

[Brasão]

Câmara dos Comuns do Reino Unido
Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte

Desinformação e 'notícias falsas': Relatório Final

Oitavo Relatório do Período 2017-19

Relatório, juntamente com as atas formais relacionadas ao relatório

Encomendado pela Câmara dos Comuns do Reino Unido para impressão em 14 de fevereiro de 2019

HC 1791

Publicado em 18 de fevereiro de 2019 por determinação da Câmara dos Comuns

Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte

O Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte foi constituído pela Casa dos Comuns para examinar o gasto, a administração e a política do Departamento Digital, da Cultura, dos Meios de Comunicação e Esporte e dos seus órgãos públicos associados.

Composição Atual

[Damian Collins MP](#) (Conservador, Folkestone e Hythe) (Presidente)
[Clive Efford MP](#) (Trabalhista, Eltham)
[Julie Elliott MP](#) (Trabalhista, Sunderland Central)
[Paul Farrelly MP](#) (Trabalhista, Newcastle-under-Lyme)
[Simon Hart MP](#) (Conservador, Carmarthen West e South Pembrokeshire)
[Julian Knight MP](#) (Conservador, Solihull)
[Ian C. Lucas MP](#) (Trabalhista, Wrexham)
[Brendan O'Hara MP](#) (Partido Nacional Escocês, Argyll and Bute)
[Rebecca Pow MP](#) (Conservador, Taunton Deane)
[Jo Stevens MP](#) (Trabalhista, Cardiff Central)
[Giles Watling MP](#) (Conservador, Clacton)

Atribuições

Este é um dos comitês especializados para supervisão dos departamentos do governo, sendo que suas atribuições são derivadas das Determinações Vigentes da Casa dos Comuns, especialmente a SO N. 152. Disponíveis pela internet em www.parliament.uk.

Publicação

© Propriedade Intelectual da Câmara dos Comuns 2019. Esta publicação pode ser reproduzida sob os termos da Licença denominada Parlamento Aberto, publicada em www.parliament.uk/copyright/. Os relatórios do comitê são publicados no site do comitê em www.parliament.uk/dcmscom e impressos por determinação da Casa.

As evidências relacionadas a este relatório estão publicadas na página de publicações de inquérito no site do Comitê.

Equipe de Trabalho do Comitê

A atual equipe de trabalho do Comitê é composta por Chloe Challender (Secretária), Mems Ayinla (Segunda Secretária), Mubeen Bhutta (Segundo Secretário), Josephine Willows (Especialista Sênior), Lois Jeary (Especialista), Andy Boyd (Assistente Sênior), Keely Bishop (Assistente), Sarah Potter (Pesquisadora Adjunta), Lucy Dargahi (Assessor de Imprensa) e Anne Peacock (Assessora Sênior de Imprensa e Comunicação).

Contatos

Qualquer contato deve ser endereçado ao secretário do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Casa dos Comuns do Reino Unido, Londres SW1A 0AA. O número de telefone para consultas gerais é 020 7219 6188; o endereço de e-mail do Comitê é cmscom@parliament.uk

Você pode acompanhar o Comitê pelo Twitter usando [@CommonsCMS](https://twitter.com/CommonsCMS)

Conteúdo

Resumo	5
1 Introdução e Contexto	7
Regulamentação e papel, definição e responsabilidade legal das empresas de	
2 tecnologia	10
Definições	10
Danos e regulação on-line	10
O Novo Centro de Ética para Dados e Algoritmos	11
Legislação na Alemanha e França	12
O Reino Unido	13
Uso de dados pessoais e dados inferidos	17
Papel aprimorado do ICO e responsabilização de empresas de tecnologia	18
3 Uso e segmentação de dados	20
Introdução	20
A multa aplicada pelo ICO sobre o Facebook	20
O ICO, SCL Group e Cambridge Analytica	21
Facebook e o Decreto de Consentimento da Comissão Federal do Comércio de 2011	23
Facebook e o caso Six4Three	26
Listas Brancas	27
Valor dos dados dos amigos	29
O vínculo entre acesso a dados e gastos com publicidade no Facebook	30
Compartilhamento de dados do Facebook com desenvolvedores	33
A coleta de dados pelo Facebook de clientes Android	35
Monitoramento pelo Facebook do uso de aplicativos	36
Investida do Facebook contra aplicativos concorrentes	38
Resposta do Facebook à publicação dos documentos Six4Three	38
Modelo de negócios do Facebook e novos desafios para reguladores	40
Leave.EU e dados da Eldon Insurance supostamente usados por campanhas	43
4 Aggregate IQ	45
Introdução	45
Relação entre AIQ e SCL/Cambridge Analytica antes do referendo no Reino Unido sobre a UE	48

Trabalho da AIQ relacionado ao referendo sobre a UE	50
Facebook, o Vote Leave e o concurso de previsão £50 Million	52
Recursos da AIQ	53
Inteligência artificial	53
Pixels do Facebook	53
Captura de Perfis do LinkedIn	55
Conclusão	55
5 Propaganda e Campanha Política	57
Introdução	57
Anúncios online	57
Propaganda política online	58
Facebook e as Redes Tradicionais	62
Conselho Constitucional de Pesquisa (CRC)	64
Relatório Cairncross: um futuro sustentável para o jornalismo	67
6 Influência estrangeira em campanhas políticas	68
Introdução	68
Interferência russa nas eleições do Reino Unido	69
Facebook e a Campanha de Desinformação da Rússia	72
Endereços IP russos no Facebook	72
Dados do Facebook de propriedade do Centro de Psicometria da Cambridge University que foram compartilhados com APIs Russos	73
Interferência russa por de outras redes sociais	73
Leave.EU, Arron Banks, os EUA e a Rússia	74
Outras investigações em andamento e denúncias criminais	76
7 Influência da SCL em eleições estrangeiras	78
Introdução	78
Mais informações sobre o trabalho da SCL	78
Oportunidades de cidadania por investimento	79
Conflitos de interesse	82
8 Educação digital	85
Introdução	85
Atrito no sistema	86
Reguladores e educação digital	87
Conclusões e recomendações	89
Anexo 1 - Participantes do 'Comitê Internacional', terça-feira, 27 de novembro de 2018	98
Anexo 2 - Princípios Internacionais sobre Regulação de Plataformas de Tecnologia	99
Atas formais	100
Testemunhas	101
Documentos comprobatórios publicados	105
Lista de Relatórios do Comitê durante a Legislatura Atual do Parlamento	108

Resumo

Este Relatório Final resulta de uma investigação sobre desinformação com duração de mais de 18 meses, cobrindo os direitos de privacidade das pessoas, como suas escolhas políticas podem ser afetadas e influenciadas pela informação online e sobre a interferência em eleições políticas tanto neste país como no mundo como um todo, promovida por forças malignas com o objetivo de causar conflitos e confusão.

Atuamos no exercício das atribuições conferidas pelo Parlamento aos Comitês, incluindo a prerrogativa de intimar pessoas para entregar evidências e obter documentos selados do sistema jurídico de outro país. Convidamos representantes eleitos democraticamente de oito países para participar do nosso Comitê no Reino Unido e criar um 'Comitê Internacional', o primeiro desse tipo, para promover mais cooperação entre os países para combater a disseminação da desinformação e limitar a sua capacidade perniciosa de distorcer, produzir conflitos e desestabilizar. Ao longo deste inquérito, contamos com o apoio de outros parlamentos. Esse trabalho continua, com novas sessões programadas para 2019. É uma evidência da disposição da comunidade mundial para combater ações similares, que também foram identificadas em outras jurisdições.

Este é o Relatório Final da nossa investigação, mas não se tem a pretensão de ser a palavra final. Sempre assistimos à veiculação de propagandas e à promoção de ações preconceituosas com objetivos políticos, transmitidas como se fossem notícia. Mas esta atividade adquiriu novas formas e alcançou uma imensa proporção devido às novas ferramentas de tecnologia da informação e a onipresença das redes sociais. Nesse contexto, as pessoas são capazes de aceitar e acreditar em informações que reforçam suas opiniões, independentemente do quão distorcidas ou imprecisas, enquanto rejeitam o conteúdo com o qual não concordam, classificando-o como 'notícias falsas'. O resultado é um aumento da polarização e redução do campo comum sobre o qual é possível construir um debate razoável, com base em fatos objetivos. Muito já foi dito sobre o espessamento do debate público, mas quando esses fatores são levados diretamente a efeito nas campanhas eleitorais, o próprio tecido de nossa democracia se torna ameaçado.

É pouco provável que ocorra uma mudança desse cenário. A mudança de que precisamos é maior transparência no mundo digital, para garantir que sabemos a fonte do que estamos lendo, quem pagou pelo conteúdo e por que as informações foram enviadas para nós. Precisamos entender como as grandes empresas de tecnologia funcionam e o que acontece com os nossos dados. O Facebook opera monitorando usuários e não usuários, rastreando suas atividades e retendo dados pessoais. O Facebook ganha dinheiro vendendo acesso aos dados dos usuários por meio de suas ferramentas de publicidade. Aumenta ainda mais seu valor ao celebrar contratos abrangentes, que prevê o compartilhamento recíproco de dados, com os principais desenvolvedores de aplicativos que operam dentro da plataforma do Facebook.

Enquanto isso, entre as inúmeras mensagens inócuas de comemoração e momentos felizes, forças perniciosas fazem uso do Facebook para ameaçar e assediar outras, publicar pornografia como vingança, disseminar discursos de ódio e propaganda de todos os tipos e para influenciar eleições e processos democráticos — para muitas dessas ações, o Facebook e as outras empresas de mídia social não podem ou não querem impedir. Precisamos lançar mão de princípios democráticos amplamente aceitos e garantir sua aplicação na era digital.

As grandes empresas de tecnologia não podem se expandir exponencialmente, sem controle ou supervisão regulatória adequada. Somente os governos e a lei possuem poderes suficientes para controlá-las. Os instrumentos legais já existem. Eles agora devem ser aplicados à atividade digital, usando ferramentas como leis de privacidade, lei de proteção de dados, leis antitruste e de defesa da concorrência. Se as empresas se converterem em monopólios, podem ser desmembradas, em qualquer setor. O manuseio de dados pessoais do Facebook e seu uso em campanhas políticas são áreas importantíssimas e legítimas para atuação dos órgãos reguladores, e não deveriam ser capazes de se eximir de toda a responsabilidade editorial pelo conteúdo compartilhado por seus usuários em suas plataformas.

Numa democracia, precisamos experimentar uma pluralidade de vozes e, de forma crítica, ter as habilidades, a experiência e o conhecimento para avaliar a veracidade dessas vozes. Embora a Internet tenha trazido muitas liberdades por todo o mundo e uma capacidade sem precedentes de comunicação, ela também tem a capacidade de distorcer, enganar e produzir ódio e instabilidade. Funciona numa escala e velocidade sem precedentes na história humana. Uma das testemunhas em nossa investigação, Tristan Harris, do Centro de Tecnologia Humana, descreve que o uso atual da tecnologia se equipara ao "sequestro das nossas mentes e da nossa sociedade". Em vez disso, devemos usar a tecnologia para libertar nossas mentes e usar a regulação para restaurar a responsabilidade democrática. Devemos garantir que as pessoas permaneçam no comando das máquinas.

1. Introdução e Contexto

1. O Relatório Preliminar do Comitê DCMS, “Desinformação e 'Notícias Falsas’”, foi publicado em julho de 2018.¹ Desde o verão de 2018, o Comitê realizou três novas audiências, convidando os reguladores e o Governo do Reino Unido para depor, e recebemos outras 23 manifestações por escrito.² Também realizamos um 'Comitê Internacional' em novembro de 2018, para o qual convidamos parlamentares de nove países: Argentina, Bélgica, Brasil, Canadá, França, Irlanda, Letônia, Cingapura e Reino Unido.

2. As definições neste campo são importantes. Até mudamos o título do nosso estudo, que inicialmente era “notícias falsas”. Optamos por chamá-lo de “Desinformação e 'Notícias Falsas’”, pois o termo 'Notícias Falsas' desenvolveu um significado próprio, carregado de outros elementos. Como dissemos em nosso Relatório Preliminar, o termo 'notícias falsas' tem sido utilizado para descrever o conteúdo de que um leitor pode não gostar ou discordar. O presidente dos EUA, Donald Trump, chamou certos veículos de comunicação de 'Fake News Media' e de 'verdadeiro inimigo do povo'.³

3. Portanto, estamos satisfeitos que o Governo tenha aceitado as recomendações do nosso Relatório Preliminar e, em vez de usar o termo 'notícias falsas', passamos a utilizar o termo 'desinformação' para descrever “a criação deliberada e o compartilhamento de informações falsas e/ou manipuladas, que são destinados a enganar e ludibriar o público, seja para causar danos ou para alcançar objetivos políticos, pessoais ou financeiros”.⁴

4. Este relatório final parte dos sete principais temas abordados no relatório preliminar, quais sejam: definição, papel e responsabilidades legais das redes sociais; uso indevido e direcionamento de dados, com base nas alegações do Facebook, Cambridge Analytica e Aggregate IQ (AIQ), incluindo documentos que obtivemos da Six4Three sobre a ciência e participação do Facebook no compartilhamento de dados; campanha política; influência russa em campanhas políticas; Influência da SCL em eleições estrangeiras; e educação digital. Também incorporamos análises da firma de consultoria 89up, presentes no arquivo de dados que recebemos de Chris Vickery, em relação à base de dados da AIQ.

1 A versão em HTML do relatório 'Desinformação e notícias falsas: Relatório Preliminar' foi a página mais visitada no portal do parlamento neste ano, com 13.646 novas visualizações da página de 'Conteúdo' (a média é de cerca de 650 visualizações). O PDF teve 4.310 novas visitas no site do parlamento, enquanto a média de todo o comitê é de cerca de 280 visualizações. O Relatório Preliminar foi a página HTML mais vista e o segundo PDF mais visto de qualquer relatório preparado por algum comitê da Câmara dos Comuns do Reino Unido nos últimos cinco anos (números fornecidos pela Unidade de Publicações e Internet da Casa dos Comuns).

2 [Manifestações Escritas - Desinformação e 'Notícias Falsas'](#)

3 [Tuite de Donald J. Trump](#), em 29 de outubro de 2018.

4 [Desinformação e 'Notícias Falsas': Resposta do Governo ao Quinto Relatório do Comitê da Legislatura de 2017-19](#), 23 de outubro de 2018, HC 1630 Resposta do Governo ao Relatório Interino, página 2.

5. Neste Relatório Final, partimos das recomendações baseadas em princípios feitas no relatório preliminar. Aguardamos uma resposta do Governo a estas recomendações dentro de dois meses. Esperamos que a resposta seja muito mais abrangente, prática e construtiva do que a apresentada por ocasião do Relatório Preliminar, publicado em outubro de 2018.⁵ Várias de nossas recomendações não foram efetivamente respondidas. Diante disso, essas questões alcançam a condição de matéria urgente, que o governo precisa responder. Ficamos satisfeitos que o Secretário de Estado, Rt Hon Jeremy Wright MP, tenha descrito nossas conversas como parte de "um processo iterativo", e que este Relatório será "bastante útil, francamente, para embasar nossas próximas conclusões antes de escrevermos o nosso White Paper" e que nossos pontos de vista farão parte das considerações do governo.⁶ Aguardamos ansiosos pelo White Paper do Governo sobre Danos Digitais, publicado pelo Departamento Digital, da Cultura, dos Meios de Comunicação e Esporte e pelo Ministério do Interior, que deve ser publicado no início de 2019 e abordará as questões de danos on-line, incluindo desinformação.⁷ Repetimos muitas das recomendações presentes no nosso Relatório Preliminar, que o governo não respondeu. Presumimos e esperamos que o governo responda tanto as recomendações deste Relatório Final como as que não foram respondidas do Relatório Preliminar.

6. Este Relatório Final é o resultado de muitos meses de colaboração com outros países, organizações, parlamentares e indivíduos de todo o mundo. Ao todo, o Comitê realizou 23 audiências, recebeu mais de 170 manifestações por escrito, ouviu 73 testemunhas, realizou mais de 4.350 perguntas nessas audiências e realizou muitas trocas de correspondências públicas e privadas com indivíduos e organizações.

7. A investigação se caracteriza pela colaboração, na tentativa de entender as complexas questões técnicas, políticas e filosóficas envolvidas, além de buscar soluções práticas para essas questões. Como fizemos em nosso Relatório Preliminar, agradecemos a todos os indivíduos e empresas, nacionais e estrangeiros —incluindo nossos colegas e associados nos Estados Unidos— pela generosidade ao compartilhar conosco suas opiniões e informações.⁸

8. Também gostaríamos de agradecer pelo trabalho de outros parlamentares que têm se debruçado sobre questões semelhantes, enquanto conduzimos a nossa investigação. O Comitê Permanente de Acesso à Informação, Privacidade e Ética do Canadá publicou seu relatório "Democracia sob ameaça: riscos e soluções na era da desinformação e monopólio de dados" em dezembro de 2018.⁹ Esse relatório destaca o estudo do comitê canadense sobre a violação de dados pessoais envolvendo a Cambridge Analytica e o Facebook, além de questões mais amplas sobre o uso de dados pessoais pelas empresas de mídia social e por que essas empresas são responsáveis pela disseminação de informação enganosa e desinformação. As recomendações desse comitê coincidem com muitas das nossas incluídas neste relatório.

5 Mesma referência acima.

6 [Q263](#), Audiência, 24 de outubro de 2018, Trabalho do Departamento Digital, da Cultura, dos Meios de Comunicação e Esporte.

7 [Desinformação e 'notícias falsas': Resposta do Governo ao Quinto Relatório da Legislatura 2017-19](#), 23

de outubro de 2018, HC 1630 resposta do governo ao Relatório Preliminar, página 1.

8 Nosso consultor especialista para o inquérito foi o Dr. Charles Kriel. Para efeito de transparência, os Interesses Pessoais do Dr. Charles Kriel são os seguintes: Associate Fellow do Centro de Comunicação Estratégica (KCSC) do King's College London; Fundador da Kriel.Agency; Co-fundador e acionista da Lightful; Assessor do comitê parlamentar de segurança nacional de Trinidad e Tobago.

O Comitê também contratou as seguintes pessoas para realizar pesquisas específicas para este inquérito:

Mike Harris, CEO da 89up; Martin Barnard, CTO da 89up; Josh Feldberg, Diretor Digital na 89up; e Peter Pomerantsev, professor visitante na London School of Economics (LSE). Também agradecemos a Ashkan Soltani, pesquisador e consultor independente e ex-Chefe de Tecnologia da Comissão Federal de Comércio, que nos auxiliou na redação dos parágrafos relacionados à FTC, no capítulo 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.

9. O Comitê Eletivo de Inteligência do Senado dos EUA tem uma investigação em andamento sobre a extensão da interferência russa nas eleições de 2016 nos EUA. Como resultado dos conjuntos de dados fornecidos pelo Facebook, Twitter e Google ao Comitê de Inteligência —sob seu Grupo de Assessoria Técnica— dois relatórios independentes foram publicados em dezembro de 2018. New Knowledge, uma empresa de integridade da informação, publicou “The Tactics and Tropes of the Internet Research Agency”, que destaca as táticas e mensagens da Agência de Pesquisa da Internet para manipular e influenciar os americanos, e inclui um conjunto de slides, destacando estatísticas, infográficos e apresentação temática de memes.¹⁰ O Projeto de Pesquisa em Propaganda Computacional e Graphika publicou o segundo relatório, que analisa atividades de contas conhecidas da Agência de Pesquisa da Internet, usando o Facebook, Instagram, Twitter e YouTube entre 2013 e 2018, tendo como alvo os usuários dos EUA.¹¹ Esses dois relatórios serão incorporados ao relatório do Comitê de Inteligência de 2019.

10. A reunião do nosso 'Comitê Internacional', realizada em novembro de 2018, foi o ponto principal deste trabalho colaborativo. O Comitê foi composto por 24 representantes eleitos democraticamente de nove países, incluindo os 11 membros do Comitê do DCMS, que juntos representam um total de 447 milhões de pessoas. Os representantes assinaram um conjunto de princípios internacionais nessa reunião.¹² Trocamos ideias e soluções, tanto de forma pública, como de forma privada, e realizamos uma audiência com duração de sete horas. Convidamos Mark Zuckerberg, CEO do Facebook — empresa de mídia social que tem mais de 2,25 bilhões de usuários e faturou US\$ 40 bilhões em 2017 — para produção de provas para nós e para esse Comitê; ele recusou o convite, três vezes.¹³ No entanto, quatro horas depois da publicação dos documentos que obtivemos do Six4three —sobre o conhecimento e a participação do Facebook no compartilhamento de dados—, Zuckerberg respondeu com um post em sua página no Facebook.¹⁴ Agradecemos aos colegas do "Comitê Internacional" por participarem dessa importante sessão, e esperamos continuar com a nossa colaboração neste ano. Regulamentação e papel, definição e responsabilidade legal das empresas de tecnologia

2. Regulamentação e papel, definição e responsabilidade legal das empresas de tecnologia

Definições

11. Em nosso Relatório Preliminar, desconsideramos o termo 'notícias falsas', já que ele “assumiu vários significados, incluindo a descrição de qualquer declaração que não seja do agrado ou aceita pelo leitor”. Em vez disso, recomendamos o uso dos termos 'informação enganosa' e 'desinformação'. Esses termos transmitem "diretrizes claras para as empresas, organizações e o governo seguirem" atreladas a "uma consistência compartilhada de significado entre as plataformas, que pode ser usada como base

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 Vide Anexo 2. Os Princípios serão a base do trabalho do Comitê Internacional e foram repassados à Câmara dos Comuns na forma de memorando. O original será colocado no arquivo parlamentar da Câmara dos Comuns.

