—to give people time to consider what they are writing and sharing. Techniques for slowing down interaction online should be taught, so that people themselves question both what they write and what they read—and that they pause and think further, before they make a judgement online.

Conclusions and recommendations

Regulation and the role, definition and legal liability of tech companies

1. *Social media companies cannot hide behind the claim of being merely a 'platform' and maintain that they have no responsibility themselves in regulating the content of their sites. We repeat the recommendation from our Interim Report 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'. This approach would see the tech companies assume legal liability for content identified as harmful after it has been posted by users. We ask the Government to consider this new category of tech company in its forthcoming White Paper. (Paragraph 14)*
2. *By choosing not to appear before the Committee and by choosing not to respond personally to any of our invitations, Mark Zuckerberg has shown contempt towards both the UK Parliament and the 'International Grand Committee', involving members from nine legislatures from around the world. (Paragraph 29)*
3. *Our Interim Report recommended that clear legal liabilities should be established for tech companies to act against harmful or illegal content on their sites. There is now an urgent need to establish independent regulation. We believe that a compulsory Code of Ethics should be established, overseen by an independent regulator, setting out what constitutes harmful content. The independent regulator would have statutory powers to monitor relevant tech companies; this would create a regulatory system for online content that is as effective as that for offline content industries. (Paragraph 37)*
4. *As we said in our Interim Report, such a Code of Ethics should be similar to the Broadcasting Code issued by Ofcom—which is based on the guidelines established in section 319 of the 2003 Communications Act. The Code of Ethics should be developed by technical experts and overseen by the independent regulator, in order to set down in writing what is and is not acceptable on social media. This should include harmful and illegal content that has been referred to the companies for removal by their users, or that should have been easy for tech companies themselves to identify. (Paragraph 38)*
5. *The process should establish clear, legal liability for tech companies to act against agreed harmful and illegal content on their platform and such companies should have relevant systems in place to highlight and remove 'types of harm' and to ensure that cyber security structures are in place. If tech companies (including technical engineers involved in creating the software for the companies) are found to have failed to meet their obligations under such a Code, and not acted against the distribution of harmful and illegal content, the independent regulator should have the ability to launch legal proceedings against them, with the prospect of large fines being administered as the penalty for non-compliance with the Code. (Paragraph 39)*
6. *This same public body should have statutory powers to obtain any information from social media companies that are relevant to its inquiries. This could include the capability to check what data is being held on an individual user, if a user requests such information. This body should also have access to tech companies' security*

mechanisms and algorithms, to ensure they are operating responsibly. This public body should be accessible to the public and be able to take up complaints from members of the public about social media companies. We ask the Government to put forward these proposals in its forthcoming White Paper. (Paragraph 40)

7. *We support the recommendation from the ICO that inferred data should be as protected under the law as personal information. Protections of privacy law should be extended beyond personal information to include models used to make inferences about an individual. We recommend that the Government studies the way in which the protections of privacy law can be expanded to include models that are used to make inferences about individuals, in particular during political campaigning. This will ensure that inferences about individuals are treated as importantly as individuals' personal information. (Paragraph 48)*
8. *In our Interim Report, we recommended a levy should be placed on tech companies operating in the UK to support the enhanced work of the ICO. We reiterate this recommendation. The Chancellor's decision, in his 2018 Budget, to impose a new 2% digital services tax on UK revenues of big technology companies from April 2020, shows that the Government is open to the idea of a levy on tech companies. The Government's response to our Interim Report implied that it would not be financially supporting the ICO any further, contrary to our recommendation. We urge the Government to reassess this position. (Paragraph 51)*
9. *The new independent system and regulation that we recommend should be established must be adequately funded. We recommend that a levy is placed on tech companies operating in the UK to fund its work. (Paragraph 52)*

Data Use and data targeting

10. The Cambridge Analytica scandal was facilitated by Facebook's policies. If it had fully complied with the FTC settlement, it would not have happened. The US Federal Trade Commission (FTC) Complaint of 2011 ruled against Facebook—for not protecting users' data and for letting app developers gain as much access to user data as they liked, without restraint—and stated that Facebook built their company in a way that made data abuses easy. When asked about Facebook's failure to act on the FTC's complaint, Elizabeth Denham, the Information Commissioner, told us: "I am very disappointed that Facebook, being such an innovative company, could not have put more focus, attention and resources into protecting people's data". We are equally disappointed. (Paragraph 76)
11. The evidence that we obtained from the Six4Three court documents indicates that Facebook was willing to override its users' privacy settings in order to transfer data to some app developers, to charge high prices in advertising to some developers, for the exchange of that data, and to starve some developers—such as Six4Three—of that data, thereby causing them to lose their business. It seems clear that Facebook was, at the very least, in violation of its Federal Trade Commission settlement. (Paragraph 135)
12. *The Information Commissioner told the Committee that Facebook needs to significantly change its business model and its practices to maintain trust. From the documents*

we received from Six4Three, it is evident that Facebook intentionally and knowingly violated both data privacy and anti-competition laws. The ICO should carry out a detailed investigation into the practices of the Facebook Platform, its use of users' and users' friends' data, and the use of 'reciprocity' of the sharing of data. (Paragraph 136)