¹³ Dominic Cummings também se recusou a testemunhar no Comitê DCMS. Terceiro Relatório Especial do Comitê na Legislatura 2017-18, [Failure of a witness to answer an Order of the Committee: conduct of Mr Dominic Cummings](#), em 5 de junho de 2018. O Relatório denunciou a recusa do Dominic Cummings em depor ao Comitê. O Comitê solicitou que a Câmara determinasse que Dominic Cummings agendasse uma data para seu comparecimento no Comitê. A Câmara proferiu a determinação, mesmo assim Dominic Cummings não cumpriu. A questão foi encaminhada ao Comitê de Prerrogativas em 28 de junho de 2018.

¹⁴ Detalhes sobre a postagem de Mark Zuckerberg no Capítulo 3.

para a regulação e responsabilização".¹⁵

12. Ficamos satisfeitos com o fato de o governo ter acatado nosso parecer sobre a inconveniência do termo 'notícias falsas', e que tenha buscado fazer uso dos termos 'informação enganosa' e 'desinformação'. A resposta do Governo afirma:

Em nosso trabalho, definimos desinformação como a criação e o compartilhamento deliberados de informações falsas e/ou manipuladas que têm por objetivo enganar e ludibriar o público, seja para causar danos ou para alcançar objetivos políticos, pessoais ou financeiros. 'Informação enganosa' se refere ao compartilhamento inadvertido de informações falsas¹⁶

13. Também recomendamos a criação de uma nova categoria de empresa de mídia social, que restrinja as responsabilidades das empresas de tecnologia e que não seja necessariamente uma 'plataforma', nem uma 'editora'. O governo não apresentou qualquer resposta a esta recomendação, mas Sharon White, Diretora Executiva da Ofcom, chamou essa nova categoria de "muito precisa" pois "as plataformas têm responsabilidade, mesmo que não sejam geradoras de conteúdo, pelo que hospedam em suas plataformas e pelo que anunciam"¹⁷

14. As empresas de mídia social não podem se esconder por trás da alegação de serem apenas uma 'plataforma' e sustentar que não têm responsabilidade de regular o conteúdo dos seus sites. Repetimos a recomendação do nosso Relatório Preliminar de que uma nova categoria de empresa de tecnologia seja criada, que restrinja as responsabilidades das empresas de tecnologia e que não seja necessariamente uma 'plataforma', nem uma 'editora'. Essa abordagem levaria as empresas de tecnologia a assumirem responsabilidade legal pelo conteúdo identificado como prejudicial depois de publicado pelos usuários. Pedimos ao governo que considere esta nova categoria de empresa de tecnologia em seu próximo White Paper.

Danos e regulação on-line

15. No início da nossa investigação, ouvimos o depoimento de Sandy Parakilas e Tristan Harris, que estavam na época envolvidas no Centro de Tecnologia Humana, com sede nos EUA. O Centro compilou um 'Livro de Danos', que resume os "impactos negativos da tecnologia que não aparecem nos balanços das empresas, mas no balanço

da sociedade.¹⁸ O Livro de Danos inclui impactos negativos da tecnologia, incluindo perda de atenção, problemas de saúde mental, confusões relacionadas a relacionamentos pessoais, risco para as nossas democracias e problemas que afetam as crianças.¹⁹

16. A proliferação on-line desses danos se torna mais perigosa, ao direcionarem mensagens específicas para indivíduos, como 'mensagens micro-direcionadas' — geralmente alterando e distorcendo as opiniões negativas das pessoas sobre si mesmas e sobre os demais. Essa distorção se torna ainda mais

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](#)

¹⁸ Ledger of Harms, Center for Humane Technology, accessed 29 November 2018.

¹⁹ Exploraremos ainda mais as questões de dependência e saúde digital em nossa investigação sobre tecnologias imersivas e viciantes em 2019.

extrema pelo uso de 'deepfakes', áudio e vídeos que parecem e soam como uma pessoa real, dizendo algo que essa pessoa nunca disse.²⁰ Como dissemos em nosso Relatório Preliminar, esses exemplos se tornarão mais complexos e difíceis de detectar, quanto mais sofisticado o software se tornar.²¹

17. A Secretária de Saúde, Rt Hon Matthew Hancock MP, alertou recentemente as empresas de tecnologia, incluindo Facebook, Google e Twitter, para que removam conteúdo inapropriado e prejudicial, após os eventos envolvendo a morte de Molly Russell, que, aos 14 anos, tirou a própria vida em novembro de 2017. Sua conta no Instagram continha material relacionado a depressão, automutilação e suicídio. O Facebook, dono do Instagram, disse que lamentava profundamente o caso.²² O chefe do Instagram, Adam Mosseri, teve uma reunião com a Secretaria de Saúde no início de fevereiro de 2019 e disse que o Instagram “não estava onde deveríamos estar em questões de autoagressão e suicídio” e que estava tentando equilibrar “a necessidade de agir agora e a necessidade de agir com responsabilidade”.²³

18. Observamos também, em seu discurso de 5 de fevereiro de 2019, Margot James MP, Ministra do Departamento Digital, da Cultura, dos Meios de Comunicação e Esporte, expressou suas preocupações:

Disse que, por muito tempo, a resposta de muitas das grandes plataformas foi insatisfatória. Ocorreu a celebração de pelo menos quinze códigos de conduta com plataformas desde 2008. O fato de estarmos onde estamos agora é uma demonstração absoluta de que esse sistema se baseou muito pouco no estado de direito. O White Paper, que o DCMS está produzindo com o Ministério do Interior, será seguido por uma consulta durante o verão e estabelecerá novas medidas legislativas para garantir que as plataformas removam conteúdo ilegal e priorizem a proteção dos usuários, especialmente crianças, jovens e adultos vulneráveis.²⁴

O Novo Centro de Ética para Dados e Algoritmos

19. Como dissemos em nosso Relatório Preliminar, as empresas de mídia social e os mecanismos de pesquisa usam algoritmos, ou sequências de instruções, para personalizar notícias e outros conteúdos para os usuários. Os algoritmos selecionam o conteúdo com base em fatores como a atividade online passada do usuário, conexões sociais e sua localização. Os modelos de negócios das empresas de tecnologia tomam por base a receita proveniente da venda de anúncios e, como o resultado final é o lucro, qualquer forma de conteúdo que aumente o lucro sempre terá prioridade. Portanto, histórias negativas sempre serão priorizadas por algoritmos, pois são compartilhadas com mais frequência do que histórias positivas.²⁵

20. Assim como as informações sobre as próprias empresas de tecnologia precisam ser mais transparentes, o mesmo ocorre com as informações sobre seus algoritmos. Eles podem ter vieses

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.

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

intrínsecos, resultado da maneira como são desenvolvidos pelos engenheiros; esses preconceitos são então replicados, espalhados e reforçados. Monika Bickert, do Facebook, admitiu que o Facebook estava preocupado com “qualquer tipo de viés, seja de gênero, racial ou outras formas de viés que possa afetar a maneira como o trabalho é feito em nossa empresa. Isso inclui a revisão dos algoritmos”. O Facebook deve assumir um papel mais ativo e urgente ao lidar com esses vieses intrínsecos ao desenvolvimento de algoritmos por engenheiros, para impedir que esses problemas sejam replicados e reforçados.²⁶

21. Após ser incluído no orçamento de 2017, o novo Centro de Ética e Inovação de Dados foi criado pelo Governo para buscar uma forma de “habilitar e garantir usos éticos, seguros e inovadores de dados, inclusive para IA”. O Secretário de Estado descreveu o seu papel:

O Centro é um componente essencial da Carta Digital do governo, que busca definir normas e regras para o mundo on-line. O Centro permitirá que o Reino Unido lidere o debate global sobre como os dados e a IA podem e devem ser usados.²⁷

22. O Centro atuará como um órgão consultivo do Governo e suas principais funções incluirão: analisar e antecipar lacunas na governança e regulamentação; avaliar e negociar a definição de boas práticas, códigos de conduta e padrões no uso da inteligência artificial; e assessorar o Governo nas ações políticas e regulatórias necessárias em relação ao uso ético e inovador dos dados.²⁸

23. A resposta do governo ao nosso Relatório Preliminar destacou as respostas à consulta, incluindo a prioridade do Centro para ação imediata, incluindo “monopólios de dados, uso de algoritmos preditivos na fiscalização, uso de análise de dados nas campanhas políticas e possibilidade de viés nas decisões de recrutamento automatizadas”. Parabenizamos a criação do Centro e esperamos contar com a participação dele nas próximas consultas.

Legislação na Alemanha e França

24. Outros países criaram legislação contra conteúdo nocivo em plataformas tecnológicas. Como dissemos em nosso Relatório Preliminar, inicialmente as empresas de tecnologia na Alemanha foram solicitadas a remover o discurso de ódio dentro de 24 horas. Quando essa autorregulação não funcionou, o governo alemão aprovou a Lei de Fiscalização Digital, conhecida como NetzDG, que se tornou lei em janeiro de 2018. Essa legislação obriga as empresas de tecnologia a remover o discurso de ódio de seus sites dentro de 24 horas, com previsão de multa de 20 milhões de euros em caso de descumprimento.²⁹ Como resultado dessa lei, um em cada seis moderadores do Facebook agora trabalha na Alemanha, o que é uma evidência prática de que a legislação pode funcionar.³⁰

25. Uma nova lei na França, aprovada em novembro de 2018, permite que os juízes ordenem a remoção imediata de artigos on-line que eles classifiquem como desinformação, durante as campanhas eleitorais. A lei estabelece que os usuários devem receber “informações justas, claras e transparentes” sobre como seus dados pessoais estão sendo usados, que os sites precisam divulgar os valores que receberam para promover informações, e a lei permite que a Agência Nacional de Transmissão da França tenha o poder de suspender canais de televisão controlados ou sob a influência de um estado

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 Mesma referência acima.

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

³⁰ Professor Lewandovsky, [Q233](#)

estrangeiro se “disseminarem deliberadamente informações falsas que possam afetar a sinceridade da votação”. As sanções por descumprimento à lei são um ano de prisão e multa de € 75.000.³¹

O Reino Unido

26. Como nos disse a Comissária de Informação do Reino Unido, Elizabeth Denham, em novembro de 2018, existe uma tensão entre o modelo de negócios das empresas de mídia social, que é focado em publicidade e direitos humanos, e a proteção da privacidade: “É aí que estamos agora, e é um trabalho muito grande para os reguladores e os formuladores de políticas garantir que os requisitos, e instrumentos de fiscalização e sanções adequados estejam em vigor”.³² Ela nos disse que o Facebook, por exemplo, deveria fazer mais e deveria estar “sujeito a uma regulação e supervisão mais rígidas”.³³ As atividades do Facebook na esfera política, de fato, vêm se expandindo; recentemente, lançou um recurso de petição de Feed de Notícias de “Ações Comunitárias”, por exemplo, para permitir que os usuários se organizem em torno de questões políticas locais, iniciando e apoiando demandas de natureza política. É difícil entender como o Facebook poderá autorregular esse recurso; quanto mais controversa e contenciosa for a questão local, maior será o envolvimento no Facebook, com as receitas associadas a anúncios.³⁴

Facebook e regulação

27. Apesar de pedir desculpas por todos os erros que o Facebook cometeu no passado, parece que ainda não está muito disposto a ser fiscalizado adequadamente. Várias vezes durante a audiência no “Comitê Internacional”, Richard Allan, Vice-Presidente de Políticas de Soluções do Facebook, foi questionado sobre a posição do Facebook sobre regulação. Ele reiteradamente afirmou que o Facebook estava muito aberto ao debate sobre regulação, e que trabalhar em conjunto com os governos seria o melhor caminho a seguir:

Estou pessoalmente satisfeito, e a empresa está muito comprometida, até o nosso CEO —ele falou sobre isso em público— com a ideia de obter o tipo certo de regulação para que possamos sair desse modo de confrontação. Não é benéfico para nós, nem para os nossos usuários. Tentaremos chegar ao lugar certo, em que você concorda que estamos fazendo um bom trabalho e que você tem poderes para nos responsabilizar se não o fizermos, e entendemos qual é o trabalho que precisamos fazer, que é a regulação.³⁵

28. Ashkan Soltani, pesquisador e consultor independente, e ex-Chefe de Tecnologia da Comissão Federal do Comércio (FTC) dos EUA, questionou a disposição do Facebook de se submeter a regulação. Ao discutir a cultura interna do Facebook, disse: “Existe um desprezo — a capacidade de sentir que a empresa conhece mais do que todos vocês e todos os formuladores de políticas”.³⁶ Ele discutiu a Lei de Privacidade do Consumidor da Califórnia, que o Facebook apoiava em público, mas fazia lobby nos bastidores para não ser aprovada.³⁷

29. O Facebook parece disposto a não se sujeitar a regulação, nem ser fiscalizado. Considera-se prática

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.

³⁵ [Q4231](#)

³⁶ [Q4337](#)

³⁷ [Q4330](#)

comum que os cidadãos estrangeiros deponham em comitês. De fato, em julho de 2011, o então Comitê de Cultura, dos Meios de Comunicação e Esporte colheu o depoimento de Rupert Murdoch, durante a investigação sobre hackeamento de por telefone,³⁸ e o Comitê do Tesouro colheu o depoimento de três cidadãos estrangeiros.³⁹ **Ao optar por não comparecer ao Comitê e não responder pessoalmente a qualquer um de nossos convites, Mark Zuckerberg demonstrou desprezo pelo Parlamento do Reino Unido e pelo "Comitê Internacional", envolvendo membros de nove casas legislativas de todo o mundo.**

30. A estrutura de gerenciamento do Facebook é opaca para as pessoas de fora da empresa e isso parece ter sido projetado para ocultar essa informação e para dificultar a responsabilização por decisões específicas. O Facebook usou a estratégia de enviar testemunhas, que eles disseram ser os representantes mais apropriados, mas não estavam adequadamente inteiradas de questões cruciais e não podiam ou escolheram não responder muitas das nossas perguntas. Eles então prometeram cooperar via correspondência, que —para surpresa de ninguém— deixaram de abordar todas as nossas perguntas. Não resta dúvida de que essa estratégia foi deliberada.

Atuais reguladores do Reino Unido

31. No Reino Unido, os principais reguladores relacionados à matéria — Ofcom, Autoridade de Padrão de Publicidade, da Secretaria de Informação, Comissão Eleitoral e a Autoridade de Competitividade e de Mercado — possuem responsabilidades específicas em relação ao uso de conteúdo, aos dados e à conduta a ser adotada. Quando Sharon White, diretora executiva da Ofcom depôs ao Comitê em outubro de 2018, após a publicação do nosso Relatório Preliminar, perguntamos a ela se sua experiência como reguladora de transmissão poderia auxiliar no processo de regulação do conteúdo on-line. Ela disse:

Tentamos examinar com muito cuidado onde achamos que estão as sinergias. [...]

Pareceu-nos que existem duas ou três áreas que podem se aplicar ao conteúdo online.

[...] O fato de o Parlamento ter estabelecido padrões, com objetivos muito ambiciosos, nos pareceu muito importante, num projeto de longo prazo com objetivos-chave, seja em torno da proteção das crianças ou preocupações com danos e ofensas. Você pode constatar isso ao ver o processo democrático sobre os danos que acreditamos como sociedade pode estar sendo amplamente praticado on-line. A outra coisa muito importante no código de transmissão é que deixa claro o fato de que essas coisas se adaptam ao longo do tempo à medida que as preocupações com os danos se adaptam e as preocupações entre os consumidores se adaptam. Em seguida, delega o trabalho a um regulador independente para alcançar na prática esses objetivos chamados de padrão. Existe transparência, o fato de publicarmos nossas decisões quando ocorre descumprimento da nossa parte, e tudo isso é muito aberto ao público. Ocorre um exame minucioso das nossas decisões e há independência em torno do julgamento.⁴⁰

32. Também acrescentou que o trabalho de um regulador de conteúdo on-line poderia ser avaliar a

³⁸ [Uncorrected transcript of oral evidence](#), CMS Committee inquiry into phone hacking, 19 July 2011. Em referência a testemunhas internacionais que prestam depoimentos perante comitês, Erskine May declara: "Cidadãos nacionais ou estrangeiros são frequentemente convidados a comparecer prestar depoimento perante os comitês. Os comissários ou representantes da Comissão Europeia, independentemente da nacionalidade, prestam depoimentos regularmente. Os comitês selecionados frequentemente obtêm informações por escrito de pessoas no exterior ou de órgãos representativos".

³⁹ Anil Kashyap (que mora e trabalha no Canadá), Membro Externo do Comitê de Política Financeira, Bank of England (16 de janeiro de 2019); Benoit Rochet, Vice-CEO, Port of Calais (5 de junho de 2018); e Joachim Coens, CEO, Port of Zeebrugge (5 de junho de 2018).

⁴⁰ [Q3781](#)

eficácia das empresas de tecnologia em agir contra conteúdo que foi classificado como prejudicial; “Uma abordagem seria dizer se as empresas têm os sistemas, os processos e a governança implementados com a transparência necessária para promover responsabilização pública e responsabilização perante o Parlamento, que o país pode cumprir o seu dever de cuidado ou que os danos estejam sendo tratados de modo consistente e efetivo”.⁴¹

33. No entanto, caso a Ofcom seja solicitada a assumir o papel de regulador da capacidade das empresas de mídia social, ele precisará receber novos poderes para investigar. Sharon White disse ao comitê que “seria absolutamente fundamental ter poderes legais para coletar informações numa área abrangente”.⁴²

34. O Conselho Britânico de Segurança na Internet (UKCIS) é uma nova organização, patrocinada pelo Departamento Digital, da Cultura, dos Meios de Comunicação e Esporte, pelo Departamento de Educação e pelo Ministério do Interior, que reúne mais de 200 organizações com a intenção de preservar a segurança das crianças no ambiente online. Seu site afirma: “Se é inaceitável offline, também é inaceitável online.” Seu foco também abrange danos causados no ambiente virtual, como: cyberbullying e exploração sexual; radicalização e extremismo; violência contra meninas e mulheres; crime de ódio e discurso de ódio; e formas de discriminação contra grupos protegidos pela Lei da Igualdade.⁴³ Guy Parker, CEO da Autoridade de Padronização de Publicidade, nos disse que o governo poderia decidir se incluirá danos à imagem em sua definição de danos on-line.⁴⁴

35. Acreditamos que o Conselho de Segurança da Internet do Reino Unido deve incluir em seu escopo “o risco para a democracia”, como identificado no “Livro de Danos” do Centro de Tecnologia Humana, particularmente em relação a filmes deepfake. Observamos que o Facebook é membro do UKCIS e, devido à sua potencial influência, entendo por quê. No entanto, dada a atitude do Facebook durante esta investigação, temos preocupações sobre a boa-fé em sua prática comercial e sua capacidade de participar do trabalho do UKCIS na preservação do interesse público, em oposição aos seus próprios interesses.

36. Quando o Secretário do Departamento Digital, da Cultura, dos Meios de Comunicação e Esporte Digital (DCMS), Rt Hon Jeremy Wright MP, foi questionado sobre a formulação de um espectro de danos on-line, ele deu uma resposta limitada: “O que precisamos entender é o grau em que as pessoas estão sendo enganadas ou o grau de interferência ou influência inapropriada nas eleições, e se precisamos conceber respostas e defesas apropriadas. Faz parte de um cenário muito mais abrangente e não acho correto tentar segmentá-lo.”⁴⁵ No entanto, tendo estabelecido as dificuldades em torno da definição, disseminação e responsabilidade dos danos on-line, o Secretário de Estado foi mais sincero quando questionado sobre a regulamentação das empresas de mídia social e disse que o Reino Unido deveria assumir papel de liderança:

Meu ponto de partida é buscar saber quais são os danos e quais as responsabilidades que podemos legitimamente esperar que as entidades on-line tenham, para assim nos ajudar a minimizar ou, de preferência, eliminar esses danos. Então, depois de estabelecer essas responsabilidades, definir os sistemas que devem estar em vigor para auxiliar no exercício dessas responsabilidades.⁴⁶

⁴¹ [Q3784](#)

⁴² [Q3785](#)

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

⁴⁴ [Q4115](#)

⁴⁵ [Q255](#)

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

Esperamos que o White Paper do Governo traga uma visão geral sobre a legislação adequada para garantir que haja segurança on-line de forma adequada e significativa, detalhando também o papel esperado do UKCIS.

37. Nosso Relatório Preliminar recomendou que sejam estabelecidas responsabilidades legais claras para as empresas de tecnologia agirem contra conteúdo prejudicial ou ilegal em seus sites. Existe agora uma necessidade urgente de estabelecer regulamentação independente. Acreditamos que um Código de Ética obrigatório deve ser estabelecido, supervisionado por um regulador independente, estabelecendo o que constitui conteúdo prejudicial. O regulador independente teria poderes previstos em lei para monitorar as principais empresas de tecnologia; isso criaria um sistema regulador de conteúdo on-line que é tão eficaz quanto o das indústrias de conteúdo off-line.

38. Como dissemos em nosso Relatório Preliminar, esse Código de Ética deve ser semelhante ao Código de Transmissão emitido pela Ofcom — baseado nas diretrizes estabelecidas na seção 319 da Lei de Comunicações de 2003. O Código de Ética deve ser desenvolvido por especialistas técnicos e supervisionado pelo regulador independente, a fim de estabelecer por escrito o que é e o que não é aceitável nas redes sociais. Deve incluir o conteúdo nocivo e ilegal que foi notificado às empresas para remoção pelos seus usuários, ou que seja facilmente identificável pelas próprias empresas de tecnologia.

39. O processo deve estabelecer uma responsabilidade clara e legal para as empresas de tecnologia agirem contra o conteúdo prejudicial e ilegal presente em sua plataforma, e essas empresas devem ter sistemas apropriados para classificar e remover certos 'tipos de danos' e garantir que as estruturas de segurança cibernética estejam em funcionamento. Se as empresas de tecnologia (incluindo engenheiros técnicos envolvidos na criação do software para as empresas) não cumprirem as obrigações previstas nesse Código e não agirem para evitar a distribuição de conteúdo nocivo e ilegal, o regulador independente deve ter a capacidade de instaurar um processo judicial contra elas, com a possibilidade de aplicar-lhes grandes multas como penalidade pelo não cumprimento do Código.

40. Esse mesmo órgão público deve conferir poderes legais para obtenção de qualquer informação de empresas de mídia social que sejam relevantes para seus inquéritos. Pode incluir a capacidade de verificar quais dados de determinado usuário estão sendo armazenados, quando solicitado por esse usuário. Esse órgão também deve ter acesso aos mecanismos e algoritmos de segurança das empresas de tecnologia, para garantir que estejam operando com responsabilidade. Esse órgão público deve estar acessível ao público e ser capaz de receber reclamações de membros da população sobre as empresas de mídia social. Pedimos ao governo que apresente essas propostas em seu próximo White Paper.

Uso de dados pessoais e dados inferidos

41. Quando Mark Zuckerberg depôs ao Congresso em abril de 2018, após o escândalo da Cambridge Analytica, ele fez a seguinte afirmação: "Você deve ter controle total sobre seus dados [...] Se não estamos comunicando essa condição com clareza, é um ponto muito importante que requer atenção da nossa parte". Quando perguntado sobre quem é o dono do seu “perfil virtual”, Zuckerberg respondeu que as próprias pessoas são donas de todo o “conteúdo” que carregam e podem excluí-lo quando quiserem.⁴⁷ No entanto, o respectivo perfil utilizado para fins publicitários de cada usuário, criado

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

pelo Facebook, não pode ser acessado, controlado ou excluído pelos usuários. É difícil conciliar esse fato com a afirmação de que os usuários são donos de todo o "conteúdo" que eles carregam.

No Reino Unido, a proteção de dados do usuário é garantida pelo Regulamento Geral de Proteção de Dados (GDPR).⁴⁸ No entanto, dados 'inferidos' não são protegidos; isso inclui características que podem ser inferidas sobre um usuário, não com base em informações específicas que eles compartilharam, mas por meio da análise do seu perfil de dados. Isso, por exemplo, permite que partidos políticos identifiquem apoiadores em sites como o Facebook, por meio da correspondência de perfil de dados e da ferramenta de direcionamento de publicidade chamada de 'público semelhante'. De acordo com a própria descrição do Facebook de 'públicos semelhantes', os anunciantes têm a vantagem de alcançar novas pessoas no Facebook “que provavelmente estarão interessadas pelos seus negócios, pois são semelhantes aos clientes existentes”.⁴⁹

43. O Relatório do ICO publicado em julho de 2018 questiona a suposição de que os partidos políticos não consideram dados inferidos como informações pessoais:

Nossa investigação constatou que os partidos políticos não consideravam dados inferidos como informações pessoais, pois não eram informações baseadas em fato. No entanto, a visão do ICO é que, como essas informações se baseiam em suposições traçadas a partir dos interesses e preferências dos indivíduos, podendo ser atribuídas a indivíduos específicos, essas informações são pessoais e os requisitos da lei de proteção de dados se aplicam a elas.⁵⁰

44. Os dados inferidos são, portanto, considerados pelo ICO como dados pessoais, o que se torna um problema quando os usuários são informados de que são donos dos seus próprios dados e que têm poder sobre o destino e sobre o uso desses dados. Proteger nossos dados nos ajuda a proteger o passado, mas precisamos da proteção das inferências e dos usos da Inteligência Artificial (IA) para proteger o nosso futuro.

45. A Comissária para Informação, Elizabeth Denham, apresentou suas preocupações sobre o uso de dados inferidos em campanhas políticas quando depôs perante o Comitê em novembro de 2018. Disse:

Existe um volume perturbador de desrespeito pelos dados pessoais dos eleitores e possíveis eleitores. É assim que eu vejo tudo isso. Aquilo com que as pessoas estão acostumadas no comércio, envolvendo direcionamento comportamental, foi transferido — ou transformado — para a arena política. Foi por isso que pedi um tempo ético, para que possamos fazê-lo da forma correta. Não queremos usar esse mesmo modelo utilizado na venda de pacotes turísticos, sapatos e carros para o relacionamento com pessoas e eleitores. As pessoas esperam mais do que isso. Precisamos de um tempo para examinar os códigos, observar as práticas das empresas de mídia social e agir nos casos em que elas descumpriram a lei. Para nós, o principal objetivo disso é abrir a cortina e mostrar ao público o que está acontecendo com seus dados pessoais.⁵¹

46. Com referência específica ao uso de 'perfis similares' no Facebook, Elizabeth Denham disse ao Comitê que “deveriam ser transparentes com as pessoas [usuários]. Eles precisariam saber que um partido político ou um deputado está fazendo uso de perfis similares. A falta de transparência é um

April 2018.

⁴⁸ [California Privacy Act homepage](#), acesso em 18 de dezembro de 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.

⁵¹ [Q4011](#)

problema”.⁵² Quando perguntamos à Comissária para Informação se ela achava que o uso de 'perfis similares' era legal sob a GDPR, ela respondeu: “A análise detalhada deve ser feita de acordo com a GDPR, mas entendo que o público não se sente confortável com o uso de perfis similares, e que precisamos de transparência”.⁵³ As pessoas precisam ter ciência de que as informações fornecidas para um propósito específico estão sendo usadas para inferir informações sobre eles para outro propósito.

47. O Secretário de Estado, Rt Hon Jeremy Wright MP, também nos disse que o arcabouço ético e regulatório relacionado a IA deve se desenvolver ao lado da tecnologia, não "correr para alcançá-la", como aconteceu com outras tecnologias no passado.⁵⁴ Vamos explorar as questões que envolvem IA de forma mais detalhada, em nossa investigação sobre tecnologias imersivas e viciantes, lançada em dezembro de 2018.⁵⁵

48. Apoiamos a recomendação do ICO de que os dados inferidos devem receber a mesma proteção em lei concedida às informações pessoais. As proteções da lei de privacidade devem extrapolar as informações pessoais para incluir modelos usados para fazer inferências sobre determinada pessoa. Recomendamos que o governo estude a maneira pela qual as proteções da lei de privacidade podem ser expandidas para alcançar modelos usados para fazer inferências sobre indivíduos, em particular durante campanhas políticas. Isso garantirá que as inferências sobre os indivíduos sejam tratadas como mesmo grau de importância que as informações pessoais das pessoas.

Papel aprimorado do ICO e responsabilização de empresas de tecnologia

49. Em nosso Relatório Preliminar, pedimos que o ICO fosse dotado de maior capacidade para atuar como um “xerife no oeste selvagem da Internet” e para se antecipar a futuras tecnologias. O ICO precisa ter o mesmo conhecimento técnico especializado, se não mais, do que as organizações fiscalizadas.⁵⁶ Recomendamos a imposição de uma taxa sobre as empresas de tecnologia que operam no Reino Unido, para ajudar no custeio desse aparato, de maneira semelhante à que ocorre com o setor bancário, que paga pelos custos operacionais da Autoridade de Conduta Financeira.⁵⁷

50. Numa pergunta sobre essa cobrança, o Secretário de Estado disse, especificamente a respeito do Facebook: “Posso garantir ao Comitê que se o Facebook disser que não deseja pagar uma taxa, essa resposta não será levada em conta para definirmos se devemos ou não estabelecer a cobrança de uma taxa.”⁵⁸ Ele também nos disse que “francamente, nem eu, nem o ICO, acreditamos que existe limitação orçamentária para realizar o trabalho que precisa ser feito neste momento. [...] Se vamos realizar novas atividades, seja por conta de novas regras regulatórias ou por causa de novas políticas educacionais, por exemplo, então isso precisa ser custeado de alguma forma. Portanto, acho que a imposição de uma taxa é algo que vale a pena ser considerado”.⁵⁹

51. Em nosso Relatório Preliminar, recomendamos a imposição de uma taxa sobre as empresas de tecnologia que operam no Reino Unido, para custear o trabalho aprimorado do ICO. Reiteramos

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.

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](#)

essa recomendação. A decisão do Chanceler, em seu Orçamento de 2018, de impor um novo imposto de serviços digitais de 2% sobre as receitas das grandes empresas de tecnologia no Reino Unido a partir de abril de 2020, demonstra que o governo está aberto à ideia de aplicar uma taxa sobre as empresas de tecnologia. A resposta do governo ao nosso Relatório Preliminar implicava que não daria qualquer apoio financeiro adicional ao ICO, contrariando a nossa recomendação. Instamos o governo a reavaliar essa posição.

52. A proposta de um novo sistema e nova regulação independentes devem contar com custeio adequado. Recomendamos a imposição de uma taxa sobre as empresas de tecnologia que operam no Reino Unido para financiar esse trabalho.

3 Uso e segmentação de dados

Introdução

53. O ICO publicou seu relatório de “Investigação sobre o uso da análise de dados em campanhas políticas” em 6 de novembro de 2018, no mesmo dia em que o Comissário para Informação e o Vice-Comissário para Informação depuseram perante o Comitê. O relatório foi uma atualização da investigação sobre o uso da análise de dados para fins políticos, iniciada em maio de 2017. Ele afirma que “tinha pouca ideia do que estava por vir. Dezoito meses depois, várias jurisdições estão lutando para manter os princípios democráticos fundamentais num cenário em que as tecnologias digitais são opacas”.⁶⁰ E o relatório continuou revelando a extensão das práticas ilegais que ocorreram durante esse período:

Descobrimos um desrespeito perturbador à privacidade pessoal dos eleitores. As redes sociais, partidos políticos, centrais de dados e agências de referência de crédito começaram a questionar seus próprios processos — gerando uma repercussão enorme no ecossistema de big data. Usamos toda a extensão dos poderes de investigação que nos foram concedidos, e onde verificamos que houve descumprimento da lei, agimos. Emitimos penalidades pecuniárias e notificações determinando que as empresas cumpram a lei. Provocamos a abertura de processos criminais pelos órgãos policiais e processos administrativos por outros órgãos reguladores, de acordo com cada caso. E onde não encontramos comprovação de ilegalidade, fomos transparentes a respeito dessas constatações. Nossa investigação descobriu problemas importantes, atos de negligência e descumprimentos da lei.

54. O foco deste capítulo são os problemas relacionados a dados apresentados em nosso Relatório Preliminar. Foi feita a atualização de acordo com os novos acontecimentos, quando foi esse o caso, e fizemos recomendações ao Governo, para garantir que futuramente tais práticas ilícitas serão tratadas de forma eficaz. Como foi dito por Elizabeth Denham em seu depoimento em novembro de 2018: “Este é um momento para fazermos uma pausa, para examinar códigos, examinar as práticas das empresas de mídia social, tomar medidas nos casos de descumprimento da lei”.⁶¹

55. Também focaremos nos documentos do Facebook de 2011 a 2015, que foram fornecidos à justiça da Califórnia pelo Facebook, sob sigilo, num processo movido por um desenvolvedor de aplicativos. O Comitê determinou a entrega desses documentos a uma pessoa no Reino Unido em 19 de novembro de 2018, e nós publicamos parte dele em 5 de dezembro de 2018. Adotamos essa postura incomum

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

⁶¹ [Q4011](#)

por acreditar que essa informação é de interesse público, inclusive para reguladores, como restou demonstrado.

A multa aplicada pelo ICO sobre o Facebook

56. O ICO afirmou em seu relatório de novembro de 2018 que está em processo de encaminhar os problemas identificados sobre as funções e técnicas de direcionamento empregadas pelo Facebook "para monitorar hábitos, interações e comportamento de navegação de indivíduos na Internet e diferentes dispositivos à Comissão de Proteção de Dados da Irlanda, por se tratar da principal autoridade fiscalizadora do Facebook nos termos do Regulamento Geral de Proteção de Dados (GDPR).⁶²

57. Em 25 de outubro de 2018, o ICO impôs a multa máxima possível no momento — £500.000 — sobre o Facebook, de acordo com a lei anterior de proteção de dados do Reino Unido (antes da aprovação, em maio de 2018, do GDPR), pela falta de transparência e segurança relacionados à coleta de dados, descumprindo dos princípios 1 e 7 de proteção de dados da Lei de Proteção de Dados de 1998.⁶³ A partir daí, o Facebook recorreu da multa, alegando que o ICO não encontrou evidências de que os dados pessoais dos usuários do Reino Unido haviam sido realmente compartilhados. No entanto, o Comissário para Informação nos disse que a aplicação da multa pelo ICO não levou em consideração o compartilhamento de dados de usuários do Reino Unido. Em vez de:

A multa que aplicamos sobre o Facebook foi porque ele permitiu que aplicativos e desenvolvedores de aplicativos coletassem as informações pessoais dos clientes sem o consentimento consciente deles — pense em amigos, e amigos de amigos — e, em seguida, o Facebook não conseguiu manter as informações em segurança. [...] Não se aplica aqui o princípio de que não ocorre ato ilícito se não houver prejuízo. As empresas são responsáveis por proteger proativamente as informações pessoais, e essa é a política praticada no Reino Unido faz trinta anos. [...] O Facebook descumpriu a lei de proteção de dados, e o Facebook não pode comparar essa atitude com o encaminhamento de e-mail, porque não é disso que se trata; trata-se da divulgação de informações de perfil dos usuários sem seu conhecimento e consentimento.⁶⁴

58. Elizabeth Denham disse ao Comitê que o ICO “descobriu que suas práticas de negócios e a maneira como os aplicativos interagem com os dados na plataforma violam a lei de proteção de dados. Essa é uma declaração muito forte e uma grande descoberta”.⁶⁵ Em seu depoimento, Elizabeth Denham disse que o Facebook enxerga as decisões do comissário federal de privacidade no Canadá e do ICO irlandês como meras orientações.⁶⁶ De acordo Elizabeth Denham, depois do depoimento de Richard Allan, Vice-Presidente de Políticas de Soluções do Facebook, ela entende que "a menos que haja uma determinação legal que obrigue uma mudança no modelo de negócios e na prática deles, eles não promoverão tal mudança”.⁶⁷

59. As multas do GDPR, aplicadas em 25 de maio de 2018, são muito mais altas do que o valor máximo de £500.000 previsto na Lei de Proteção de Dados de 1998. O novo regulamento prevê multas

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

⁶³ Mesma referência acima.

⁶⁴ [Q4284](#)

⁶⁵ [Q4294](#)

⁶⁶ [Q4284](#)

⁶⁷ [Q4284](#)

administrativas de até 4% do faturamento global anual, ou € 20 milhões, o que for maior.⁶⁸ No quarto trimestre de 2018, a receita do Facebook aumentou 30% em relação à do ano anterior, para US\$ 16,9 bilhões, e seus lucros aumentaram 61%, para US\$ 6,9 bilhões, o que representa uma possibilidade de multas muito maiores no futuro.⁶⁹

O ICO, SCL Group e Cambridge Analytica

60. Nosso Relatório Preliminar descreveu uma “complexa rede de relacionamentos”, que começou com um grupo de empresas chamado de SCL [Strategic Communications Laboratories], do qual a Cambridge Analytica fazia parte.⁷⁰ O Grupo SCL entrou em processo de falência em abril de 2018. O último relatório do ICO, publicado em novembro de 2018, comentou sua investigação no Cambridge Analytica. Naquele momento, o ICO já havia:

- emitido intimação exigindo que a Cambridge Analytica processe a solicitação de acesso a conteúdo apresentada pelo Professor David Carroll;⁷¹
- instaurado um processo criminal por não lidar adequadamente com a intimação;
- identificado “descumprimentos graves dos princípios de proteção de dados e teria emitido uma multa significativa se a empresa não tivesse entrado em processo de falência”;
- encaminhado o caso da Cambridge Analytica para o Serviço de Falência.⁷²

61. Em 9 de janeiro de 2019, a SCL Elections Ltd foi multada em £15.000 por não cumprir a intimação emitida pelo ICO em maio de 2018, relacionada à solicitação de acesso a conteúdo de David Carroll. A empresa se declarou culpada, por meio de seus administradores, por descumprir a Seção 47 (1) da Lei de Proteção de Dados de 1998 (novamente, a multa estava foi imposta com base na legislação anterior, e não com o GDPR). O Tribunal de Magistrados de Hendon também determinou que a empresa pagasse £6.000 em custas e uma compensação de vítima de £170. Numa resposta pública, a Comissária da Informação, Elizabeth Denham fez a seguinte declaração:

Esse processo, o primeiro contra a Cambridge Analytica, é um aviso de que existem consequências para quem desrespeita a lei. Independentemente de onde você viva no mundo, se seus dados estiverem sendo processados por uma empresa do Reino Unido, aplicam-se as leis de proteção de dados do Reino Unido. As organizações que lidam com dados pessoais devem respeitar os direitos legais de privacidade das pessoas. Onde isso não acontecer e as empresas ignorarem os avisos de aplicação do ICO, tomaremos medidas cabíveis.⁷³

62. Estávamos ansiosos para saber quando e quais pessoas que trabalhavam no Facebook souberam

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.

⁷⁰ [Desinformação e 'notícias falsas': Interim Report](#), DCMS Committee, Fifth Report of Session 2017-19, HC 363, 29 July 2018, para 124.

⁷¹ Para mais informações sobre a solicitação de acesso a conteúdo do Professor David Carroll, vide parágrafo 100 do [Desinformation 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.

sobre o descumprimento da GSR/Cambridge Analytica. O ICO confirmou, numa manifestação dirigida ao Comitê, que três “gerentes seniores” estavam envolvidos em trocas de e-mail no início de 2015 sobre o descumprimento do GSR antes de dezembro de 2015, quando foi relatado pela primeira vez pelo The Guardian.⁷⁴ A pedido do ICO, concordamos em manter os nomes em sigilo, mas parece que essas informações importantes não foram compartilhadas com os executivos mais seniores do Facebook, levando-nos a questionar os motivos para esse tratamento.

63. A infração GSR/Cambridge Analytica foi de tal monta e com tal extensão que sua ocorrência deveria ter sido encaminhada imediatamente para o Mark Zuckerberg, CEO da empresa. A falta em encaminhar o caso ao CEO comprova que o Facebook não tratou esse descumprimento com a seriedade que o caso merecia. Foi um profundo fracasso de governança no Facebook, que o CEO não estava ciente do que estava acontecendo, de acordo com a empresa agora, até que o problema se tornou público para todos em 2018. O incidente demonstra uma fragilidade fundamental do Facebook na gestão das suas responsabilidades em relação às pessoas cujos dados são usados para alcançar os interesses comerciais da empresa.

Facebook e o Decreto de Consentimento da Comissão Federal do Comércio de 2011

64. Quando Richard Allan, vice-presidente de soluções de políticas do Facebook, depôs em novembro de 2018, ele disse que “nossa intenção é que vocês não sejam surpreendidos com a forma como seus dados são usados [...] O fato de haver surpresa não é um bom resultado para nós”.⁷⁵ No entanto, muitas vezes, este Comitê e o público em geral são surpreendidos com a natureza porosa dos protocolos de segurança de dados do Facebook e com a extensão em que os dados pessoais dos usuários foram compartilhados e continuam sendo compartilhados até hoje. Ainda existe o risco de aumento considerável da escala desse compartilhamento de dados, diante do anúncio que no início de 2020 o Facebook planeja integrar a infraestrutura técnica do Messenger, Instagram e WhatsApp, que, ao todo, possuem mais de 2,6 bilhões de usuários.⁷⁶

65. O Decreto de Consentimento da Comissão Federal do Comércio de 2011 é um exemplo da maneira pela qual os protocolos e práticas de segurança do Facebook nem sempre estão alinhados. Em novembro de 2009, os usuários do Facebook tinham uma 'página central de privacidade', com o seguinte texto pelo Facebook: "Controle quem pode ver seu perfil e as suas informações pessoais". O perfil e as informações pessoais de um usuário podem incluir: nome; gênero; endereço de e-mail; aniversário; foto do perfil; cidade natal; informações de relacionamento; visões políticas e religiosas; gostos e interesses; educação e trabalho; lista de amigos; fotos e vídeos; e mensagens.⁷⁷

66. Em novembro de 2011, a Comissão Federal de Comércio (FTC) dos EUA apresentou uma queixa contra o Facebook, alegando que, de maio de 2007 a julho de 2010, permitiu acesso irrestrito, para desenvolvedores externos de aplicativos, a informações sobre o perfil pessoal dos usuários do Facebook e informações relacionadas, apesar de o Facebook ter informado aos usuários que os aplicativos da plataforma “acessarão apenas as informações de perfil que esses aplicativos precisem para operar”.⁷⁸ A queixa da FTC lista vários exemplos de compromissos assumidos pelo Facebook

⁷⁴ Harry Davies publicou previamente este artigo [Ted Cruz using firm that harvested data on millions of unwitting Facebook users](#), in The Guardian, on 11 December 2015, que inicialmente revelou a coleta de dados promovida pelo Facebook.