13. Ireland is the lead authority for Facebook, under GDPR, and we hope that these documents will provide useful evidence for Helen Dixon, the Irish Data Protection Commissioner, in her current investigations into the way in which Facebook targeted, monitored, and monetised its users. (Paragraph 137)
14. *In our Interim Report, we stated that the dominance of a handful of powerful tech companies has resulted in their behaving as if they were monopolies in their specific area, and that there are considerations around the data on which those services are based. Facebook, in particular, is unwilling to be accountable to regulators around the world. The Government should consider the impact of such monopolies on the political world and on democracy. (Paragraph 138)*
15. *The Competitions and Market Authority (CMA) should conduct a comprehensive audit of the operation of the advertising market on social media. The Committee made this recommendation its interim report, and we are pleased that it has also been supported in the independent Cairncross Report commissioned by the government and published in February 2019. Given the contents of the Six4Three documents that we have published, it should also investigate whether Facebook specifically has been involved in any anti-competitive practices and conduct a review of Facebook's business practices towards other developers, to decide whether Facebook is unfairly using its dominant market position in social media to decide which businesses should succeed or fail. We hope that the Government will include these considerations when it reviews the UK's competition powers in April 2019, as stated in the Government response to our Interim Report. Companies like Facebook should not be allowed to behave like 'digital gangsters' in the online world, considering themselves to be ahead of and beyond the law. (Paragraph 139)*
16. From the evidence we received, which has been supported by the findings of both the ICO and the Electoral Commission, it is clear that a porous relationship existed between Eldon Insurance and Leave.EU, with staff and data from one organisation augmenting the work of the other. There was no attempt to create a strict division between the two organisations, in breach of current laws. We look forward to hearing the findings of the ICO's audits into the two organisations. (Paragraph 146)
17. As set out in our Interim Report, Arron Banks and Andy Wigmore showed complete disregard and disdain for the parliamentary process when they appeared before us in June 2018. It is now evident that they gave misleading evidence to us, too, about the working relationship between Eldon Insurance and Leave.EU. They are individuals, clearly, who have less than a passing regard for the truth. (Paragraph 147)

Aggregate IQ

18. There is clear evidence that there was a close working relationship between Cambridge Analytica, SCL and AIQ. There was certainly a contractual relationship, but we

believe that the information revealed from the repository would imply something closer, with data exchanged between both AIQ and SCL, as well as between AIQ and Cambridge Analytica. (Paragraph 166)

19. AIQ worked on both the US Presidential primaries and for Brexit-related organisations, including the designated Vote Leave group, during the EU Referendum. The work of AIQ highlights the fact that data has been and is still being used extensively by private companies to target people, often in a political context, in order to influence their decisions. It is far more common than people think. The next chapter highlights the widespread nature of this targeting. (Paragraph 192)

Advertising and political campaigning

20. *We repeat the recommendation from our Interim Report, that the Government should look at the ways in which the UK law should define digital campaigning, including having agreed definitions of what constitutes online political advertising, such as agreed types of words that continually arise in adverts that are not sponsored by a specific political party. There also needs to be an acknowledgement of the role and power of unpaid campaigns and Facebook Groups that influence elections and referendums (both inside and outside the designated period).* (Paragraph 210)
21. *Electoral law is not fit for purpose and needs to be changed to reflect changes in campaigning techniques, and the move from physical leaflets and billboards to online, microtargeted political campaigning. There needs to be: absolute transparency of online political campaigning, including clear, persistent banners on all paid-for political adverts and videos, indicating the source and the advertiser; a category introduced for digital spending on campaigns; and explicit rules surrounding designated campaigners' role and responsibilities.* (Paragraph 211)
22. *We would expect that the Cabinet Office's consultation will result in the Government concluding that paid-for political advertising should be publicly accessible, clear and easily recognisable. Recipients should be able to identify the source, who uploaded it, who sponsored it, and its country of origin.* (Paragraph 212)
23. *The Government should 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; defining what constitutes political campaigning; and reducing the time for spending returns to be sent to the Electoral Commission.* (Paragraph 213)
24. *The Government should explore ways in which the Electoral Commission can be given more powers to carry out its work comprehensively, including the following measures:*
 - *the legal right to compel organisations that they do not currently regulate, including social media companies, to provide information relevant to their inquiries;*
 - *The Electoral Commission's current maximum fine limit of £20,000 should be increased, and changed to a fine based on a fixed percentage of turnover, in line with powers already conferred on other statutory regulators;*

- *The ability for the Electoral Commission to petition against an election due to illegal actions, which currently can only be brought by an individual;*
 - *The ability for the Electoral Commission to intervene or stop someone acting illegally in a campaign if they live outside the UK. (Paragraph 214)*
25. *Political advertising items should be publicly accessible in a searchable repository—who is paying for the ads, which organisations are sponsoring the ad, who is being targeted by the ads—so that members of the public can understand the behaviour of individual advertisers. It should be run independently of the advertising industry and of political parties. This recommendation builds on paragraph 144 of our Interim Report. (Paragraph 215)*
 26. *We agree with the ICO's proposal that a Code of Practice, which highlights the use of personal information in political campaigning and applying to all data controllers who process personal data for the purpose of political campaigning, should be underpinned by primary legislation. We urge the Government to act on the ICO's recommendation and bring forward primary legislation to place these Codes of Practice into statute. (Paragraph 216)*
 27. *We support the ICO's recommendation that all political parties should work with the ICO, the Cabinet Office and the Electoral Commission, to identify and implement a cross-party solution to improve transparency over the use of commonly-held data. This would be a practical solution to ensure that the use of data during elections and referenda is treated lawfully. We hope that the Government will work towards making this collaboration happen. We hope that the Government will address all of these issues when it responds to its consultation, "Protecting the Debate: Intimidating, Influence, and Information" and to the Electoral Commission's report, "Digital Campaigning: increasing transparency for voters". A crucial aspect of political advertising and influence is that of foreign interference in elections, which we hope it will also strongly address. (Paragraph 217)*
 28. *Mainstream Network is yet another, more recent example of an online organisation seeking to influence political debate using methods similar to those which caused concern over the EU Referendum and there is no good case for Mainstream Network to hide behind anonymity. We look forward to receiving information from Facebook about the origins of Mainstream Network, which—to date—we have not received, despite promises from Richard Allan that he would provide the information. We consider Facebook's response generally to be disingenuous and another example of Facebook's bad faith. The Information Commissioner has confirmed that it is currently investigating this website's activities and Facebook will, in any event, have to co-operate with the ICO. (Paragraph 222)*
 29. *Tech companies must address the issue of shell companies and other professional attempts to hide identity in advert purchasing, especially around political advertising—both within and outside campaigning periods. There should be full disclosure of the targeting used as part of advertising transparency. The Government should explore ways of regulating the use of external targeting on social media platforms, such as Facebook's Custom Audiences. (Paragraph 223)*

30. Donations made to political parties in Northern Ireland before July 2017 are protected from disclosure, under Section 71E of the Political Parties, Elections and Referendums Act 2000. This prevents the Electoral Commission from disclosing any information relating to such donations before July 2017. We concur with the Electoral Commission that it is “deeply regrettable” that they are unable, by law, to tell Members of Parliament and the public about details surrounding the source of the £435,000 donation that was given by the Constitutional Research Council (CRC) to the DUP or the due diligence that was followed. Because of the law as it currently stands, this Committee and the wider public have no way of investigating the source of the £435,000 donation to the DUP made on behalf of the CRC and are prevented from even knowing whether it came from an organisation, whose membership had either sanctioned the donation or not, or from a wealthy individual. (Paragraph 232)
31. *There is an absence of transparency surrounding the relationship between the Constitutional Research Council, the DUP and Vote Leave. We believe that, in order to avoid having to disclose the source of this £435,000 donation, the CRC, deliberately and knowingly, exploited a loophole in the electoral law to funnel money to the Democratic Unionist Party in Northern Ireland. That money was used to fund pro-Brexit newspaper advertising outside Northern Ireland and to pay the Canadian-based data analytics company, Aggregate IQ.* (Paragraph 233)
32. *We support the Electoral Commission in its request that the Government extend the transparency rules around donations made to political parties in Northern Ireland from 2014. This period of time would cover two UK general elections, two Northern Ireland Assembly elections, the Scottish independence referendum, the EU referendum, and EU and local government elections. We urge the Government to make this change in the law as soon as is practicable to ensure full transparency over these elections and referendums.* (Paragraph 234)
33. *We welcome Dame Frances Cairncross’s report on safeguarding the future of journalism, and the establishment of a code of conduct to rebalance the relationship between news providers and social media platforms. In particular, we welcome the recommendation that online digital newspapers and magazines should be zero rated for VAT, as is the case for printed versions. This would remove the false incentive for news companies against developing more paid-for digital services. We support the recommendation that chimes with our own on investigating online advertising, in particular focussing on the major search and social media companies, by the Competitions and Markets Authority.* (Paragraph 236)

Foreign influence in political campaigns

34. *In common with other countries, the UK is clearly vulnerable to covert digital influence campaigns and the Government should be conducting analysis to understand the extent of the targeting of voters, by foreign players, during past elections. We ask the Government whether current legislation to protect the electoral process from malign influence is sufficient. Legislation should be in line with the latest technological developments, and should be explicit on the illegal influencing of the democratic process by foreign players. We urge the Government to look into this issue and to respond in its White Paper.* (Paragraph 249)