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 Referência acima, parágrafo 30.

com os seus usuários que não foram cumpridos:

- Em dezembro de 2009, o Facebook alterou seu site para que certas informações que os usuários possam ter designado como particulares — como Lista de Amigos — se tornassem públicas. Eles não alertaram os usuários que essa mudança estava chegando, nem obtiveram a aprovação prévia dos usuários;
- O Facebook afirmou que aplicativos de terceiros que os usuários instalaram teriam acesso apenas às informações do usuário necessárias para operar. Na verdade, os aplicativos podem acessar quase todos os dados pessoais dos usuários;
- O Facebook disse aos usuários que poderiam restringir o compartilhamento dos seus dados a públicos limitados — por exemplo, com "Somente Amigos". Na verdade, o fato de selecionar "Somente Amigos" não impedia que suas informações fossem compartilhadas com aplicativos de terceiros que amigos dos usuários utilizavam;
- O Facebook tinha uma opção de "Aplicativos Verificados", que deveria garantir a segurança dos aplicativos participantes, mas não era esse o caso;
- Apesar de prometer aos usuários que não compartilhariam suas informações pessoais com os anunciantes, o Facebook compartilhou tais informações;
- O Facebook afirmou que, quando os usuários desativavam ou excluía suas contas, suas fotos e vídeos ficavam inacessíveis, mas esse conteúdo ainda estava acessível;
- O Facebook afirmou que cumpria a Estrutura de Porto Seguro EUA/UE que governa a transferência de dados entre os EUA e a União Europeia, mas não era esse o caso.⁷⁹

67. Ao celebrar o acordo, o Facebook concordou em obter o consentimento dos usuários antes de compartilhar seus dados com terceiros. O acordo também exigia que o Facebook estabelecesse um “programa abrangente de privacidade” para proteger os dados dos usuários e realizasse auditorias independentes de terceiros a cada dois anos pelos próximos 20 anos para certificar que possui um programa de privacidade que atende ou excede o requisito previsto pela FTC.

68. Quando perguntaram a Richard Allan em que momento o Facebook havia feito essas alterações em seus próprios sistemas, para impedir que os desenvolvedores recebessem informações (o que resultou numa burla das configurações de privacidade dos usuários do Facebook), ele respondeu que a mudança havia ocorrido em 2014:

A FTC rejeitou a ideia de que os dados podem ter sido acessados do Facebook sem consentimento e sem permissão. Estávamos seguros de que os controles que implementamos representavam consentimento e permissão — outros contestariam isso, mas acreditávamos que tínhamos controles que faziam isso e que nos cobriam naquele período até 2014”.⁸⁰

Richard Allan estava se referindo aqui à mudança da versão 1 do API [Application Programming Interface] do Facebook para a sua versão 2 mais restritiva.

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

⁸⁰ [Q4178](#)

69. Depois do acordo, Richard Allan foi questionado se Mark Zuckerberg sabia que o Facebook continuava permitindo que os desenvolvedores tivessem acesso a essas informações. Ele respondeu que o Mark Zuckerberg e "todos nós" sabíamos que a plataforma continuava permitindo o acesso às informações. Quanto ao descumprimento do Decreto de Consentimento da FTC (mais de dois anos depois de o Facebook ter concordado com ele), ele nos disse que "contanto que mantivéssemos os controles adequados, isso não era visto como algo que descumprisse a ordem de consentimento da FTC".⁸¹

70. Richard Allan estava se referindo à Acusação 1 da queixa apresentada pela Comissão Federal de Comércio de 2011, que afirma ser falsa a alegação do Facebook de que os controles adequados estavam sendo mantidos:

O Facebook declarou, de forma expressa ou implícita, que, por meio das Configurações de Privacidade, os usuários podem restringir o acesso às informações de seu perfil para grupos específicos, como "Somente Amigos" ou "Amigos de Amigos". Na verdade, em muitos casos, os usuários não podiam restringir o acesso às informações de seu perfil a grupos específicos, como "Apenas Amigos" ou "Amigos de Amigos" por meio das Configurações de Privacidade do usuário. Em vez disso, essas informações podiam ser acessadas pelos Aplicativos de Plataforma que seus Amigos usavam.⁸²

71. O argumento de Richard Allan era que, enquanto o Facebook continuava a permitir o mesmo acesso a dados —previsto na primeira denúncia da queixa da FTC e da qual o CEO, Mark Zuckerberg, também estava ciente—, isso era aceitável devido ao fato de que o Facebook supostamente havia adotado "controles" que representariam consentimento e permissão.

72. Ashkan Soltani, pesquisador e consultor independente, que nessa época ocupava o cargo de técnico de primeiro grau na Comissão Federal de Comércio, trabalhou na investigação do Facebook entre 2010 e 2011 e se tornou o Chefe de Tecnologia da FTC em 2014. Perante o nosso Comitê, ele questionou o depoimento prestado por Richard Allan:

Richard Allan corrigiu um dos comentários, que dizia especificamente que os aplicativos da Versão 1 do API não tinham acesso irrestrito às informações pessoais. Na verdade, essa informação é falsa. No acordo celebrado com a FTC em 2011, a FTC alegou que, se um usuário tivesse um aplicativo instalado, ele teria acesso a quase todas as informações de perfil do usuário, mesmo que essas informações fossem definidas como privadas. Acho que existe um problema em relação à V1, mas isso ocorreu no início da V1, e acredito que só foi enfrentado após o acordo.⁸³

73. Ashkan Soltani esclareceu o cronograma dos eventos:

Os prazos variam, mas, na minha opinião, foi a V1, se eles estão considerando as mudanças em 2014 como V2.⁸⁴ Em resumo, descobri que o Facebook permitiu inúmeras vezes que os

⁸¹ [Q4184](#)

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

⁸³ [Q4327](#)

⁸⁴ Os APIs do Facebook foram lançados da seguinte forma: A V1.0 foi lançada em abril de 2010, a V2.0-2.12 foi lançada em abril de 2014 e a V3.0-3.2, lançada em abril de 2018. A V2 limitou o acesso em nível industrial dos desenvolvedores do Facebook às informações dos usuários. Mas no mesmo dia em que o Facebook lançou a V2, anunciou sua maior iniciativa de rastreamento e direcionamento de anúncios até o momento. Chamada de Facebook Audience Network, ampliou o perfil de dados e a direcionamento de anúncios da empresa, aplicativos e serviços próprios para o resto da Internet.

desenvolvedores acessassem informações pessoais de usuários e amigos, a despeito das configurações de privacidade e as declarações de política.⁸⁵

74. Richard Allan não especificou quais controles foram implementados pelo Facebook, mas eles não impediram que os desenvolvedores de aplicativos, que não eram autorizados pelo usuário, acessassem dados que não deveriam ser compartilhados (além de um pequeno grupo de amigos na página de configurações de privacidade). A queixa da FTC contestou tanto o fato de os aplicativos terem acesso irrestrito às informações dos usuários quanto os controles de privacidade que de acordo com o Facebook deveriam permitir que os usuários controlassem quem viu suas informações pessoais, enquanto que, de fato, não representavam as informações a que os aplicativos tiveram acesso.

75. A repercussão foi muito negativa em março de 2018, quando o escândalo de dados da Cambridge Analytica foi revelado e a grande maioria dos usuários do Facebook não fazia ideia de que seus dados podiam ser acessados por desenvolvedores desconhecidos, apesar de terem definido configurações de privacidade, proibindo especificamente essa prática.⁸⁶ Richard Allan também admitiu para nós que as pessoas poderiam realmente questionar a posição do Facebook: "entendemos que os controles que implementamos constituíam consentimento e permissão — uma posição passível de questionamento".⁸⁷ Sua intenção era justificar a permissão de acesso permanente concedida pelo Facebook aos desenvolvedores de aplicativos, afirmando que os usuários haviam concordado com esse acesso. O fato de o Facebook continuar a permitir esse acesso após o Decreto de Consentimento não é uma informação nova; as novas informações são uma confissão de Richard Allan de que o CEO e a alta administração — “todos nós” — sabíamos que o Facebook continuava permitindo que a prática ocorresse, apesar das declarações públicas sobre sua mudança de política. Isso, as pessoas podem muito bem contestar, foi enganoso, temos que admitir.⁸⁸ Ashkan Soltani nos disse que acreditava que o Facebook descumpriu o Decreto de Consentimento e a FTC confirmou publicamente que está investigando a empresa.⁸⁹

76. O escândalo da Cambridge Analytica só foi possível graças às políticas do Facebook. Se tivesse cumprido totalmente o acordo celebrado com a FTC, não teria ocorrido. A Queixa da Comissão Federal de Comércio dos EUA (FTC) de 2011 contra o Facebook — por não proteger os dados dos usuários e por permitir que os desenvolvedores de aplicativos obtivessem o acesso que desejavam, sem restrições, aos dados do usuário — afirmou que o Facebook construiu a empresa de modo a facilitar a ocorrência de abusos de dados. Quando questionada sobre a falha por parte do Facebook em tomar as medidas cabíveis a partir da denúncia da FTC, Elizabeth Denham, Comissária da Informação, disse: “Estou muito desapontada com o Facebook, por ser uma empresa tão inovadora, por não ter focado, dado mais atenção e recursos para proteger os dados das pessoas”.⁹⁰ Nós, também, estamos decepcionados.

Facebook e o caso Six4Three

77. Um processo em curso no Tribunal Superior de San Mateo, na Califórnia, também diz respeito às práticas de dados do Facebook. A alegação diz que o Facebook descumpriu a privacidade dos cidadãos dos EUA ao explorar ativamente sua política de privacidade e que Mark Zuckerberg construiu um esquema de maximização de receita e de supressão da concorrência em meados de 2012, ao discutir o

⁸⁵ [Q4327](#)

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

⁸⁷ [Q4178](#)

⁸⁸ [Q4184](#)

⁸⁹ [Q4340](#)

⁹⁰ [Q4316](#)

caso com Chris Cox, Javier Olivan, Sheryl Sandberg, Dan Rose e Sam Lessin, e outros colegas seniores do Facebook, em suas tentativas de mudar os negócios do Facebook de um modelo de desktop voltado para jogos e aplicativos para um modelo de negócios de publicidade, utilizando smartphones.⁹¹

78. O "memorando corrigido de pontos e poderes dos réus", apresentado pelo Autor do caso, Six4Three, um desenvolvedor de aplicativos com sede nos EUA, descreve as alegações contra o Facebook. Afirma que o Facebook fez uso dos dados dos seus usuários para convencer os desenvolvedores de aplicativos a criar plataformas em seu sistema, prometendo acesso aos dados dos usuários, incluindo o acesso aos dados dos amigos dos usuários.⁹² Alega ainda que os desenvolvedores que obtivessem sucesso eram identificados e teriam que fazer repasses de dinheiro para o Facebook. Se os aplicativos se tornassem bem-sucedidos demais, o Facebook teria removido o acesso aos dados, privando-os das informações necessárias para se sobressair. A Six4Three iniciou com o processo em 2015, depois que o Facebook eliminou o acesso dos desenvolvedores aos dados dos amigos, incluindo o acesso do Autor.

79. O Comitê DCMS tomou a medida incomum, mas legal, de requerer cópia desses documentos, produzidos entre 2012 e 2014, apesar de estarem sob sigilo por determinação do Tribunal de San Mateo, pois acreditávamos fortemente que os documentos estavam relacionados especificamente a graves questões de privacidade de dados que exploramos nos últimos 18 meses. O Comitê recebeu os documentos após solicitá-los a Ted Kramer, fundador da Six4three, enquanto ele visitava Londres numa viagem de negócios em novembro de 2018. Ted Kramer obedeceu à determinação da comissão, devido ao risco de desrespeito ao Parlamento. Desde que publicamos esses documentos sigilosos, em 14 de janeiro de 2019, outro tribunal concordou em liberar o sigilo de 135 páginas de memorandos internos do Facebook, estratégias e e-mails de funcionários entre 2012 e 2014, relacionadas ao lucro obtido ilegitimamente pelo Facebook em transações comerciais envolvendo crianças.⁹³ Uma investigação do New York Times publicada em dezembro de 2018 com base em documentos internos do Facebook também revelou que a empresa havia oferecido acesso preferencial aos dados dos usuários a outras grandes empresas de tecnologia, incluindo Microsoft, Amazon e Spotify.⁹⁴

80. Entendemos que a publicação dos documentos feita por nós era de interesse público e também seria de interesse dos órgãos reguladores, em particular o ICO e a FTC. De fato, tanto o Comissário de Informações do Reino Unido, quanto Ashkan Soltani, ex-FTC, concordaram com essa avaliação. Publicamos 250 páginas de provas selecionadas dos documentos em 5 de dezembro de 2018 e, juntamente com a publicação deste Relatório, divulgaremos mais provas. Os documentos destacam a ação agressiva do Facebook contra certos aplicativos, incluindo a privação de acesso a dados que foram originalmente prometidos. Eles destacam o vínculo entre os dados dos amigos e o valor financeiro do relacionamento dos desenvolvedores com o Facebook. Os principais problemas seriam: 'listas de autorização'; o valor dos dados dos amigos; reciprocidade; o compartilhamento de dados de usuários que possuem telefones Android; e ataque à concorrência pelo Facebook.⁹⁵

Listas de Autorização

⁹¹ O antigo modelo do Facebook estava recebendo uma porcentagem dos pagamentos on-line feitos para aplicativos do Facebook (como jogos gratuitos), executados em computadores, mas não em smartphones.

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

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 Os termos específicos serão explicados abaixo.

81. O Facebook celebrou acordos envolvendo 'listas de autorização' com certas empresas. Por esses acordos, após a mudança da plataforma em 2014/15, essas empresas manteriam acesso total aos dados dos amigos. Não está totalmente claro se houve solicitação de consentimento do usuário para isso, nem precisamente como o Facebook decidiu quais empresas deveriam ser incluídas na lista de autorizações.⁹⁶

82. Quando questionado sobre as configurações de privacidade do usuário e acesso a dados, Richard Allan disse de forma consistente que havia controles para limitar o acesso a dados e que as pessoas estavam cientes de como os dados estavam sendo usados. Ele disse que o Facebook estava confiante de que os controles implementados incluíam o consentimento e permissão dos usuários.⁹⁷ Ele admitiu que "seria válido questionar o qual bem as pessoas entendem os controles e se eles são complexos demais", mas disse que as configurações de privacidade não podem ser substituídas.⁹⁸ Finalmente, ele afirmou que: "Nossa intenção é que vocês não sejam surpreendidos com a forma como seus dados são usados. Nossa intenção é que fique claro e que você não seja surpreendido. O fato de haver surpresa não é um bom resultado para nós".⁹⁹

83. Ashkan Soltani rejeitou esta alegação, afirmando que até 2012 não existiam esses controles da plataforma e os controles de privacidade não se aplicavam aos aplicativos. Portanto, mesmo que um usuário defina seu perfil como privado, os aplicativos instalados ainda poderão acessar às informações. Depois de 2012, o Facebook adicionou controles de plataforma e tornou os controles de privacidade aplicáveis aos aplicativos. No entanto, havia aplicativos na "lista de autorizações" que ainda podiam acessar os dados do usuário sem permissão e que, segundo Ashkan Soltani, podiam acessar os dados dos amigos de forma retroativa a quase uma década.¹⁰⁰ Os aplicativos conseguiram burlar a privacidade dos usuários nas configurações da plataforma e acessar as informações de amigos, mesmo quando o usuário desativou a plataforma.¹⁰¹ Este foi um exemplo do modelo de negócios do Facebook que produziu violações de privacidade.

84. A expansão do esquema de lista de permissões resultou num grande número de empresas fechando acordos especiais com o Facebook. Uma discussão por email de novembro de 2013 revela que o Facebook estava gerenciando 5.200 aplicativos na lista de autorizações.¹⁰² Dos documentos que recebemos, os aplicativos a seguir, bem conhecidos, faziam parte da lista de autorizações:

- **Lyft, aplicativo de taxi:** Konstantinos Papamiltiadis, do Facebook, escreveu para o Lyft em 30 de março de 2015: "Até onde eu sei, o ID do aplicativo abaixo foi incluído na lista de autorizações para acesso a todos os Amigos em Comum";¹⁰³

- **AirBnB:** Papamiltiadis escreveu para o Airbnb em 18 de março de 2015: "Como prometido, seguem documentos para o API de Hashed Friends, que podem ser utilizados para classificação social. Deixe-me saber se tem interesse nisso, pois precisaremos assinar um contrato que permita o acesso a esse API";¹⁰⁴

- **Netflix:** Chris Barbour e Papamiltiadis, do Facebook, escreveram para a Netflix em 17 de

⁹⁶ Os documentos da [Six4Three](#), anexos 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 94 e 95, incluem discussões sobre listas de autorização de empresas.

⁹⁷ [Q4178](#)

⁹⁸ Mesma referência acima.

⁹⁹ [Q4188](#)

¹⁰⁰ [Q4343](#)

¹⁰¹ [Q4327](#), Ashkan Soltani.

¹⁰² [Anexo 100](#)

¹⁰³ [Anexo 87](#)

¹⁰⁴ [Anexo 91](#)

fevereiro de 2015, e a Netflix em 13 de fevereiro: “estaremos na lista de autorizações para receber todos os amigos, não apenas amigos conectados”,¹⁰⁵

85. Todas as empresas na lista de permissões usaram um contrato padrão chamado de "Anexo de Acesso Estendido API Privado", de onde foram extraídos os trechos abaixo:

Acesso Estendido aos APIs Privados. De acordo com os termos do Contrato, o FB reserva para si o direito exclusivo de decidir sobre a liberação de Acesso Estendido aos APIs Privados disponíveis para Desenvolvedores para uso em conexão com os Aplicativos de Desenvolvedores. O FB poderá interromper esse acesso a qualquer momento, sem necessidade de apresentar justificativa para fazê-lo. O Acesso Estendido aos APIs Privados e as Diretrizes de Acesso Estendido aos APIs Privados passam a integrar a Plataforma e as Políticas da Plataforma, respectivamente, para efeito do Contrato... "Acesso Estendido aos APIs Privados" significa um conjunto de APIs e serviços prestados pelo FB ao desenvolvedor que permite ao desenvolvedor recuperar dados ou funcionalidades relacionadas ao Facebook que, de modo geral, não estão disponíveis na Plataforma, podendo incluir autenticação permanente, upload de fotos, vídeos e mensagens, além de conexão à agenda.¹⁰⁶

86. A partir dos documentos, também restou claro que a lista de autorizações estava sendo considerada há algum tempo na preparação de todas essas permissões especiais que foram concedidas. Houve uma discussão interna no Facebook, por exemplo, sobre o processo de lista de autorizações em um email enviado em 5 de setembro de 2013: **“Precisamos construir uma experiência coletiva sobre como revisar o acesso concedido e como tomar decisões sobre manter/eliminar/contratar”**.¹⁰⁷

Valor dos dados dos amigos

87. Está claro que o aumento da receita dos principais desenvolvedores de aplicativos foi um dos principais fatores por trás das mudanças nas políticas feitas pelo Facebook. A ideia de vincular o acesso aos dados dos amigos ao valor financeiro do relacionamento dos desenvolvedores com o Facebook era uma característica recorrente dos documentos.

88. A FTC descobriu que o Facebook deturpou as informações prestadas sobre o seu programa de supervisão de aplicativos, especificamente o 'programa de aplicativos verificados', uma revisão que supostamente foi projetada para oferecer aos usuários garantias adicionais e ajudá-los a identificar aplicativos confiáveis. Não existia revisão e não havia fiscalização desses aplicativos. Alguns aplicativos pré-instalados conseguiram burlar as configurações de privacidade ou configuração da plataforma para obter acesso às informações de amigos e informações de usuários, como aniversários e afiliação política, mesmo quando o usuário desativou a plataforma. Por exemplo, o Yelp e o Rotten Tomatoes conseguiram acesso automático às informações pessoais dos usuários.