35. We are pleased that our recommendation set out in the Interim Report in July 2018, concerning Arron Banks and his donation, has been acted on by both the Electoral Commission—which has concerns that Banks is not the ‘true source’ of the donation—and by the National Crime Agency, which is currently investigating the source of the donation. (Paragraph 266)
36. *There is a general principle that, subject to certain spending limits, funding from abroad is not allowed in UK elections. However, as the Electoral Commission has made clear, the current rules do not explicitly ban overseas spending. We recommend that, at the earliest opportunity, the Government reviews the current rules on overseas involvement in our UK elections to ensure that foreign interference in UK elections, in the form of donations, cannot happen. We also need to be clear that Facebook, and all platforms, have a responsibility to comply with the law and not to facilitate illegal activity.* (Paragraph 267)
37. Information operations are part of a complex, interrelated group of actions that promote confusion and unrest through information systems, such as social media companies. These firms, in particular Facebook, need to take action against untransparent administrators of groups, which are being used for political campaigns. They also need to impose much more stringent punishment on users who abuse the system. Merely having a fake disinformation account shut down, but being able to open another one the next moment, is hardly a deterrent. (Paragraph 271)
38. *The Government should put pressure on social media companies to publicise any instances of disinformation. The Government needs to ensure that social media companies share information they have about foreign interference on their sites—including who has paid for political adverts, who has seen the adverts, and who has clicked on the adverts—with the threat of financial liability if such information is not forthcoming. Security certificates, authenticating social media accounts, would ensure that a real person was behind the views expressed on the account.* (Paragraph 272)
39. *We repeat our call to the Government to make a statement about how many investigations are currently being carried out into Russian interference in UK politics. We further recommend that the Government launches an independent investigation into past elections—including the UK election of 2017, the UK Referendum of 2016, and the Scottish Referendum of 2014—to explore what actually happened with regard to foreign influence, disinformation, funding, voter manipulation, and the sharing of data, so that appropriate changes to the law can be made and lessons can be learnt for future elections and referenda.* (Paragraph 273)

SCL influence in foreign elections

40. *We stated in our Interim Report that “SCL Group and associated companies have gone into administration, but other companies are carrying out similar work. Senior individuals involved in SCL and Cambridge Analytica appear to have moved onto new corporate vehicles.” We recommended that “the National Crime Agency, if it is not already, should investigate the connections between the company SCL Elections Ltd and Emerdata Ltd. We repeat those recommendations in this Report.* (Paragraph 296)

41. *We recommend that the Government looks into ways that PR and strategic communications companies are audited, possibly by an independent body, to ensure that their campaigns do not conflict with the UK national interest and security concerns and do not obstruct the imposition of legitimate sanctions, as is the case currently with the legal selling of passports. Barriers need to be put in place to ensure that such companies cannot work on both sensitive UK Government projects and with clients whose intention might be to undermine those interests. (Paragraph 298)*
42. *The transformation of Cambridge Analytica into Emerdata illustrates how easy it is for discredited companies to reinvent themselves and potentially use the same data and the same tactics to undermine governments, including in the UK. The industry needs cleaning up. As the SCL/Cambridge Analytica scandal shows, the sort of bad practices indulged in abroad or for foreign clients, risk making their way into UK politics. Currently the strategic communications industry is largely self-regulated. The UK Government should consider new regulations that curb bad behaviour in this industry. (Paragraph 299)*
43. *There needs to be transparency in these strategic communications companies, with a public record of all campaigns that they work on, both at home and abroad. They need to be held accountable for breaking laws during campaigns anywhere in the world, or working for financially non-transparent campaigns. We recommend that the Government addresses this issue, when it responds to its consultation, 'Protecting the Debate: Intimidating, Influence and Information'. (Paragraph 300)*
44. *We recommend that the Government revisits the UK Bribery Act, to gauge whether the legislation is enough of a regulatory brake on bad behaviour abroad. We also look to the Government to explore the feasibility of adopting a UK version of the US Foreign Agents and Registration Act (FARA), which requires "persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationships with the foreign principal, as well as activities, receipts and disbursements in support of those activities". (Paragraph 301)*

Digital literacy

45. *On the one hand, Facebook gives the impression of working towards transparency, with regard to the auditing of its news content; but on the other, there is considerable obfuscation concerning the auditing of its adverts, which provide Facebook with its ever-increasing revenue. To make informed judgments about the adverts presented to them on Facebook, users need to see the source and purpose behind the content. (Paragraph 306)*
46. *As we wrote in our Interim Report, digital literacy should be a fourth pillar of education, alongside reading, writing and maths. In its response, the Government did not comment on our recommendation of a social media company levy, to be used, in part, to finance a comprehensive educational framework—developed by charities, NGOs, and the regulators themselves—and based online. Such a framework would inform people of the implications of sharing their data willingly, their rights over their data, and ways in which they can constructively engage and interact with social media*

sites. People need to be resilient about their relationship with such sites, particularly around what they read and what they write. We reiterate this recommendation to the Government, and look forward to its response. (Paragraph 312)

47. *The public need to know more about their ability to report digital campaigning that they think is misleading and or unlawful. Ofcom, the ASA, the ICO and the Electoral Commission need to raise their profiles so that people know about their services and roles. The Government should take a leading role in co-ordinating this crucial service for the public. The Government must provide clarity for members of the public about their rights with regards to social media companies. (Paragraph 313)*
48. *Social media users need online tools to help them distinguish between quality journalism, and stories coming from organisations that have been linked to disinformation or are regarded as being unreliable sources. The social media companies should be required to either develop tools like this for themselves, or work with existing providers, such as Newsguard, to make such services available for their users. The requirement for social media companies to introduce these measures could form part of a new system of content regulation, based on a statutory code, and overseen by an independent regulator, as we have discussed earlier in this report. (Paragraph 314)*
49. Social media companies need to be more transparent about their own sites, and how they work. Rather than hiding behind complex agreements, they should be informing users of how their sites work, including curation functions and the way in which algorithms are used to prioritise certain stories, news and videos, depending on each user's profile. The more people know how the sites work, and how the sites use individuals' data, the more informed we shall all be, which in turn will make choices about the use and privacy of sites easier to make. (Paragraph 315)
50. *Ofcom, the ICO, the Electoral Commission and the Advertising Standards Authority have all written separately about their role in promoting digital literacy. We recommend that the Government ensures that the four main regulators produce a more united strategy in relation to digital literacy. Included in this united approach should be a public discussion on how we, as individuals, are happy for our data to be used and shared. People need to know how their data is being used (building on recommendations we set out in Chapter Two of this Final Report). Users need to know how to set the boundaries that they want to, and how those boundaries should be set, with regard to their personal data. Included in this debate should be arguments around whether users want an agreed basic expectation of privacy, in a similar vein to a basic level of hygiene. Users could have the ability of opting out of such minimum thresholds, if they chose. (Paragraph 316)*
51. We recommend that participating in social media should allow more pause for thought. More obstacles or 'friction' should be both incorporated into social media platforms and into users' own activities—to give people time to consider what they are writing and sharing. Techniques for slowing down interaction online should be taught, so that people themselves question both what they write and what they read—and that they pause and think further, before they make a judgement online. (Paragraph 317)

Annex 1 'International Grand Committee' attendees, Tuesday 27 November 2018

Argentina: Leopoldo Moreau, Chair, Freedom of Expression Commission, Chamber of Deputies

Belgium: Nele Lijnen, member, Committee on Infrastructure, Communications and Public Enterprises, Parliament of Belgium

Brazil: Alessandro Molon, Member of the Chamber of Deputies

Canada: Bob Zimmer, Chair, Standing Committee on Access to Information, Privacy and Ethics, House of Commons; Nathaniel Erskine-Smith, Vice-chair, Standing Committee on Access to Information, Privacy and Ethics, House of Commons; Charlie Angus, Vice-chair, Standing Committee on Access to Information, Privacy and Ethics, House of Commons

France: Catherine Morin-Desailly, Chair, Standing Committee on Culture, Education and Media, French Senate

Ireland: Hildegard Naughton, Chair, Joint Committee on Communications, Climate Action and Environment; Eamon Ryan, member, Joint Committee on Communications, Climate Action and Environment

Latvia: Inese Libina-Egnere, Deputy Speaker

Singapore: Pritam Singh, Member, Select Committee on Deliberate Online Falsehoods; Edwin Tong, Member, Select Committee on Deliberate Online Falsehoods; Sun Xueling, Member, Select Committee on Deliberate Online Falsehoods

United Kingdom: Damian Collins, Chair, Digital, Culture, Media and Sport Committee, House of Commons; Clive Efford, Member, Digital, Culture, Media and Sport Committee, House of Commons; Julie Elliott, Member, Digital, Culture, Media and Sport Committee, House of Commons; Paul Farrelly, Member, Digital, Culture, Media and Sport Committee, House of Commons; Simon Hart, Member, Digital, Culture, Media and Sport Committee, House of Commons; Julian Knight, Member, Digital, Culture, Media and Sport Committee, House of Commons; Ian C. Lucas, Member, Digital, Culture, Media and Sport Committee, House of Commons; Brendan O'Hara, Member, Digital, Culture, Media and Sport Committee, House of Commons; Rebecca Pow, Member, Digital, Culture, Media and Sport Committee, House of Commons; Jo Stevens, Member, Digital, Culture, Media and Sport Committee, House of Commons; Giles Watling, Member, Digital, Culture, Media and Sport Committee, House of Commons.