89. Ashkan Soltani disse ao Comitê:

Em resumo, descobri que o Facebook permite que os desenvolvedores acessem informações pessoais de usuários e amigos, em contraste com as configurações de privacidade e as políticas anunciadas. Essa arquitetura significa que, se um agente mal-intencionado obtiver esses tokens, [...] existe pouca coisa que o usuário possa fazer para impedir que suas informações sejam

¹⁰⁵ [Anexo 92](#)

¹⁰⁶ [Anexo 93](#) - ainda não publicado

¹⁰⁷ 'Gks' e 'Sitevars' fazem referência aos termos internos do Facebook. (aqui com acréscimo de destaque).

acessadas. O Facebook deu prioridade a esses desenvolvedores em detrimento aos seus usuários.¹⁰⁸

90. Como um exemplo da importância que os clientes do Facebook atribuem ao acesso aos dados de amigos, existe uma longa discussão interna no Facebook nos documentos que publicamos — também desde 2013 — em torno dos gastos 'Neko' do Royal Bank of Canada, discutindo também se eles deveriam figurar na lista de autorizações. 'Neko' era o nome interno do Facebook para seu novo produto de publicidade para celular, chamado oficialmente de Mobile App Install Ads.

91. Sachin Monga, do Facebook, enviou um e-mail para Jackie Chang, também do Facebook, em 20 de agosto de 2013, às 10h38. Eles discutiram o prejuízo das mudanças da plataforma para o Royal Bank of Canada: “Sem a capacidade para acessar amigos que não são de aplicativos, o API de mensagens se torna drasticamente menos útil”.

92. Em resposta, minutos depois, Sachin Monga respondeu:

Seria realmente útil para nós se você pudesse primeiramente fornecer as informações abaixo:

2/ eles assinaram um contrato de API estendido quando você os colocou na lista de autorizações desse API?

3/ quem lhe deu autorização interna para conceder acesso a eles pela lista de autorizações? Envie para mim um e-mail ou um link permanente do Grupo de Aprovação da Lista de Autorizações da Plataforma.

4/ Existe orçamento dedicado especificamente para essa integração? Quanto? Precisamos das informações acima e estamos cientes do contexto apresentado.'

93. O próximo email foi de Sachin Monga para Jackie Chang, 10h58, 20 de agosto de 2013:

Obrigado pela resposta rápida. Respostas abaixo:

2/ Eles não assinaram um contrato estendido de API. Eles deveriam ter assinado? Eu não sabia disso...

3/ Foi o Doug que aprovou.

4/ Existe um orçamento dedicado especificamente para a atualização deste aplicativo (todos os Mobile App Install Ads para clientes atuais do RBC, por meio de públicos personalizados). Acredito que será uma das maiores campanhas neko já realizadas no Canadá.¹⁰⁹

94. As discussões internas sobre o Royal Bank of Canada continuaram no outono, citando os precedentes que o Facebook já havia usado em seu processo de acesso estendido à lista de autorizações. Simon Cross escreveu para Jackie Chang, Sachin Monga, Bryan Hurren (Facebook), 25 de outubro de 2013: “+ Bryan que recentemente incluiu a Netflix na lista de autorizações de API de mensagens — ele terá uma idéia melhor de quais contratos precisamos conceder a eles para acessar este API”. No mesmo dia, Bryan Hurren respondeu a Sachin Monga, Jackie Chang e Simon Cross: “No campo das relações públicas, a história é sobre o aplicativo, não o API; portanto, o fato de ele usar o Titan não é

¹⁰⁸ [Q4327](#)

¹⁰⁹ [Anexo 83](#)

muito relevante. Do ponto de vista jurídico, eles precisam de um "Contrato de Acesso Estendido de API" (que utilizamos com a Netflix) que disciplinará o uso daqui para frente e nos dará a liberdade de fazer as alterações mencionadas abaixo pelo Simon (sem ser muito explícito)". Jackie Chang escreveu para o grupo do Facebook, em 28 de outubro de 2013, afirmando "Bryan — você poderia tomar frente da redação deste contrato?"

95. Essas trocas sobre apenas um dos nossos principais clientes do país, o Royal Bank of Canada, demonstram as interligações entre o valor do acesso aos dados dos amigos e os gastos com publicidade, e o processo preferencial de lista de autorizações do Facebook, que vamos avaliar de forma mais detalhada.

O vínculo entre acesso a dados e gastos com publicidade no Facebook

96. A partir dos documentos do caso Six4three, fica claro que o gasto de valores elevados com o Facebook era uma condição para manter o acesso preferencial a dados pessoais. Fazia parte da estratégia da empresa de desenvolvimento de plataforma, ao embarcar no mundo da publicidade móvel. E essa abordagem foi conduzida pelos níveis mais elevados da empresa.

97. Está incluído nos documentos um e-mail entre Mike Vernal, então Vice-Presidente de Produtos de Pesquisa, Local e Desenvolvedor do Facebook, e Mark Zuckerberg, Chris Daniels, Dan Rose e Douglas Pardy, de 7 de outubro de 2012. Ele discute o vínculo entre dados e receita:

Mark Zuckerberg:

Eu estive pensando bastante no modelo de negócios da plataforma neste fim de semana [...] se fizermos isso para que os desenvolvedores possam gerar receita para nós de diferentes maneiras, então seria mais aceitável cobrar um pouco mais pelo uso da plataforma. A ideia básica é que qualquer outra receita que você gerar para receber um crédito referente às taxas que você possui por usar a plataforma. Para a maioria dos desenvolvedores, isso provavelmente cobriria todo o custo que terão. Portanto, em vez de todo mundo nos pagar diretamente, eles usariam nossos pagamentos ou produtos de anúncios.

Um modelo básico pode ser:

- Login no Facebook é sempre gratuito;
- Envio de conteúdo para o Facebook é sempre gratuito;
- Ler qualquer coisa, incluindo amigos, vale muito dinheiro. Talvez na ordem de USD 0,10/usuário a cada ano.

Pelo dinheiro que você passa a dever, você pode pagar de qualquer uma das seguintes maneiras:

- Aquisição dos nossos anúncios em neko ou outro sistema;
- Exibição dos nossos anúncios em seu aplicativo ou website (os aplicativos de tela já fazem isso; -Utilize nossos pagamentos;
- Venda seus itens em nossa loja Karma.

Ou, se a receita que obtivermos dessas cobranças não ultrapassar o valor que você nos deve, pode efetuar um pagamento para nós, diretamente.¹¹⁰

98. Em 27 de outubro de 2012, Mark Zuckerberg enviou um e-mail interno para Sam Lessin, discutindo a vinculação de dados à receita, destacando o fato de que os dados dos usuários eram valiosos e que ele estava cético quanto ao risco de tais dados vazarem entre os desenvolvedores. Ou seja, isso é exatamente o que aconteceu durante o escândalo da Cambridge Analytica. A seguinte citação ilustra esse fato:

Existe muita curiosidade por saber de onde conseguimos obter receita. Tornamos mais fácil para os desenvolvedores usarem nossa rede de pagamentos/anúncios, mas não os obrigamos a fazê-lo? Nós exigiremos deles? Apenas cobramos diretamente um valor e deixamos que os desenvolvedores que utilizarem o acesso a obter o crédito para abater no saldo devedor deles conosco? Não está bem claro para mim esta parte. Não sei se temos um modelo que realmente nos proporcionará a receita que queremos em escala.

Estou cada vez mais convencido a bloquear algumas partes da plataforma, incluindo dados de amigos e possíveis endereços de e-mail para aplicativos móveis. **“Geralmente sou cético quanto ao risco estratégico de vazamento de dados como você imagina.** Concordo que existe um risco claro do lado do anunciante, mas ainda não descobri como isso se conecta ao restante da plataforma. **Acho que vazamos informações para os desenvolvedores, mas simplesmente não consigo pensar num exemplo em que esses dados vazaram de desenvolvedor para desenvolvedor e que tivemos um problema real por causa disso.** Você algum exemplo disso?”¹¹¹

[...]

Sem limitar a distribuição ou o acesso a amigos que usam esse aplicativo, acho que não temos como fazer com que os desenvolvedores nos paguem, além de oferecer pagamentos e anúncios na rede.”¹¹²

99. No ano seguinte, a nova abordagem do Facebook, que acompanhou o lançamento da Neko no mundo da publicidade móvel, estava claramente dando frutos. Uma troca de e-mail em 20 de junho de 2013 de Sam Lessin para Deborah Lin, com cópia para Mike Vernal e Douglas Purdy, mostra o rápido crescimento das receitas de publicidade com a Neko: “O crescimento nekkko [sic.] é simplesmente incrível. Está superando completamente minhas expectativas com o que é possível para aumentar os produtos pagos”.¹¹³

100. Até o outono de 2013, pelo menos, o vínculo entre receita substancial dos clientes do Facebook para obter acesso preferencial aos dados pessoais foi estabelecido de forma muito rígida. A mensagem interna abaixo, do Facebook, de Konstantinos Papamiltiadis para Ime Archibong, em 18 de setembro de 2013, discutiu slides preparados para uma apresentação com 'DevOps' no dia seguinte, destacando a necessidade de os desenvolvedores de aplicativos gastarem US\$ 250.000 por ano para manter o acesso aos seus dados atuais do Facebook: "Pontos chave: 1/ Descobrir quais outros aplicativos, como o Refresh, não queremos compartilhar dados e descobrir se eles gastam no NEKO. Comunicar de uma só vez a todos os aplicativos que não gastam que essa permissão será revogada. Comunicar ao restante

¹¹⁰ [Anexo 170](#)

¹¹¹ Aqui com acréscimo de destaque.

¹¹² [Anexo 38](#)

¹¹³ [Anexo 158](#)

que eles precisam gastar em US\$ 250 mil por ano para manter o acesso aos dados”.¹¹⁴

101. Os documentos do Six4Three também mostram que o Facebook não apenas considerou receber pagamento em dinheiro como condição para conceder acesso preferencial, mas também receber bens dos desenvolvedores de aplicativos, como nomes comerciais. Por exemplo, o termo 'Moments' já estava registrado pelo Tinder. Este e-mail de 11 de março de 2015 destaca uma discussão sobre como conceder acesso à lista de permissões para o Tinder a APIs restritas em troca do Facebook usando o termo 'Moments':

Não tinha certeza de que não havia uma questão sobre compensação, peço desculpas; em minha mente, trabalhamos em colaboração com Sean e com a equipe de boa-fé nos últimos 16 meses. Ele é membro de um grupo confiável de consultores da nossa plataforma (Developer Advisory Board) e, com base no nosso compromisso de fornecer uma experiência excelente e segura para os usuários do Tinder, desenvolvemos dois novos APIs que permitem efetivamente ao Tinder manter a paridade do produto no novo mundo de API".¹¹⁵

Outro email de Konstantinos Papamiliadis para o Tinder, enviado no dia seguinte, afirma: "Trabalhamos com o Sean e sua equipe sob o espírito de parceria o tempo todo, agregando valor que acreditamos ser muito maior que esta marca registrada". O Facebook lançou um aplicativo de compartilhamento de fotos com o nome de 'Moments' em junho de 2015.¹¹⁶

102. Sob o tema 'direcionamento da concorrência do Facebook', ao final deste capítulo, discutimos outros exemplos do uso da sua posição pelo Facebook no mundo das redes sociais para aprimorar seu domínio, e os problemas que isso representa para o público, para o mercado e para os reguladores.

Compartilhamento de dados do Facebook com desenvolvedores

103. 'Reciprocidade de dados' é a troca de dados entre o Facebook e os aplicativos para que, em seguida, permita que os usuários dos aplicativos compartilhem seus dados com o Facebook. Como Ashkan Soltani nos disse, o modelo de negócios do Facebook é "capitalizar com dados",¹¹⁷ um modelo que evoluiu para o pagamento pelo Facebook a desenvolvedores de aplicativos pela criação de aplicativos, usando as informações pessoais dos usuários do Facebook. Para Soltani, o Facebook estava e ainda está passando a seguinte mensagem: “Desenvolvedores, por favor, passem suas muitas horas de engenharia em troca de acesso aos dados do usuário”¹¹⁸

104. A reciprocidade de dados entre o Facebook e os desenvolvedores de aplicativos foi um recurso central nas discussões sobre o relançamento da sua plataforma. A troca de emails abaixo, de 30 de outubro de 2012, destaca esse problema:

Mike Vernal: Sobre a reciprocidade de dados — na prática, acho que esse será um desses direitos que reservamos. [...] Prestaremos mais atenção nos parceiros estratégicos, para garantir que a troca de valor seja recíproca.

Greg Schechter: Parece que a Reciprocidade de Dados exigirá um novo nível de avaliação subjetiva dos aplicativos que a equipe de operações da plataforma precisará avançar —

¹¹⁴ [Anexo 79](#)

¹¹⁵ [Anexo 97](#)

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

¹¹⁷ [Q4358](#)

¹¹⁸ [Q4327](#)

avaliando se os importadores de ação/UI de reciprocidade são suficientemente recíprocos.'

Mike Vernal: Como muitos de vocês sabem, mantemos uma série de conversas com Mark há meses sobre o Modelo de Negócio da Plataforma. [.]

Vamos exigir que todos os parceiros da plataforma concordem com a reciprocidade de dados. Se você acessar determinado tipo de dados (por exemplo, ouvir músicas), deverá permitir que o usuário publique novamente o mesmo tipo de dados. Os usuários devem poder ativá-lo facilmente tanto no seu próprio aplicativo quanto no Facebook (via importadores de ações).¹¹⁹

105. Mark Zuckerberg escreveu um longo e-mail intitulado “Nada de Modelo de Plataforma”, enviado em 19 de novembro de 2012, para os executivos seniores Sheryl Sandberg, Mark Vernal, Douglas Purdy, Javier Olivan, Alex Schultz, Ed Baker, Chris Cox e Mike Schroepfer (que depuseram ao Comitê DCMS em abril de 2018), Dan Rose, Chris Daniels, David Ebersman, Vladimir Fedrov, Cory Ondrejka e Greg Badros. Ele discute o conceito de reciprocidade e valor dos dados e também se refere a "retirar amigos de outros aplicativos de friends.get", priorizando assim o acesso do desenvolvedor aos dados dos usuários que não concederam permissão de dados ao desenvolvedor:

Depois de pensar muito nos negócios de plataforma, eu queria enviar uma nota explicando em que estou me baseando. Isso não é definitivo e teremos a chance de discutir isso pessoalmente antes de decidirmos com certeza, mas, como é um processo complexo, gostaria de escrever o que estou pensando. Será uma mensagem longa, mas espero que útil.

Em resumo, que acho que devemos ter total reciprocidade e acesso a amigos de aplicativos sem nenhum custo. Reciprocidade total significa que os aplicativos são obrigados a fornecer a qualquer usuário que se conecte ao FB uma opção importante para compartilhar todo o seu conteúdo social dentro desse serviço de volta [...] ao Facebook.

[...]

Estamos tentando permitir que as pessoas compartilhem tudo o que querem e façam no Facebook. Às vezes, a melhor maneira de permitir que as pessoas compartilhem algo é fazer com que um desenvolvedor construa um aplicativo ou rede para fins especiais para esse tipo de conteúdo e torne esse aplicativo social ao ter o Facebook conectado. **Muito embora isso possa ser bom para o mundo, não é bom para nós, a menos que as pessoas também compartilhem no Facebook e que o conteúdo aumente o valor da nossa rede.** ¹²⁰ Então, em última análise, acho que o objetivo da plataforma — mesmo a leitura — é aumentar o compartilhamento em torno do Facebook.'

[...]

Parece que precisamos de uma maneira de mudar rapidamente de aplicativo para o aplicativo FB, para mostrar uma caixa de diálogo do nosso lado, que permite selecionar quais dos seus amigos você deseja convidar para um aplicativo. Precisamos garantir que essa experiência seja realmente possível de criar e tornar a melhor qualidade que queremos, especialmente no iOS, onde estamos mais restritos. Também precisamos descobrir como vamos cobrar por isso. **Quero garantir que isso esteja explicitamente vinculado a tirar amigos que não são de aplicativos de friends.get '.** ¹²¹(informação de amigos)

¹¹⁹ [Anexo 45](#)

¹²⁰ Aqui com acréscimo de destaque.

¹²¹ Aqui com acréscimo de destaque.

[...]

Estou supondo que teremos alguns limites básicos de uso do API e, quando você ultrapassar um limite, precisará nos pagar uma quantia fixa para chegar ao próximo limite ou a taxa será limitada no limite inferior.

[...]

No geral, eu me sinto bem com essa direção. O objetivo da plataforma é unir o universo de todos os aplicativos sociais, para que possamos permitir muito mais compartilhamento e ainda permanecer como centro social central. **Acho que isso encontra o equilíbrio certo entre onipresença, reciprocidade e lucro.**¹²² Em 19 de novembro de 2012, Sheryl Sandberg respondeu a este e-mail de Mark Zuckerberg, afirmando: "Gosto da ideia de reciprocidade total, e esse é o coração do porquê".¹²³

106. O uso da 'reciprocidade' destaca as perspectivas e o modelo de negócios do Facebook. Os acordos de 'reciprocidade' com certos aplicativos permitiram ao Facebook obter o máximo de informações possível, exigindo que os aplicativos que usassem dados do Facebook permitissem que seus usuários compartilhassem seus dados no Facebook (com pouca atenção à privacidade dos usuários). Os interesses comerciais do Facebook basearam-se e ainda se baseiam no equilíbrio das necessidades dos desenvolvedores de trabalhar com o Facebook, dando-lhes acesso aos dados dos usuários, enquanto supostamente protegem a privacidade dos usuários. Ao fazer login em um aplicativo como o Tinder, por exemplo, o usuário não teria percebido que estava dando todas as suas informações no Facebook. O interesse comercial do Facebook é reunir o máximo de informações possível dos usuários, diretamente e dos desenvolvedores de aplicativos na Plataforma.

A coleta de dados pelo Facebook de clientes Android

107. Paul-Olivier Dehaye e Christopher Wylie descreveram a maneira como o aplicativo do Facebook coleta os dados dos usuários de outros aplicativos em telefones Android.¹²⁴ De fato, o Facebook era um dos milhões de aplicativos Android com potencial acesso às chamadas e mensagens dos usuários no sistema operacional Android, que remonta a 2008.¹²⁵ Os documentos da Six4Three revelam discussões sobre como o Facebook pode obter essas informações. O Facebook sabia da controvérsia envolvendo as mudanças em suas políticas no sistema de telefonia móvel Android, que permitiam ao aplicativo do Facebook coletar um registro de chamadas e textos enviados pelo usuário. Para atenuar qualquer repercussão pública ruim, o Facebook planejava dificultar ao máximo para os usuários saberem que esse era um dos recursos subjacentes à atualização do aplicativo.

108. A troca de e-mails abaixo, enviada em 4 de fevereiro de 2015, de Michael LeBeau para colegas, destaca a alteração das permissões de 'ler registro de chamadas' no Android e a desconsideração da privacidade dos usuários:

Michael LeBeau - 'Olá pessoal, como vocês sabem, toda a equipe de crescimento planeja enviar uma atualização de permissões no Android no final deste mês. Eles incluirão a permissão 'ler registro de chamadas', que acionará a caixa de diálogo de permissões do Android na

¹²² [Anexo 48](#) (com acréscimo de destaque).

¹²³ [Anexo 48](#)

¹²⁴ [Q1396](#)

¹²⁵ Em outubro de 2017, havia 3,3 milhões de aplicativos, statistica.com.

atualização, exigindo que os usuários aceitem a atualização. Eles fornecerão uma opção no aplicativo no NUX para um recurso que permite fazer upload contínuo do seu SMS e histórico de chamadas no Facebook para serem usados para melhorar recursos como PYMK, cálculo de coeficiente, classificação de feeds etc. **Existe um alto risco nisso, do ponto de vista de relações públicas, mas parece que a equipe de crescimento cobrará antecipadamente e fará isso.**¹²⁶

109. Em 25 de março de 2018, o Facebook emitiu uma declaração sobre o registro do histórico de chamadas e texto dos usuários, sem a permissão deles:

O registro de chamadas e histórico de texto faz parte de um recurso de inscrição para pessoas que usam o Messenger ou o Facebook Lite no Android. Isso ajuda você a encontrar e se manter conectado com as pessoas de quem gosta e oferece uma melhor experiência no Facebook. [...] Os importadores de contato são bastante comuns entre aplicativos e serviços sociais, como uma forma de encontrar mais facilmente as pessoas com quem você deseja se conectar.¹²⁷

Essa rotação positiva no registro de dados das pessoas pode ter sido precisa, mas não destacou a enorme vantagem financeira do Facebook realizar uma coleta extensiva de dados das interações diárias dos seus usuários.