Annex 2 International Principles on the Regulation of Tech Platforms

**‘INTERNATIONAL GRAND COMMITTEE’
ON DISINFORMATION AND FAKE NEWS**

Preamble
We the undersigned:—

Members of the national Parliaments of: the Argentine Republic; the Kingdom of Belgium; the Federative Republic of Brazil; Canada; the French Republic; Ireland; the Republic of Latvia; the Republic of Singapore; and the United Kingdom of Great Britain and Northern Ireland.

Noting that:— the world in which the traditional institutions of democratic government operate is changing at an unprecedented pace; it is an urgent and critical priority for legislatures and governments to ensure that the fundamental rights and safeguards of their citizens are not violated or undermined by the unchecked march of technology; the democratic world order is suffering a crisis of trust from the growth of disinformation, the proliferation of online aggression and hate speech, concerted attacks on our common democratic values of tolerance and respect for the views of others, and the widespread misuse of data belonging to citizens to enable these attempts to sabotage open and democratic processes, including elections.

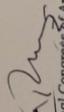
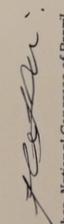
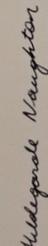
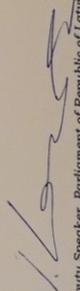
Affirming that:— representative democracy is too important and too hard-won to be left undefended from online harms, in particular aggressive campaigns of disinformation launched from one country against citizens in another, and the co-ordinated activity of fake accounts using data-targeting methods to try manipulate the information that people see on social media.

Believing that:— it is incumbent on us to create a system of global internet governance that can serve to protect the fundamental rights and freedoms of generations to come, based on established codes of conduct for agencies working for nation states, and govern the major international tech platforms which have created the systems that serve online content to billions of users around the world.

Declaration
In the interests of transparency, accountability and the protection of representative democracy we hereby declare and endorse the following principles:

- i. The internet is global and law relating to it must derive from globally agreed principles;
- ii. The deliberate spreading of disinformation and division is a credible threat to the continuation and growth of democracy and a civilising global dialogue;
- iii. Global technology firms must recognise their great power and demonstrate their readiness to accept their great responsibility as holders of influence;
- iv. Social Media companies should be held liable if they fail to comply with a judicial, statutory or regulatory order to remove harmful and misleading content from their platforms, and should be regulated to ensure they comply with this requirement;
- v. Technology companies must demonstrate their accountability to users by making themselves fully answerable to national legislatures and other organs of representative democracy.

SIGNED:

 <i>María Eugenia Rodríguez Cordero</i> Member, National Congress of Argentina	 <i>Peter Krieger</i> Member, Parliament of Belgium	 <i>Roberto Freixo</i> Member, National Congress of Brazil	 <i>Jean-Marie Harlé</i> Member, Parliament of France
 <i>Hildegunde Naughton</i> Chairperson of the Joint Committee on Communications, Climate Action and Environment, Parliament of Ireland	 <i>Ivars Cakšs</i> Deputy Speaker, Parliament of Republic of Latvia	 <i>P. V. Narayana Murthy</i> Member, Parliament of Singapore	 <i>James Callaghan</i> Member, Parliament of the UK

On this Tuesday, the Twenty-Seventh of November MMXVIII in WESTMINSTER, LONDON

Formal minutes

Wednesday 13 February 2019

Damian Collins, in the Chair

Clive Efford	Jo Stevens
Paul Farrelly	Giles Watling
Ian C Lucas	

Draft Report (*Disinformation and 'fake news': Final 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 317 read and agreed to.

Summary agreed to.

Annexes agreed to.

Resolved, That the Report be the Eighth 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 Tuesday 26 February 2019 at 10.00 a.m.]

Witnesses

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

Tuesday 19 December 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, Internet Advertising Bureau, **Phil Smith**, Managing Director, Incorporated Society of British Advertisers (ISBA), and **Ben Williams**, Adblock Plus [Q160–188](#)

Tuesday 23 January 2018

Professor Vian Bakir, Bangor University, **Professor Stephan Lewandowsky**, University of Bristol, and **Dr Caroline Tagg**, the Open University [Q189–237](#)

Matt Breen, Commercial Director, Media Chain (part of the Social Chain Group), **Adam Hildreth**, Chief Executive, Crisp, and **Dr Charles Kriel**, Corsham Institute [Q238–272](#)

Thursday 8 February 2018

Richard Gingras, Vice President of News, Google, and **Juniper Downs**, Global Head of Public Policy, YouTube [Q273–342](#)

Monika Bickert, Head of Global Policy Management, and **Simon Milner**, Policy Director, UK, Middle East and Africa, Facebook [Q343–478](#)

Carlos Monje, Director, Public Policy and Philanthropy, U.S. and Canada, 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 Center, **Frank Sesno**, Director, Professor of Media and Public Affairs and International Affairs, George Washington University, and **Claire Wardle**, Research Fellow, Shorenstein Centre on Media, Politics and Public Policy [Q569–600](#)

David Chavern, President and Chief Executive, New Media Alliance, Major Garrett, Chief White House Correspondent, CBS News, **Tony Maddox**, Executive Vice President and Managing Director, CNN International, and **Kinsey Wilson**, Special Advisor to the President and Chief Executive, 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 Chief Executive, Hermitage Capital Management, and **Edward Lucas**, Senior Vice President, Center for European Policy Analysis

[Q849–894](#)

Elizabeth Denham, Information Commissioner

[Q895–942](#)

Wednesday 14 March 2018

Rt Hon Matt Hancock MP, 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**, social media experts

[Q1271–1461](#)

Tuesday 17 April 2018

Brittany Kaiser, former Director of Program Development, Cambridge Analytica

[Q1462–1769](#)

Tuesday 24 April 2018

Dr Aleksandr Kogan, Cambridge University researcher

[Q1770–2086](#)

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, **Bob Posner**, Director of Political Finance and Regulation and Legal Counsel, and **Louise Edwards**, Head of Regulations, 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, and **Andy Wigmore** [Q3481–3780](#)

Wednesday 31 October 2018

Sharon White, Chief Executive, and **Lord Burns**, Chair, Ofcom [Q3781–3893](#)

Tuesday 6 November 2018

Elizabeth Denham, Information Commissioner, and **James Dipple-Johnstone**, Deputy Commissioner, Information Commissioner's Office [Q3894–4018](#)

Claire Bassett, Chief Executive, **Bob Posner**, Director of Political Finance and Regulation and Legal Counsel, and **Louise Edwards**, Head of Regulations, Electoral Commission [Q4019–4100](#)

Guy Parker, Chief Executive, Advertising Standards Authority [Q4101–4130](#)

Tuesday 27 November 2018

Richard Allan, Vice President of Policy Solutions, Facebook; [Q4131–4273](#)

Tuesday 27 November 2018

Elizabeth Denham, Information Commissioner, and **Steve Wood**, Deputy Information Commissioner, Information Commissioner's Office

[Q4274–4326](#)

Ashkan Soltani, tech expert

[Q4327–4382](#)

Published written evidence

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

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

- 1 89up ([FKN0106](#))
- 2 Adblock Plus ([FKN0046](#))
- 3 Advertising Standards Authority, supplementary ([FKN0110](#))
- 4 Age of Autism ([FKN0010](#))
- 5 Age of Autism, supplementary ([FKN0027](#))
- 6 AggregatIQ ([FKN0086](#))
- 7 Alegre, Ms Susie ([FKN0081](#))
- 8 Alexander Nix, supplementary ([FKN0072](#))
- 9 Amy Mitchell, Pew Research Centre ([FKN0041](#))
- 10 Andrews, Professor Leighton ([FKN0006](#))
- 11 Arundel Bypass Neighbourhood Committee ([FKN0097](#))
- 12 Association for Citizenship Teaching ([FKN0012](#))
- 13 Avaaz ([FKN0073](#))
- 14 Bangor University ([FKN0003](#))
- 15 Banks, Arron, supplementary ([FKN0059](#))
- 16 Banks, Arron ([FKN0056](#))
- 17 Banks, Arron ([FKN0080](#))
- 18 BBC, supplementary ([FKN0118](#))
- 19 Bernal, Dr Paul ([FKN0096](#))
- 20 Bontcheva, Kalina, supplementary ([FKN0054](#))
- 21 Borden Ladner Gervais LLP ([FKN0089](#))
- 22 Briant, Dr Emma, Senior Lecturer at University of Essex ([FKN0099](#))
- 23 Briant, Dr Emma, Senior Lecturer at University of Essex ([FKN0109](#))
- 24 Brody, Dorje ([FKN0103](#))
- 25 Cahill, Mr Kevin, supplementary ([FKN0063](#))
- 26 Cahill, Mr Kevin ([FKN0062](#))
- 27 Cambridge Analytica ([FKN0045](#))
- 28 Communications Chamber ([FKN0100](#))
- 29 Competition & Markets Authority ([FKN0113](#))
- 30 Corsham Institute ([FKN0007](#))
- 31 David Brear ([FKN0065](#))
- 32 David Chavern, President and CEO, News Media Alliance ([FKN0039](#))
- 33 Deer, Brian ([FKN0019](#))