Monitoramento pelo Facebook do uso de aplicativos

110. Onavo era uma empresa israelense que construiu um aplicativo VPN, que poderia ocultar os endereços IP dos usuários para que terceiros não pudessem rastrear os sites ou aplicativos usados. O Facebook comprou a Onavo em 2013, anunciando para os clientes que o objetivo era “manter você e seus dados em segurança quando estiver online, bloqueando sites potencialmente prejudiciais e protegendo suas informações pessoais”.¹²⁸ No entanto, o Facebook usou a Onavo para coletar dados de uso de aplicativos dos seus clientes para avaliar não apenas quantas pessoas haviam baixado aplicativos, mas com que frequência eles os utilizavam. Esse fato foi incluído no botão 'Leia Mais', na descrição da App Store da Onavo: “A Onavo coleta seu tráfego de dados móveis [...] Como fazemos parte do Facebook, também usamos essas informações para melhorar os produtos e serviços do Facebook, **obter informações sobre os produtos e serviços que as pessoas valorizam e criar melhores experiências**”.¹²⁹

111. Esse conhecimento os ajudou a decidir quais empresas estavam com bom desempenho e, portanto, forneceu dados inestimáveis sobre possíveis concorrentes. Eles poderiam então adquirir essas empresas ou encerrar aquelas que consideravam uma ameaça. O Facebook adquiriu e usou esse aplicativo, dando a impressão de que os usuários tinham maior privacidade, quando na verdade ele estava sendo usado pelo Facebook para espioná-los.¹³⁰

112. Os slides a seguir são de uma apresentação, intitulada “Industry Update”, realizada em 26 de abril de 2013, mostrando a análise de mercado conduzida pelos dados da Onavo, comparando dados sobre aplicativos nos telefones dos usuários e minerando esses dados para analisar os concorrentes do

¹²⁶ Nota de rodapé necessária (aqui com acréscimo de destaque).

¹²⁷ [Anexo 172](#)

¹²⁸ Informações promocionais da Onavo.

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 (com acréscimo de destaque)

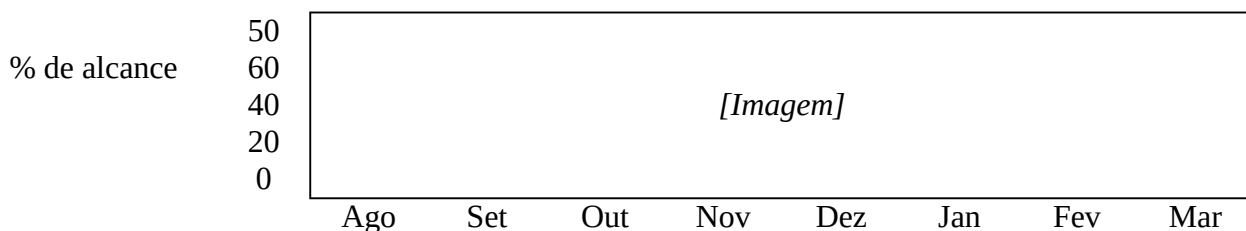
¹³⁰ [Apple removed Facebook's Onavo from the App Store for gathering app data](#), Taylor Hatmaker Techcrunch.com, 22 August 2018.

Facebook.

113. O slide a seguir ilustra as estatísticas coletadas de diferentes aplicativos populares, como Vine, Twitter, Path e Tumblr:

Alcance de Aplicativos para iPhone nos EUA, agosto de 2012 - março 2013 (fonte: Onavo)

Facebook
Instagram -----
Twitter - - -
FB Messenger -----
Snapchat -----



	<u>% de alcance,</u>		<u>Classificação</u>	
	<u>Março</u>			
Facebook	72,6%	+0.6	1	-
Instagram	34,0%	+1.7	3	-
Twitter	27.2%	+0.1	6	
FB Msgr	13,7%	+0.2	15	-
Snapchat	13,2%	+1.6	16	+4
Pirterest	11,3%	+0.2	20	+1
WnatsApp	8,6%	+0,3	30	-
Tumblr	6,9%	+0,4	43	+3
Foursquare	5,0%	+0.2	57	+1
Vine	3,9%	+1,2	71	+25
Google*	2,9%	-0,2	07	-4
Path	1,0%	+0,1	243	+22

Fonte: Onavo
FB - 01367813

ALTAMENTE CONFIDENCIAL

Apresentação do Facebook “Industry Update”, realizada em 26 de abril de 2013

114. Em agosto de 2018, a Apple descobriu que o Facebook violou seus termos e condições e removeu a Onavo da App Store, afirmando:

Trabalhamos duro para proteger a privacidade do usuário e a segurança dos dados em todo o ecossistema da Apple. Com a atualização mais recente de nossas diretrizes, deixamos explicitamente claro que os aplicativos não devem coletar informações sobre quais outros aplicativos estão instalados no dispositivo do usuário para fins de análise ou publicidade/marketing e devem deixar claro quais dados do usuário serão coletados e como será usado.¹³¹

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

115. Desde 2016, o Facebook adotou práticas semelhantes em relação ao seu aplicativo 'Facebook Research', que violava as regras da Apple em torno da distribuição interna de aplicativos dentro de uma organização. O Facebook paga secretamente para usuários, com idades entre 13 e 25 anos, até US\$ 20 em cartões-presente por mês para vender suas atividades por telefone e em websites, instalando o aplicativo 'Facebook Research' do Android. A Apple bloqueou o aplicativo de pesquisa do Facebook em janeiro de 2019, quando percebeu que o Facebook violara os termos e condições da Apple. No entanto, o aplicativo continuará a ser executado no Android.¹³² Um porta-voz da Apple afirmou:

O Facebook está usando as suas contas para distribuir um aplicativo de coleta de dados aos consumidores, o que é uma clara violação do contrato com a Apple.

Qualquer desenvolvedor que use seus certificados corporativos para distribuir aplicativos aos consumidores terá seus certificados revogados, o que fizemos neste caso para proteger nossos usuários e seus dados.¹³³

¹³² [Facebook pays teens to install VPM that spied on them, Josh Constine](#), Technocrunch.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.

Investida do Facebook contra aplicativos concorrentes

116. Desde o início, o Facebook fez várias aquisições, incluindo o Instagram em 2012, e o WhatsApp em 2014. Os arquivos da Six4Three mostram evidências de que o Facebook assume posições agressivas contra certos aplicativos, especialmente contra concorrentes diretos, o que resultou na negação de acesso a dados. De modo inevitável, essa conduta levou ao fracasso desses negócios, incluindo a Six4Three. Um email, enviado em 24 de janeiro de 2013, de Justin Osofsky para Mike Vernal, Mark Zuckerberg, Kevin Systrom, Douglas Purdy e Dan Rose, descreve a investida contra o Vine do Twitter, um concorrente direto do Instagram, desativando o uso de API de amigos do Facebook:

Justin Osofsky - O **Twitter lançou o Vine hoje**, que permite gravar vários segmentos curtos de vídeo para criar um único vídeo de 6 segundos. Como parte do NUX deles, ¹³⁴ você pode encontrar amigos via FB. A menos que alguém levante objeções, encerraremos o acesso ao API de amigos hoje. Preparamos um anúncio público reativo e vou informar a Jana sobre a nossa decisão.

MZ - **Sim, vamos lá.** ¹³⁵

117. Instagram Video, também criado em 2013, permitiu que os usuários enviassem vídeos de 15 segundos ao seu perfil. A partir da troca de e-mails acima, fica claro que Mark Zuckerberg aprovou pessoalmente a decisão de negar o acesso aos dados para o Vine. Em outubro de 2016, o Vine anunciou que o Twitter interromperia o aplicativo móvel Vine, em parte devido ao fato de eles não conseguirem aumentar sua base de usuários. ¹³⁶ No mesmo dia em que publicamos os documentos da Six4Three em dezembro de 2018, o co-fundador da Vine, Rus Yusupov, tuitou "lembro-me daquele dia como se fosse ontem". ¹³⁷

Resposta do Facebook à publicação dos documentos Six4Three

118. Publicamos uma pequena parcela das evidências obtidas no processo da Six4Three. Por mais de um ano, em várias ocasiões, Mark Zuckerberg se recusou a depor ao Comitê DCMS. No entanto, quatro horas depois da publicação das provas da Six4Three no site do Comitê DCMS, ele respondeu, com o seguinte post em sua página no Facebook:

Nesta semana, um comitê do Parlamento Britânico publicou alguns e-mails internos do Facebook, que incluem principalmente discussões internas que levaram a alterações que fizemos em nossa plataforma de desenvolvedores para desligar aplicativos abusivos em 2014-15. Como esses e-mails eram apenas parte das nossas discussões, quero compartilhar um pouco mais de contexto sobre as decisões que foram tomadas.

Lançamos a plataforma Facebook em 2007 com a ideia de que que mais aplicativos deveriam ser sociais. Por exemplo, seu calendário deve mostrar os aniversários dos seus amigos e seu catálogo de endereços deve ter as fotos dos seus amigos. Muitas novas empresas e grandes experiências foram criadas nessa plataforma, mas, ao mesmo tempo, alguns desenvolvedores criaram aplicativos obscuros que abusavam dos dados das pessoas.

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

¹³⁵ [Anexo 44](#) (aqui, com acréscimo de destaque).

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

¹³⁷ Mesma referência acima.

Em 2014, para evitar aplicativos abusivos, anunciamos que estávamos alterando toda a plataforma para limitar drasticamente os dados que os aplicativos poderiam acessar.

Essa mudança significou que muitos aplicativos obscuros — como o aplicativo de questionário que vendia dados para a Cambridge Analytica — não podiam mais operar em nossa plataforma. Alguns dos desenvolvedores cujos aplicativos obscuros foram lançados em nossa plataforma nos processaram para reverter a mudança e dar a eles mais acesso aos dados das pessoas. Estamos confiantes de que essa mudança foi a coisa certa a fazer e que venceremos esses processos.¹³⁸

119. Os "aplicativos obscuros" aos quais Zuckerberg se referia - 'o aplicativo de questionário que vendia dados para a Cambridge Analytica' — era o aplicativo 'thisisyourdigitallife', de propriedade da GSR, que nos leva de volta ao ponto inicial das nossas investigações sobre os métodos e práticas empresariais do Facebook.

120. Um dos co-fundadores da GSR foi Joseph Chancellor, que estava empregado, até recentemente, no Facebook, como pesquisador quantitativo da equipe de Pesquisa da Experiência do Usuário, apenas dois meses após deixar a GSR. O Facebook não forneceu nenhuma explicação para o recrutamento de Joseph Chancellor, depois de o Facebook anunciar a ocorrência de um sério descumprimento dos seus termos e condições. Acreditamos que a verdade está contida no depoimento de Aleksandr Kogan, co-fundador juntamente com Joseph Chancellor.

121. Quando perguntaram a Richard Allan por que Joseph Chancellor trabalhava no Facebook, ele respondeu que "Joseph Chancellor, pelo que entendi, é alguém que teve um histórico acadêmico trabalhando em áreas relevantes". Ele reconheceu que Joseph Chancellor estava envolvido com a origem dos abusos cometidos pela Cambridge Analytica e que o Facebook não havia tomado nenhuma medida contra ele.¹³⁹

122. Quando Aleksandr Kogan depôs no Comitê DCMS em abril de 2018, foi perguntado por que Joseph Chancellor havia sido contratado pelo Facebook, dadas as circunstâncias do seu envolvimento com o GSR. Quanto a parecer estranho, o Dr. Kogan respondeu: "A razão pela qual não acho estranho é porque, na minha opinião, os comentários do Facebook parecem ter sido divulgados num modo de contenção de crise de relações públicas. Não acredito que eles realmente pensem nessas coisas, porque acho que eles percebem que a plataforma foi fragilizada por mais de um lado, por milhares de outras pessoas".¹⁴⁰

123. A interpretação do Dr. Aleksandr Kogan sobre o que aconteceu parece se basear nas provas da Six4Three. O Facebook estava desrespeitando a privacidade dos usuários porque, desde o início, sua plataforma havia sido projetada dessa maneira. O Facebook promoveu uma tensão entre o acesso do desenvolvedor aos dados e a privacidade do usuário; ele projetou sua plataforma para aplicar configurações de privacidade apenas aos aplicativos do Facebook, mas aplicou configurações diferentes e variáveis aos dados transmitidos pelas APIs da plataforma. Por exemplo, uma troca de e-mail entre Papamiltiadis e seus colegas revela que mais de 40.000 aplicativos que solicitaram acesso por APIs foram classificados levando-se em conta: aqueles que podem causar uma repercussão pública negativa; aqueles que oferecem valor estratégico, agregando valor ao Facebook; e aqueles que são competitivos, gerando pouco valor para o Facebook; e aqueles que causarão problemas para a empresa.

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

¹³⁹ [Qs 4144-4149](#)

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

Lessin disse que todos os aplicativos de estilo de vida devem ter seu acesso removido "porque, em última análise, somos concorrentes de todos eles".¹⁴¹

124. Outro documento fornecido ao comitê pela Six4Three mostra preocupações levantadas pela equipe do Facebook em 2011 sobre os aplicativos serem removidos da plataforma, que não eram necessariamente 'spam' ou 'superficial', para usar a terminologia utilizada pelo Mark Zuckerberg. Em um email interno, Mike Vernal, do Facebook, escreveu: “É muito, muito ruim quando desabilitamos um aplicativo legítimo. Isso compromete a confiança na plataforma, porque faz com que os desenvolvedores pensem que todo o seu negócio pode desaparecer a qualquer momento.”¹⁴² Essa é realmente a queixa que os desenvolvedores tentaram encaminhar ao Facebook, e está no centro da denúncia da Six4Three contra a empresa.

125. O Facebook se esconde continuamente atrás da ofuscação. Os documentos sigilosos continham e-mails internos, revelando o fato de que o lucro do Facebook vem antes de qualquer outra coisa. Quando expostos, o Facebook “sempre se arrepende, está sempre numa jornada de melhoria”, como Charlie Angus, MP (vice-presidente do Comitê Permanente Canadense de Acesso à Informação, Privacidade e Ética e membro do 'Comitê Internacional ') os descreveu.¹⁴³ O Facebook continua a priorizar o lucro em vez da segurança dos dados, assumindo riscos para priorizar seu objetivo de ganhar dinheiro com os dados do usuário.

Modelo de negócios do Facebook e novos desafios para reguladores

126. O Facebook completou 15 anos recentemente, o que faz dele uma empresa relativamente jovem. O que começou como uma maneira aparentemente inócua de compartilhar informações com amigos e familiares se transformou num fenômeno global, influenciando eventos políticos. Theresa Hong, membro da campanha eleitoral digital de Trump, descreveu o 'Projeto Alamo', que envolveu funcionários que trabalhavam para o então candidato presidencial Donald Trump, funcionários da Cambridge Analytica e funcionários do Facebook, trabalhando juntos com os conjuntos de dados da Cambridge Analytica, visando estados específicos e eleitores específicos. O projeto investiu US\$ 85 milhões em anúncios no Facebook, e Hong disse que "sem o Facebook, não teríamos vencido".¹⁴⁴

127. O Facebook cresceu exponencialmente, comprando concorrentes como WhatsApp e Instagram. Como Charlie Angus disse a Richard Allan: “O Facebook quebrou tanto a confiança que foi depositada nele que permitir que ele simplesmente devore todas as formas de concorrência provavelmente não é do interesse público. [...] O problema é o controle econômico sem precedentes de todas as formas de discurso e comunicação social pelo Facebook”.¹⁴⁵

128. Ao se mostrar um serviço gratuito, o Facebook conta apenas metade da história. Como Ashkan Soltani, ex-Chefe de Tecnologia da Comissão Federal de Comércio dos Estados Unidos da América, nos disse:

Ou é gratuito — existe uma troca de informações não monetárias — ou é uma troca pelas informações pessoais que são fornecidas à plataforma, extraídas e depois revendidas ou reutilizadas por desenvolvedores independentes para desenvolver aplicativos, ou revendido aos anunciantes para anunciar.¹⁴⁶

¹⁴¹ [Anexo 75](#)

¹⁴² [Anexo 19](#).

¹⁴³ [Q4131](#)

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

¹⁴⁵ [Q4273](#)

¹⁴⁶ [Q4370](#)

129. Os documentos que recebemos destacaram o fato de que o Facebook queria maximizar as receitas a todo custo e, ao fazê-lo, favoreceram os desenvolvedores de aplicativos que estavam dispostos a pagar muito dinheiro por anúncios e direcionaram os aplicativos que representavam uma concorrência futura direta ou potencial — e em alguns casos bem conhecidos os adquiriu.

130. Fica claro que o comportamento do Facebook apresenta desafios para dos órgãos de defesa da concorrência. Numa iniciativa conjunta do Tesouro e do Departamento de Negócios, Energia e Estratégia Industrial (BEIS), um grupo de especialistas, presidido pelo professor Jason Furman, foi reunido para considerar as oportunidades e desafios potenciais que a economia digital pode representar para a política de concorrência e pró-concorrência, e fazer recomendações sobre as alterações necessárias. O período de consulta terminou no início de dezembro de 2018 e o painel deve apresentar um relatório no início de 2019. Esperamos que esse relatório contemple também as provas que nós obtivemos.

131. Desde a publicação de uma seleção dos documentos do caso Six4Three, eles estão claramente disponíveis para os reguladores, incluindo o Comissão de Informação do Reino Unido e a Comissão Federal de Comércio dos EUA, para auxiliar na condução dos seus trabalhos. Em março de 2018, após as revelações sobre a Cambridge Analytica, a FTC disse que estava lançando uma investigação adicional sobre as práticas de dados do Facebook, cujo resultado ainda está sendo aguardado — incluindo a possibilidade de multas substanciais.

132. Quando perguntado se seria justo considerar que o Facebook é culpado por descumprir a Lei de Chantagem Civil, de Influência e de Organizações Corruptas dos Estados Unidos, na sua conspiração para prejudicar outros negócios, Richard Allan discordou. Ele descreveu a empresa como “um grupo de pessoas com quem eu tenho trabalhado de modo muito próximo por muitos anos, que desejam construir um negócio de sucesso”.¹⁴⁷ Recebemos as provas que comprovam que o Facebook não apenas segmentava os desenvolvedores para aumentar a receita, mas também buscava desativar os aplicativos dos que eram considerados concorrentes ou aqueles que operavam em áreas lucrativas da sua plataforma e vulneráveis a aquisição. Desde 1970, os EUA possuem uma legislação federal de alta envergadura, a Lei de Chantagem Civil, de Influência e de Organizações Corruptas (chamada de RICO); e muitos estados também aprovaram alguma lei com dispositivos similares depois disso. Originalmente destinada a combater organizações do crime organizado, também tem sido usada em casos comerciais, com dispositivos utilizados para ação civil por danos no caso de infrações abrangidas pela RICO.

133. Acreditamos que a resposta de Mark Zuckerberg à publicação das provas da Six4Three foi, para utilizar a mesma expressão do Dr. Kogan, num “modo de contenção de crise de relações públicas”. Não é que Facebook estava agindo contra aplicativos “obscuros” ou “abusivos”, sendo que nenhuma evidência foi produzida nesse sentido. De fato, o trabalho com esses aplicativos se tornou uma parte indissociável do seu modelo de negócios. Isso explica por que recrutou as pessoas que os criaram, como Joseph Chancellor. As ações do Facebook de modo algum respaldam as declarações de Mark Zuckerberg que, acreditamos, entrou no “modo de contenção de crise de relações públicas”, diante da exposição do seu verdadeiro modelo de negócios. Este é apenas um exemplo de má-fé. Diante de um cenário assim, defendemos ser justificável que os governos limitem o campo de atuação de empresas como o Facebook. Parece evidente que o Facebook atua apenas quando se tornam públicas as infrações graves que foram cometidas. Foi o que ocorreu em 2015 e 2018.

¹⁴⁷ [Q4213](#)

134. Apesar de intimações específicas, o Facebook não nos forneceu qualquer exemplo de empresa que tenha sido excluída da sua plataforma devido a sérias infrações envolvendo dados. Acreditamos que essa medida só chega a ser implementada quando as infrações se tornam públicas. Consideramos que captação sobre transferência de dados é o modelo de negócios do Facebook, e que a afirmação de Mark Zuckerberg de que "nunca vendemos os dados de ninguém" é simplesmente falsa.

135. As evidências que obtivemos dos documentos judiciais da Six4Three indicam que o Facebook estava disposto a substituir as configurações de privacidade dos seus usuários para transferir dados para alguns desenvolvedores de aplicativos, cobrar preços altos de publicidade de alguns desenvolvedores, pelo compartilhamento desses dados e privar alguns desenvolvedores — como a Six4Three — desses dados, fazendo com que eles interrompam suas atividades. Parece claro que o Facebook descumpriu, pelo menos, o seu acordo celebrado com a Comissão Federal de Comércio.

136. O Comissário de Informação disse ao Comitê que o Facebook precisa mudar significativamente seu modelo de negócios e suas práticas para manter a confiança. A partir dos documentos que recebemos da Six4Three, é evidente que o Facebook descumpriu, de forma deliberada e consciente, as leis de privacidade de dados e de defesa da concorrência. O ICO deve realizar uma investigação detalhada sobre as práticas da Plataforma Facebook, seu uso de dados de usuários e amigos de usuários e o uso da 'reciprocidade' no compartilhamento de dados.

137. A Irlanda é a principal autoridade para o Facebook, sob a GDPR, e esperamos que esses documentos representem provas úteis para Helen Dixon, a Comissária Irlandesa de Proteção de Dados, em suas investigações em curso sobre a maneira pela qual o Facebook direcionou, monitorou e capitalizou sobre seus usuários.

138. Em nosso Relatório Preliminar, declaramos que o domínio de algumas empresas poderosas de tecnologia as levou a se comportarem como se fossem monopólios em sua área específica, e que existem contrapartida pelos dados sobre os quais esses serviços se baseiam. O Facebook, em particular, não está disposto a prestar contas aos reguladores de todo o mundo. O governo deve considerar o impacto de tais monopólios no mundo político e na democracia.

139. A Autoridade de Mercado e Defesa da Concorrência (CMA) deve realizar uma auditoria abrangente sobre a operação do mercado de publicidade nas redes sociais. O Comitê apresentou esta recomendação no seu Relatório Preliminar, e felizmente essa recomendação também foi apoiada pelo Relatório Cairncross, realizado de forma independente a pedido do governo e publicado em fevereiro de 2019. Dado o conteúdo dos documentos da Six4Three que publicamos, também deveria investigar se o Facebook esteve especificamente envolvido em alguma prática anticompetitiva e conduzir uma verificação das práticas de negócios do Facebook com relação a outros desenvolvedores, para decidir se o Facebook está usando injustamente sua posição dominante no mercado das redes sociais para determinar quais empresas devem prosperar ou fracassar. Esperamos que o governo inclua essas considerações ao verificar os poderes de concorrência do Reino Unido em abril de 2019, como declarado na resposta do governo ao nosso Relatório Preliminar. Empresas como o Facebook não devem se comportar como 'gangsters digitais' no mundo on-line, como se estivessem fora do alcance da lei.

Leave.EU e dados da Eldon Insurance supostamente usados por campanhas

140. Nosso Relatório Preliminar destacou os métodos utilizados na campanha de Arron Banks durante o Referendo. Em suas próprias palavras, envolveu a criação de "incêndios" e, em seguida, "ligar um

grande ventilador e fazer com que o vento soprasse".¹⁴⁸ Ele descreveu a questão da imigração como um ponto capaz de provocar um "incêndio incontrollável".¹⁴⁹ As provas recebidas indicam que os dados foram compartilhados entre a campanha Leave.EU — com sua linha direta de 'deixar a UE fora do Reino Unido'¹⁵⁰ — e a companhia de seguros da Arron Banks, Eldon Insurance Ltd.¹⁵¹ Quando perguntamos para Arron Banks se os funcionários da Eldon Insurance também trabalharam na campanha do movimento Leave.EU, ele respondeu que essa alegação era "simplesmente mentirosa".¹⁵²

141. A alegação de compartilhamento de dados das pessoas durante uma campanha de referendo é uma questão tanto para o Gabinete do Comissário da Informação (no que se refere ao suposto compartilhamento não autorizado de dados, em violação ao Regulamento de Privacidade e Comunicação Eletrônica de 2003)¹⁵³ quanto para a Comissão Eleitoral (no que se refere a supostas infrações de regras relacionadas a limites de gastos durante um referendo).

142. Desde que publicamos nosso Relatório Preliminar, o ICO publicou as conclusões das suas investigações sobre esses problemas.¹⁵⁴ Seu relatório afirma que o movimento Leave.EU e a Eldon Insurance estão intimamente ligados, com ambas as organizações compartilhando pelo menos três diretores, com compartilhamento de funcionários e projetos.¹⁵⁵ O ICO encontrou provas de que os dados pessoais dos clientes da Eldon Insurance, na forma de endereços de e-mail, eram acessados pela equipe que trabalhou no Leave.EU e eram usados ilegalmente para enviar mensagens políticas de marketing:

- O Leave.EU enviou 1.069.852 mensagens de e-mail aos assinantes que aceitaram receber informações do Leave.EU entre 25 de fevereiro e 31 de julho de 2017, sendo que essas mensagens também incluíram marketing para os serviços GoSkippy e uma oferta de desconto para os apoiadores do Leave.EU, para os quais o Leave.EU não obtiveram autorização; e
- O Leave.EU enviou um único email para mais de 49.000 endereços de email em 23 de agosto de 2016, anunciando um acordo de 'patrocínio' celebrado com o GoSkippy.¹⁵⁶

143. O relatório do ICO destacou seu aviso de intenção de multar as seguintes empresas:

- Leave.EU e Eldon Insurance (pela negociação com o GoSkippy) em £60.000 cada, por infração grave dos Regulamentos de Privacidade e Comunicações Eletrônicas (PECR) de 2003; e
- Leave.EU em £15.000 por outra infração ao regulamento PECR 22, depois que quase 300.000 emails foram enviados aos clientes da Eldon Insurance, contendo o boletim da Leave.EU.¹⁵⁷

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 Referência acima, parágrafo 155.

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

¹⁵⁵ Referência acima, p. 45.

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

¹⁵⁷ Referência acima, p. 9.

144. A Comissária da Informação nos repassou provas, no dia da publicação do seu relatório, e descreveu a “falha em segregar os dados dos clientes de seguros da Eldon e as mensagens de marketing e mensagens para possíveis apoiadores e eleitores, e os dados do Leave.EU. Emitimos notificações, com base no regulamento de marketing eletrônico, considerando também o nosso trabalho no lado da proteção de dados, para examinar profundamente as políticas ou a desconsideração da segregação de dados. Esse ponto ainda será objeto de uma auditoria”.¹⁵⁸ O ICO emitiu notificação de execução preliminar para a Eldon Insurance, exigindo ação imediata para garantir que a empresa cumpra as leis de proteção de dados.¹⁵⁹

145. Em 1 de fevereiro de 2019, depois de considerar as declarações das empresas, o ICO impôs multas, confirmando a mudança de um valor, mantendo inalterado o valor das outras duas (a multa para a campanha de marketing do Leave.EU foi reduzida em £15.000 em relação à notificação original do ICO). O Comissário da Informação também emitiu duas notificações de avaliação para o Leave.EU e a Eldon Insurance, para informar dar ciência de que ambas as organizações serão auditadas.¹⁶⁰

146. Das provas recebidas, que foram respaldadas pelas conclusões do ICO e da Comissão Eleitoral, fica claro que existia uma relação porosa entre a Eldon Insurance e o Leave.EU, com funcionários e dados de uma organização potencializando o trabalho da outra. Não houve um esforço de criar uma divisão estrita entre as duas organizações, descumprindo a legislação vigente. Estamos ansiosos para receber as conclusões das auditorias do ICO sobre as duas organizações.

147. Como estabelecido em nosso Relatório Preliminar, Arron Banks e Andy Wigmore demonstraram total desrespeito e desdém pelo processo parlamentar quando depuseram aqui em junho de 2018. Fica evidente, agora, que eles também apresentaram informações enganosas sobre o trabalho entre a Eldon Insurance e o Leave.EU. Esses indivíduos não demonstraram qualquer compromisso com a verdade.

Aggregate IQ

Introdução

148. Aggregate IQ é uma empresa canadense de desenvolvimento de software e web para publicidade digital, constituída em 2012 por seus proprietários Jeff Silvester e Zack Massingham. Jeff Silvester nos disse que conhecia Christopher Wylie, o denunciante da Cambridge Analytica, desde 2005, e veio a conhecer Alexander Nix, então SCO da Cambridge Analytica, “por volta do início de 2014”.¹⁶¹

149. A AIQ trabalhou para a SCL para “criar uma ferramenta de software de gestão de relacionamento com clientes para fins políticos” para a campanha eleitoral de Trinidad e Tobago em 2014. Em seguida, desenvolveu uma ferramenta de software — chamada de Ripon —, por encomenda e de propriedade da SCL”.¹⁶² De acordo com o ICO, no início de 2014, a SCL Elections buscou a AIQ para “ajudá-la a construir uma nova ferramenta de gestão de relacionamento com clientes para fins políticos (CRM) a ser usada durante as eleições minoritárias dos Estados Unidos de 2014”.¹⁶³ Os arquivos da AIQ contêm

¹⁵⁸ [Q3894](#)

¹⁵⁹ Relatório do ICO, p. 47.

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.

¹⁶¹ [Q2765](#) e [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

uma quantidade considerável do trabalho de desenvolvimento, com grande quantidade de dados pessoais, em texto sem formatação, dos residentes de Trinidad e Tobago.

150. A ferramenta Ripon foi descrita por Jeff Silvester como "uma ferramenta de gestão de relacionamento com clientes para fins políticos com foco no mercado dos Estados Unidos" ¹⁶⁴e foi descrita por Christopher Wylie como "o software que utilizava os algoritmos de dados do Facebook".¹⁶⁵ Como resultado do desenvolvimento da ferramenta Ripon, para que os eleitores pudessem receber anúncios micro-direcionados, a AIQ também trabalhou em campanhas políticas nos EUA.¹⁶⁶ Este trabalho ainda estava em andamento quando eles também se envolveram em campanhas relacionadas ao Brexit no referendo da UE no Reino Unido. Segundo o Facebook, "a AIQ publicou 1.390 anúncios em nome das páginas vinculadas à campanha do referendo entre fevereiro de 2016 e 23 de junho de 2016, inclusive".¹⁶⁷

151. Chris Vickery, diretor da Cyber Risk Research, na consultoria UpGuard, trabalha como investigador de falhas envolvendo dados, localizando dados expostos e encontrando ameaças comuns. Depois das reportagens feitas pelo *The Observer*, *Channel 4* e pelo *New York Times* sobre a Cambridge Analytica (e empresas associadas), a Upguard publicou quatro artigos que explicavam as conexões entre a AIQ, a Cambridge Analytica e a SCL, e o trabalho da AIQ durante o referendo no Reino Unido.¹⁶⁸ Esses documentos foram baseados nos dados que Chris Vickery havia encontrado no site inseguro da AIQ. Em seu depoimento ao Comitê, ele apresentou ¹⁶⁹dados do Gitlab ¹⁷⁰contendo mais de 20.000 pastas e 113.000 arquivos, que ele havia baixado do site inseguro da AIQ.¹⁷¹ O Comitê disponibilizou todo o conjunto de dados ao ICO

152. Chris Vickery descreveu as provas que apresentou no inquérito:

Este conjunto de arquivos contém aplicativos sofisticados, programas de gerenciamento de dados, rastreadores de publicidade e bancos de dados de informações que coletivamente podem ser usados para direcionar e influenciar indivíduos através de uma variedade de métodos, incluindo telefonemas automatizados, e-mails, sites políticos, recrutamento de voluntários e anúncios no Facebook.¹⁷²

153. O gráfico a seguir apresentado como prova por Chris Vickery destaca o relacionamento que a

Parliament, ICO, 6 November 2018.

¹⁶⁴ [Q2776](#)

¹⁶⁵ [Q1299](#)

¹⁶⁶ [Q2784](#). Como dissemos no parágrafo 110 do Relatório Preliminar, em agosto de 2014, o Dr. Kogan trabalhou com a SCL para fornecer dados

sobre eleitores individuais, com o objetivo de apoiar os candidatos norte-americanos promovidos pelo John Bolton Super Pac nas eleições minoritárias de novembro daquele ano. Elaborou perfis psicográficos dos usuários para direcionar anúncios aos eleitores em cinco grupos distintos de personalidade.

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 é uma plataforma online acessada por desenvolvedores para compartilhamento de códigos.

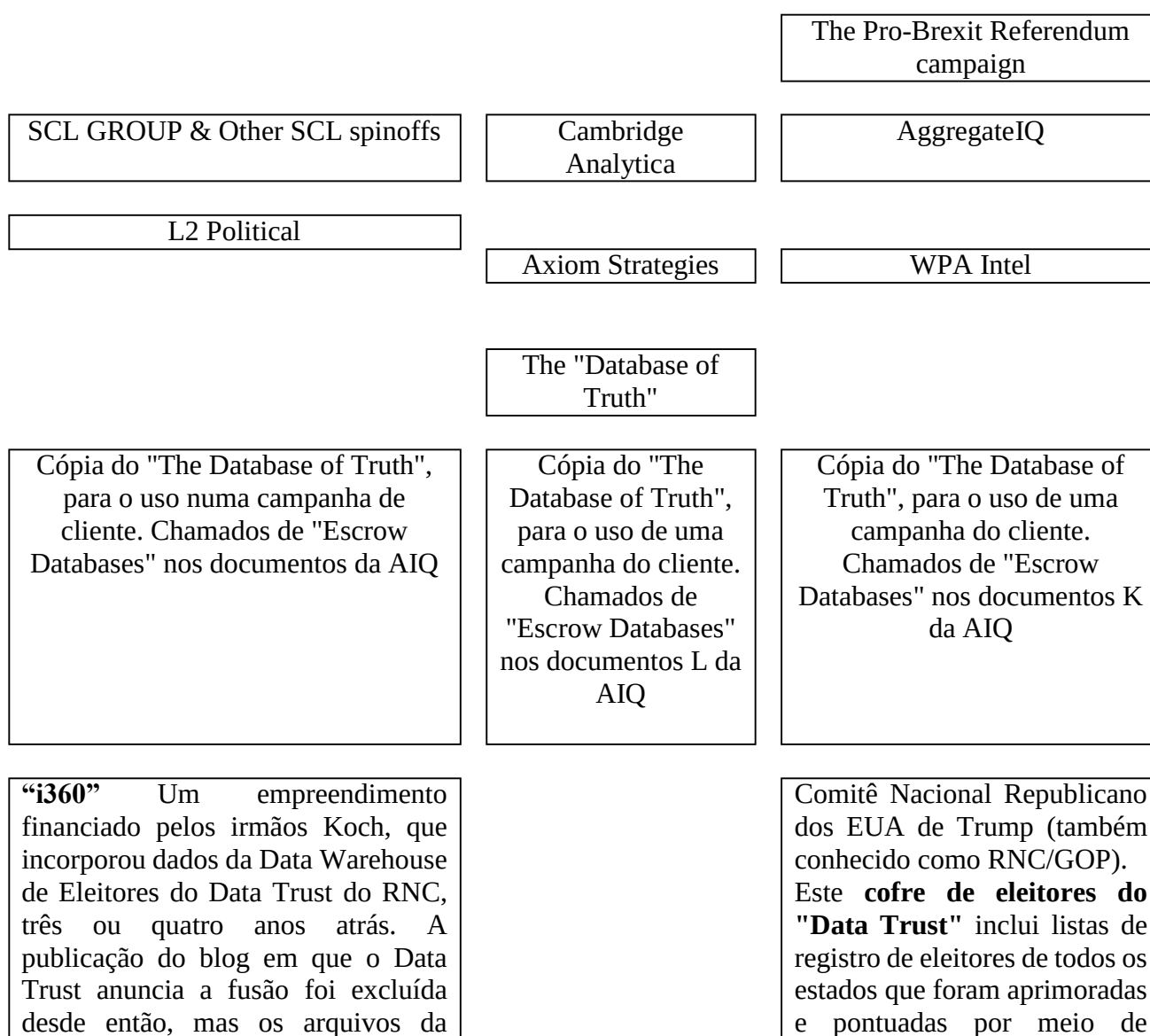
¹⁷¹ [Chris Vickery oral evidence session](#), 2 May 2018.

¹⁷² [The Aggregate IQ Files, Part One: How a political engineering firm exposed their code base](#), 30 April 2018.

AIQ tinha com a Cambridge Analytica, SCL e outros clientes. A lista completa dos projetos atuais nos arquivos da AIQ que envolvem entidades do Reino Unido é:

- “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. De acordo com Chris Vickery, “os 15 nós mostrados abaixo estão embasados por documentos e testemunho fidedigno. Esta não é uma lista exaustiva de todos os gateway de dados e fluxos envolvidos, mas ainda tenho a segurança para declara que é uma descrição razoável do que ocorreu”:¹⁷³



¹⁷³ [FKN0125](#)

Internet ainda a possuem.

análise comportamental
preditiva e modelos avançados
de correlação.

Várias fontes de Deep Root Analytics e Deep Root (por exemplo, Experian e uma variedade de sistemas de classificação de métricas de impacto de publicidade).

Campanha Presidencial
Donald J. Trump

Fonte: Chris Vickery¹⁷⁴

155. Em seu relatório de julho de 2018, o ICO confirmou que a AIQ tinha acesso aos dados pessoais dos eleitores do Reino Unido, repassados pela campanha Vote Leave, e que a AIQ "mantinha dados do Reino Unido que eles não deviam ter mantido".¹⁷⁵ Este capítulo explorará os dados não seguros da AIQ descobertos por Chris Vickery, estudando: o relacionamento entre a AIQ, a SCL e a Cambridge Analytica; o trabalho que a AIQ realizou no referendo da UE; e os recursos abertos contra a AIQ, pelos tipos de ferramentas encontradas nos arquivos. Acionamos a agência de comunicação, 89up,¹⁷⁶ para realizar a análise desses dados e também utilizamos a experiência de Chris Vickery em nosso trabalho.

Relação entre AIQ e SCL/Cambridge Analytica antes do referendo no Reino Unido sobre a UE

156. De acordo com Jeff Silvester, CEO da AggregateIQ, aproximadamente 80% da receita da AIQ veio da SCL, de 2013 até meados de 2015.¹⁷⁷ Parece que nos arquivos de Chris Vickery, em que a AIQ e SCL trabalhavam juntos, a equipe tinha acesso mútuo a certos bancos de dados.¹⁷⁸ Alexander Nix nos disse que “depois que eles construíram a plataforma de software para nós, a AIQ continuou a trabalhar conosco como consultores, principalmente para ajudar alguns dos nossos clientes a interagir com o produto que eles criaram e ensinar-lhes a usá-lo.”¹⁷⁹

157. Em nosso Relatório Preliminar, descrevemos o software Ripon — uma ferramenta de gestão de relacionamento com clientes para fins políticos — desenvolvido pela AIQ, por encomenda e de propriedade da SCL.¹⁸⁰ Os arquivos obtidos por Chris Vickery ilustram uma clara colaboração entre a Cambridge Analytica e a AIQ, com a importação do projeto de desenvolvimento Ripon original de um domínio controlado pela Cambridge Analytica para o repositório da AIQ. O envolvimento da AIQ com o software Ripon veio de um repositório fonte localizado em “scl.ripon.us”. O domínio foi registrado em nome do então CEO da Cambridge Analytica, Alexander Nix. O ICO descobriu transações e contatos financeiros entre as organizações e também concluiu que era uma relação puramente contratual:

Não encontramos evidências de atividade ilegal em relação aos dados pessoais dos cidadãos do Reino Unido e ao trabalho da AIQ com a SCLE. Até o momento, não temos evidências de que a SCLE [SCL Elections] e a CA [Cambridge Analytica] estivessem envolvidos em qualquer

¹⁷⁴ [FKN 0125](#)

¹⁷⁵ [Investigation into data analytics for political purposes: investigation update, ICO, July 2018, p4.](#)

¹⁷⁶ [89up website.](#)

¹⁷⁷ [Q2964](#)

¹⁷⁸ [Q3270](#), Damian Collins MP.

¹⁷⁹ [Q3270](#)

¹⁸⁰ [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017–19, HC 363, para 117

trabalho de análise de dados com as campanhas do referendo da UE.¹⁸¹

158. Os advogados da AIQ, Borden Ladner Gervais, escreveram ao Comitê para declarar: “AggregateIQ não é uma empresa associada da Cambridge Analytica, SCL ou qualquer outra empresa nesse setor. AggregateIQ é possui capital e operação 100% canadense. AggregateIQ escreveu software para a SCL. AggregateIQ não manipulou o micro-direcionamento nem facilitou sua manipulação.”¹⁸²

159. De acordo com os arquivos obtidos, certamente houve troca de dados entre a AIQ e a SCL, bem como entre a AIQ e a Cambridge Analytica. Os arquivos do repositório incluem logs 'debug' perdidos, que documentam a importação de dados, incluindo pontuações psicográficas do OCEAN, que Jeff Silvester reconheceu abertamente, em seu segundo depoimento perante o Parlamento canadense, terem vindo da Cambridge Analytica e foram usadas na parte desenvolvida pela AIQ do software Ripon.¹⁸³ Ao ser questionado por Nathaniel Erskine-Smith MP, vice-presidente do Comitê Permanente Canadense de Acesso à Informação, Privacidade e Ética e membro do 'Comitê Internacional', se a AIQ deveria ter sido mais diligente na obtenção de informações da SCL e convertendo-o em publicidade e direcionamento, Jeff Silvester disse:

Nós questionamos sobre a origem, mas a resposta que obtivemos foi de que era proveniente de fontes públicas de dados, e existem muitas delas nos Estados Unidos. Na época, não sabíamos que eles estavam obtendo informações de forma indevida. [...] Tendo em vista tudo o que aconteceu depois de trabalhar com a SCL, eu faria de novo? Provavelmente não.¹⁸⁴

160. Chris Vickery conseguiu encontrar o repositório da AIQ somente depois que um desenvolvedor da SCL deixou um script de software aberto em sua própria conta privada do Github.¹⁸⁵ O arquivo de script possui um cabeçalho informando que ele se originou de um desenvolvedor da AIQ. A equipe da SCL tinha acesso aos dados da AIQ e as duas empresas pareciam intimamente ligadas de uma forma incomum. De acordo com Chris Vickery, as evidências disponíveis apontavam para um relacionamento especial entre a AIQ, Cambridge Analytica, SCL, algo diferente do que normalmente ocorre num relacionamento comercial regular.

161. Dentro do repositório da AIQ, há referências ao "The Database of Truth", um sistema que obtém e integra dados de diversas fontes, coletando informações de centenas de milhares, talvez milhões, de eleitores.¹⁸⁶ Parte disso veio do banco de dados do RNC — o Republic National Committee Data Trust é o principal provedor de arquivos de eleitores do Partido Republicano — e outros vieram da campanha de Ted Cruz. Esse banco de dados pode ser buscado usando vários parâmetros, incluindo, entre outros: nome, sobrenome, ano de nascimento, idade, faixa etária, endereço de registro, se eram apoiadores de Trump e se votariam.