- 34 Dehaye, Paul-Olivier ([FKN0055](#))
- 35 Denham, Elizabeth, Information Commissioner, supplementary ([FKN0057](#))
- 36 Denham, Elizabeth, Information Commissioner([FKN0051](#))
- 37 Disinformation Index ([FKN0058](#))
- 38 Dommett, Dr Katharine ([FKN0104](#))
- 39 Dr Carlo Kopp, Dr Kevin B. Korb and Dr Bruce I. Mills ([FKN0120](#))
- 40 Dr Emma Briant ([FKN0071](#))
- 41 Dr Emma Briant, Senior Lecturer at University of Essex ([FKN0092](#))
- 42 Ebley, Mr Richard ([FKN0015](#))
- 43 Electoral Commission ([FKN0031](#))
- 44 Denham, Elizabeth, Information Commissioner further, supplementary ([FKN0116](#))
- 45 Erin Anzelmo ([FKN0074](#))
- 46 Facebook ([FKN0048](#))
- 47 Facebook - Mike Schroepfer ([FKN0082](#))
- 48 Facebook - Rebecca Stimson ([FKN0095](#))
- 49 Facebook, supplementary ([FKN0078](#))
- 50 Factmata Limited, UK ([FKN0035](#))
- 51 Google, supplementary ([FKN0038](#))
- 52 Hajela, Ruchi ([FKN0066](#))
- 53 Helena Kennedy Centre for International Justice ([FKN0005](#))
- 54 Helena Kennedy Centre for International Justice ([FKN0090](#))
- 55 Hills, Dr Mils ([FKN0014](#))
- 56 HonestReporting ([FKN0047](#))
- 57 Incorporated Society of British Advertisers (ISBA), supplementary ([FKN0036](#))
- 58 Independent Press Standards Organisation ([FKN0004](#))
- 59 Institute of Practitioners in Advertising ([FKN0101](#))
- 60 Internet Advertising Bureau UK, supplementary ([FKN0043](#))
- 61 IPA ([FKN0093](#))
- 62 Kaiser, Brittany ([FKN0076](#))
- 63 Kiely, Mr Mike ([FKN0115](#))
- 64 Kogan, Dr Aleksandr ([FKN0077](#))
- 65 Leopoldo Moreau, Chair, Freedom of Expression Commission, Chamber of Deputies, Argentina ([FKN0117](#))
- 66 London School of Economics and Political Science ([FKN0119](#))
- 67 Lucas, Edward ([FKN0052](#))
- 68 Major Garrett, Chief Whitehouse Correspondent, CBS News ([FKN0042](#))
- 69 McGrath, M C ([FKN0067](#))
- 70 McHugh, Mr Alistair ([FKN0020](#))

- 71 Mercer, Stuart ([FKN0016](#))
- 72 Miller, Mr C ([FKN0009](#))
- 73 MoneySavingExpert.com ([FKN0068](#))
- 74 Morley, Professor Neville ([FKN0091](#))
- 75 Morris, W ([FKN0085](#))
- 76 Muslim Engagement and Development (MEND) ([FKN0011](#))
- 77 National Crime Agency ([FKN0112](#))
- 78 National Literacy Trust ([FKN0037](#))
- 79 The Open University ([FKN0026](#))
- 80 The Open University, supplementary ([FKN0044](#))
- 81 Penna, Mr Dominic ([FKN0021](#))
- 82 Professor Lorna Woods and William Perrin ([FKN0105](#))
- 83 Pupils 2 Parliament ([FKN0025](#))
- 84 Reilly, Dr Paul ([FKN0084](#))
- 85 Rostron, Mark ([FKN0121](#))
- 86 Second Draft ([FKN0050](#))
- 87 Shiner, Bethany ([FKN0107](#))
- 88 Steve Willis and Jeremy Joynson ([FKN0098](#))
- 89 Still, Prof. Dr. G. Keith ([FKN0070](#))
- 90 The Stonehenge Alliance ([FKN0053](#))
- 91 Townsend, Mr Samuel ([FKN0018](#))
- 92 University of Westminster - Communication and Media Research Institute & Westminster Institute for Advanced Studies ([FKN0013](#))
- 93 Dr Sander van der Linden et al ([FKN0049](#))
- 94 Wardle, Dr Claire, Shorenstein Centre on Media, Politics and Public Policy, ([FKN0040](#))
- 95 Watt, Dr Andrew ([FKN0108](#))
- 96 Weatherley, Isabella ([FKN0002](#))
- 97 Wisty, Edmund ([FKN0008](#))
- 98 Wylie, Chris, supplementary ([FKN0079](#))

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)
Fifth Report	Disinformation and 'fake news': Interim Report	HC 363 (HC 1630)
Sixth Report	BBC Annual Report and Accounts 2017–18: Equal pay at the BBC	HC 993
Seventh Report	BBC Annual Report and Accounts 2017–18: Equal Pay at the BBC: BBC Response to the Committee's Sixth Report of Session 2017–19	HC 1875
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
Fifth Special Report	Disinformation and 'fake news': Government Response to the Committee's Fifth Report of Session 2017–19	HC 1630