162. Os dados completos dos eleitores foram armazenados num local diferente do repositório do código, apesar de que o repositório incluía os meios pelos quais qualquer pessoa poderia ter acesso aos dados completos dos eleitores. As informações incluídas no 'Database of Truth' poderiam ter sido usadas para o direcionamento a usuários específicos no Facebook, usando seu recurso de direcionamento demográfico, para criar anúncios na plataforma do Facebook. Segundo Chris Vickery,

¹⁸¹ Referência acima, p. 42.

¹⁸² [Letter from Borden Ladner Gervais LLP to Damian Collins MP](#), 20 September 2018.

¹⁸³ [Evidence on Tuesday 12 June 2018](#), Standing Committee on access to information, privacy and ethics, Parliament of Canada, Q1045.

¹⁸⁴ Mesma referência acima.

¹⁸⁵ Github é um serviço de hospedagem na Web.

¹⁸⁶ No repositório, existe acesso apenas ao resultado de buscas, portanto, o número de usuários é desconhecido.

as credenciais contidas no "Database of Truth" poderiam ter sido usadas por qualquer pessoa que as encontrasse. Em outras palavras, qualquer pessoa pode encontrar senhas expostas no site e acessar milhões de informações particulares sobre indivíduos.

163. As referências no repositório explicam como o 'Database of Truth' foi usado pela WPAi, uma empresa que se descreve como “uma provedora líder de inteligência política para campanhas presidenciais, de governadores, de Senador Federal, prefeito e câmara de vereadores em todos os 50 estados dos Estados Unidos e em diversos países estrangeiros”.¹⁸⁷ O repositório também mostra que a WPAi trabalhou com a AIQ para o partido Osnova da Ucrânia.¹⁸⁸ WPAi foi apresentado como um parceiro da AIQ.

164. Com informações detalhadas sobre os eleitores disponíveis para a AIQ, a empresa poderia criar anúncios altamente direcionados no Facebook para alcançar potenciais eleitores. Mais especificamente, eles poderiam usar essas informações para segmentar usuários por: idade; gênero; localização, dentro de determinado raio (usando a ferramenta de direcionamento hiperlocal do Facebook); e raça (em 2018, o Facebook removeu mais de 5.000 opções que poderiam ter sido usadas para excluir determinados grupos minoritários religiosos e étnicos).¹⁸⁹

165. Chris Vickery descobriu um arquivo de "configuração" que ilustrava a interação entre a AIQ, a Cambridge Analytica e o site de notícias de direita Breitbart, dirigido pelo ativista ultra-conservador Steve Bannon. Um arquivo de configuração é uma coleção de configurações às quais o software se refere durante a execução, a fim de preencher variáveis. É um arquivo que descreve as preferências do usuário sobre como um programa deve ser executado, mas só pode solicitar o que o programa sabe fazer. Como consta do Relatório Preliminar, Steve Bannon atuou como estrategista-chefe da Casa Branca no início do mandato do Presidente Trump, tendo anteriormente atuado como Chefe Executivo da campanha eleitoral de Trump. Ele foi o presidente executivo do Breitbart News, um site que ele descreveu como 'a plataforma do movimento alt-right'. Ele também já ocupou o cargo de vice-presidente da Cambridge Analytica.¹⁹⁰

166. Existem evidências claras de que houve uma estreita relação de trabalho entre Cambridge Analytica, SCL e AIQ. Certamente havia uma relação contratual, mas acreditamos que as informações reveladas no repositório implicariam algo ainda mais próximo, com os dados compartilhados entre a AIQ e a SCL, bem como entre a AIQ e a Cambridge Analytica.

Trabalho da AIQ relacionado ao referendo sobre a UE

167. A AIQ realizou um trabalho de publicidade on-line para as organizações que apoiaram o Brexit, Vote Leave, Veterans for Britain, Be Leave e DUP Vote to Leave, todas elas, de acordo com Jeff Silvester, chegaram até a AIQ de forma independente.¹⁹¹ A maioria dos anúncios — 2.529 de um total de 2.823 — foi criada pela AIQ em nome do Vote Leave.¹⁹² O valor dessa campanha realizada e paga à AIQ pelas campanhas do Brexit incluía:

- £2,9 milhões pelo Vote Leave;

¹⁸⁷ [WPAi website](#), accessed 1 February 2019.

¹⁸⁸ O caso do partido Osnova será discutido mais adiante, no capítulo 7.

¹⁸⁹ [Keeping advertising safe and civil](#), Facebook blog post, 21 August 2018.

¹⁹⁰ [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017-19, HC 363, para 96

¹⁹¹ [Q2986](#)

¹⁹² [Investigation into the use of data analytics in political campaigns, a report to Parliament](#), 6 November 2018, para 3.6.

- £625.000 pelo BeLeave;
- £100.000 pelo Veterans for Britain; e
- £32.000 pelo DUP.¹⁹³

168. Por escrito, a AIQ negou o fato de a AIQ ter informações de indivíduos relacionadas ao referendo da UE:

As informações acessadas pelo pesquisador de segurança são principalmente códigos de software, mas também incluem informações de contato de apoiadores e eleitores de alguns dos nossos antigos clientes. Nenhum desses arquivos continha informações financeiras, senha ou outras informações pessoais confidenciais, e nenhuma das informações pessoais veio da campanha do Brexit.¹⁹⁴

169. Essa posição concorda com o trabalho do Departamento Federal de Privacidade do Canadá (OPC) e do Departamento de Informações e Privacidade da Colúmbia Britânica (OIPC), que estão conduzindo uma investigação conjunta. De acordo com o ICO “ainda não se chegou a uma conclusão. [...] eles nos informaram que não localizaram nenhum dado pessoal do Reino Unido, além dos identificados no escopo da nossa notificação de execução.”¹⁹⁵

170. Acreditamos que a AIQ manipulou, coletou, armazenou e compartilhou dados de cidadãos do Reino Unido, no contexto de seu trabalho no referendo da UE. Existe toda uma área do projeto AIQ - “Brexit Sync” - dedicada à sincronização de dados relevantes do Reino Unido e do Brexit, incluindo informações sobre indivíduos, de várias entidades clientes pró-Brexit. Os scripts de processamento contidos no repositório da AIQ também mostram que os IDs da conta do Facebook estavam sendo coletados e juntados aos perfis de eleitores de pessoas que moram no Reino Unido.

171. Chris Vickery nos disse que:

Desde o meu depoimento perante o Comitê, localizei uma planilha nos arquivos do repositório da AIQ contendo o nome, sobrenome e endereços de e-mail de 1.438 pessoas, aparentemente cidadãos britânicos. Estou presumindo a nacionalidade deles com base no domínio do endereço de email (exemplos: yahoo.com.uk, btinternet.com, hotmail.com.br, sky.com).¹⁹⁶

172. Como dissemos anteriormente, a AIQ fez uso de dados extraídos por Aleksandr Kogan que tinham como alvo eleitores nas eleições nos EUA. Portanto, a AIQ tinha a capacidade de enviar mensagens de e-mail para potenciais eleitores durante o referendo da UE e também buscar pessoas via Facebook. Ao enviar as mensagens de e-mail do Facebook para um “público personalizado”, todos os usuários cujos e-mails foram enviados e correspondiam aos e-mails usados para registrar contas no Facebook podiam ser direcionados com precisão por meio da plataforma.

173. Em resposta à intimação encaminhada pela Comissão Eleitoral para a campanha Vote Leave, Darren Grimes e Veterans for Britain, o Facebook disse à Comissão Eleitoral em maio de 2018 que a AIQ havia feito uso dados sobre público personalizado — permitindo que a AIQ alcançasse tanto usuários no Facebook que eram clientes como usuários que não eram clientes — alvos personalizados em sites e perfis similares.¹⁹⁷ A AIQ afirmou que se tratava de um erro administrativo, que foi

¹⁹³ [Q3000](#)

¹⁹⁴ [FKN0086](#)

¹⁹⁵ ICO, p42.

¹⁹⁶ Correspondence between the Committee and Chris Vickery, 22 January 2019.

¹⁹⁷ As explicações do Facebook sobre os diferentes públicos personalizados podem ser encontradas aqui: [Letter from Rebecca Stimson, Facebook to Louise Edwards, The Electoral](#)

rapidamente corrigido.¹⁹⁸

174. Além disso, o Facebook escreveu à Comissão Eleitoral em maio de 2018, em resposta a um pedido de informações relacionadas a grupos da campanha pró-Brexit. A carta afirma que “as eleições da SCL estão listadas como o contato de pelo menos uma conta de anúncio da AIQ no Facebook”. O endereço de email fornecido pertence a um funcionário da SCL.¹⁹⁹ Nenhuma explicação foi dada sobre por que esse deveria ser o caso.

175. James Dipple-Johnstone, Vice-Comissário de Informações, nos disse que os endereços de e-mail no repositório “vieram de outro trabalho que a empresa havia feito para empresas e organizações do Reino Unido, e que foram mantidos após o encerramento desses contratos anteriores que possuíam”.²⁰⁰ Em seu relatório de julho de 2018, o ICO confirmou que a AIQ tinha acesso aos dados pessoais dos eleitores do Reino Unido, repassados pela campanha Vote Leave, e que a AIQ “mantinha dados do Reino Unido que eles não deviam ter mantido”.²⁰¹ Esses dados foram descobertos no repositório da AIQ Gitlab que foi apresentado ao ICO pelo Comitê. Em outubro de 2018, expediu uma Notificação de Execução, mencionando que “o Comissário está convencido de que o responsável pelo tratamento descumpriu os Artigos 5(1)(a)-(c) e o Artigo 6 do GDPR”.²⁰² Dipple-Johnstone nos disse que o ICO “pediu que eles excluíssem esses dados como parte da notificação de execução”.²⁰³ **O AIQ tinha a capacidade de usar os dados extraídos pelo Dr. Kogan. Sabemos que eles fizeram isso durante as eleições nos EUA em 2014. Os dados do Dr. Kogan também incluíram dados dos cidadãos britânicos, levantando questionamentos sobre o uso durante o referendo da UE. Sabemos pelo Facebook que os dados correspondentes ao Dr. Kogan foram encontrados nos dados usados pela AIQ na campanha pró-Brexit. O Facebook acredita que isso é uma coincidência ou, nas palavras de Mike Schroepfer, CTO do Facebook, um “caso efetivamente aleatório”.**²⁰⁴ Não se sabe se os dados de Kogan foram destruídos pela AIQ.

176. Entre os repositórios da AggregateIQ que foram apresentados, estão aqueles relacionados a quatro grupos de campanhas do referendo da UE pró-Brexit: ChangeBritain; Vote Leave; DUP; e VeteransForBritain:²⁰⁵

- c / Client-ChangeBritain-Site
- c / Client-ChangeBritain-MailSend
- c / Client VoteLeave-MyPollingStation
- c / Client-VoteLeave-PlatformSync
- c / Client-DUP-ActionSite
- c / Client-VeteransForBritain-Site

Em julho de 2018, o Comitê publicou anúncios no Facebook que foram rodados pela AIQ durante o referendo da UE, o que ilustra o fato de que vários anúncios estavam sendo executados e direcionados pela AIQ para diferentes públicos. A série de PDFs destacou os anúncios executados pela AIQ durante

[Commission](#), 14 May 2018, p2.

¹⁹⁸ [Letter from Borden Ladner Gervais to the Committee, re testimony of AggregateIQ Data Services Limited before the DCMS Committee](#), 20 September 2018.

¹⁹⁹ [Letter from Rebecca Stimson, Facebook to Louise Edwards, The Electoral Commission](#), 14 May 2018, p4.

²⁰⁰ [Q3941](#)

²⁰¹ [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017-19, HC 363, 29 July 2018, para 119.

²⁰² [AIQ enforcement notice, 24 October 2018](#), ICO.

²⁰³ [Q3943](#)

²⁰⁴ [Q2497](#)

²⁰⁵ A Change Britain foi fundada como sucessora da campanha a favor do Vote Leave.

o referendo em nome do Vote Leave e do concurso de previsão '50 Million'.

Facebook, o Vote Leave e o concurso de previsão £50 Million

177. O concurso £50 Million foi uma iniciativa para coletar dados promovida pela campanha Vote Leave, que ofereceu aos fãs de futebol a chance de ganhar 50 milhões de libras. Para participar do concurso, os fãs tiveram que digitar seu nome, endereço, e-mail e número de telefone, e também como pretendiam votar no Referendo. Mas a elaboração da mensagem a ser enviada e para qual público foi absolutamente crucial. As capturas de tela publicadas em nosso site provam que a AIQ processou todos os dados do concurso de previsão £50 Million de futebol que eles organizaram, e coletaram IDs do Facebook e e-mail de inscrições no concurso.²⁰⁶

178. Além disso, um blog escrito por Dominic Cummings admitiu que o concurso era um exercício de coleta de dados: “Os dados chegaram ao solo e foram analisados pela equipe de cientistas de dados, logo integrados a todos os outros dados transmitidos. Esse foi o objetivo do nosso prêmio de 50 milhões de libras por prever os resultados do campeonato europeu de futebol, que reuniu dados de pessoas que geralmente ignoram a política.”²⁰⁷ Se as pessoas se dispuseram a preencher o questionário, seus dados foram coletados. Não há evidências para mostrar que esse processo foi fraudulento, mas é possível questionar se essa forma de coleta de dados é ética. Além disso, as chances de ganhar o prêmio de 50 milhões de libras foram estimadas em uma em 9,2 quintilhões (bilhões de bilhões).²⁰⁸

Recursos da AIQ

179. Os dados do repositório enviados por Chris Vickery destacam os recursos que a AIQ havia construído para obter e usar os dados pessoais das pessoas. Não está claro se essas ferramentas foram realmente usadas, mas está claro que elas foram desenvolvidas com o potencial de extrair e manipular dados. A inclusão de logs de depuração no repositório mostra que as ferramentas foram usadas. Não se sabe ao certo qual a total extensão do seu uso.

Inteligência artificial

180. Três linhas de machine learning foram usadas para processar texto e imagens. O software pode ser usado para ler fotografias de pessoas em sites, combiná-las com seus perfis do Facebook e direcionar publicidade a esses perfis individuais.

Pixels do Facebook

181. O Pixel do Facebook é um pedaço de código colocado em sites. O Pixel pode ser usado para registrar quando usuários do Facebook visitam o site. O Facebook pode usar as informações coletadas pelo Pixel para permitir que os anunciantes façam direcionamentos para usuários do Facebook que visitaram esse site. Definitivamente, a AIQ utilizou Pixels e outras ferramentas para ajudar nos esforços de coleta e direcionamento de dados.

182. Por exemplo, se um usuário visitou um site durante a campanha do referendo que estava usando um pixel de rastreamento do Facebook, que foi colocado ali pela campanha Vote Leave/AIQ, esses usuários poderiam receber anúncios dessa campanha sem saber por meio do Facebook. Esses usuários

²⁰⁶ [Capturas de tela no repositório da AIQ](#), enviadas por Chris Vickery

²⁰⁷ [Dominic Cummings's blog](#)

²⁰⁸ [Vote Leave launches £50m football prediction competition](#), Andrew Sparrow, The Guardian, 27 May 2016.

poderiam receber outros anúncios da campanha pelo Leave, se tivessem acesso aos mesmos dados de pixel. Isso seria possível se todos os anúncios sociais estivessem sendo gerenciados pela mesma entidade para todas as campanhas (é fácil compartilhar informações em pixels entre diferentes campanhas de publicidade do Facebook). No repositório, fica claro que a equipe da AIQ teve acesso a mais de uma campanha.

183. Chris Vickery, com base em sua análise do conteúdo do repositório Gitlab, acredita que os recursos da AIQ foram muito além:

“A AIQ coletou e juntou a perfis os IDs do Facebook de eleitores registrados no Reino Unido que tinham uma conta no Facebook. Esses dados foram todos sincronizados (combinados entre várias fontes de dados) e coletados através da plataforma oferecida pelo Nationbuilder.com. [...] Eu tenho os scripts de sincronização mostrando a agregação nessa plataforma, bem como os nomes dos bancos de dados controlados diretamente pela AggregateIQ que contêm esses dados (junto com os nomes de usuário e senhas para acessar os bancos de dados)”²⁰⁹

184. O Facebook nos contou sobre os diferentes tipos de ferramentas oferecidas a terceiros para fazer a integração em seus sites ou em outros produtos. Perguntamos para Mike Schroepfer, diretor de tecnologia do Facebook, o percentual de sites na internet em que o Facebook rastreia os usuários.²¹⁰ Ele apresentou uma resposta adequada, por isso pedimos novamente por escrito.

185. Em sua próxima carta, o Facebook novamente deixou de informar um valor, mas pelo menos apresentou exemplos de outras ferramentas que ele usa para rastrear usuários, por exemplo, plug-ins sociais (software que permite um serviço personalizado), como o botão Curtir e o botão Compartilhar. O Facebook nos disse que esses plugins "enriquecem a experiência dos usuários do Facebook, permitindo que eles vejam o que seus amigos do Facebook gostaram, compartilharam ou comentaram na Web".²¹¹ Esses plugins também beneficiam o Facebook, pois recebem informações quando um site com o plugin é visitado. Seus servidores registram: que um dispositivo visitou um site ou aplicativo; e qualquer informação adicional sobre as atividades da pessoa nesse site que o site opte por compartilhar com o Facebook. O Facebook nos disse que, entre 9 e 16 de abril de 2018, o botão Curtir do Facebook apareceu em 8,4 milhões de sites, o botão Compartilhar apareceu em 931 mil websites e havia 2,2 milhões de Pixels do Facebook instalados em sites.²¹²

186. Como a AIQ mantém vários sites contendo interesses britânicos, seria fácil instalar os pixels do Facebook em cada um dos sites que a AIQ construiu e depois compartilhar as informações de uma campanha com outra. Além de criar sites para campanhas baseadas no Reino Unido, existem evidências da criação mais ampla de criação e implantação de ferramentas para direcionamento dos eleitores do Reino Unido. Por exemplo, uma pasta chamada 'ChangeBritain-MailSend-master' contém uma biblioteca de aplicativos e também uma pasta chamada 'test'. Dentro dessa pasta, há um documento que parece ser uma carta modelo para os eleitores enviarem aos seus parlamentares, incentivando-os a votar em favor da denúncia baseada no artigo 50, caso haja uma votação parlamentar.

Captura de Perfis do LinkedIn

187. Existe uma ferramenta de captura de dados, dentro do repositório, com capacidade para extrair

²⁰⁹ [Written evidence](#), submitted by Chris Vickery

²¹⁰ [Qq 2104 - 2108](#)

²¹¹ [Letter from Rebecca Stimson, Facebook, to Damian Collins MP](#), 14 May 2018.

²¹² Mesma referência acima.

dados do LinkedIn. Há uma pasta chamada 'LinkedIn-person-fondler-master', que é um aplicativo que captura dados do usuário do LinkedIn. Dentro do repositório, há um arquivo que contém informações sobre 92.000 perfis do LinkedIn. Esses nomes poderiam ter sido usados para reunir a localização, a posição e o local de trabalho do usuário por meio da ferramenta de captura do LinkedIn. Usando o direcionamento de anúncios do Facebook, a AIQ poderia alcançar esses usuários por meio da segmentação de locais, locais de trabalho e cargos.

188. O [script LInbot.py](#) (robô ou bot do LinkedIn) contém comentários de quem o escreveu, explicando que ele captura dados das contas do LinkedIn. Há até um log perdido no mesmo diretório, sugerindo que esse bot foi executado pelo menos de 8 de outubro de 2017 a 19 de outubro de 2017. A captura de dados do LinkedIn, dessa maneira, descumpra os termos do Contrato do usuário do LinkedIn, que declara: "não permitimos o uso de software de terceiros, incluindo "rastreadores", bots, plug-ins de navegador ou extensões de navegador (também chamados de "add-ons"), que façam captura de dados".²¹³

189. Os advogados da AIQ, Borden Ladner Gervais, escreveram ao Comitê em 20 de setembro de 2019, afirmando que "a AggregateIQ desenvolveu uma ferramenta para buscar usuários no LinkedIn e abrir o perfil deles de forma a parecer que um candidato das eleições locais visualizou o perfil deles. Não era uma ferramenta de captura de dados. Além disso, essa ferramenta nunca foi implantada".²¹⁴

190. No entanto, de acordo com Chris Vickery, o comentário dentro da ferramenta afirma explicitamente que realiza captura de dados, "nem se dá ao trabalho de usar um termo mais leve". A correspondência sofisticada de dados entre o LinkedIn e o Facebook, quando combinada com um banco de dados detalhado de contatos capturados, poderia ter sido usada pela AIQ para dar aos seus clientes políticos uma vantagem importante na exibição de anúncios políticos altamente direcionados, quando o alvo desses anúncios não consentisse com o uso dos seus dados dessa forma. Acreditamos que a AIQ certamente desenvolveu uma ferramenta para o LinkedIn com a intenção de capturar dados dessa rede social.

Conclusão

191. O Relatório do ICO, "Investigação sobre o uso da análise de dados em campanhas políticas", destacou o trabalho deles na investigação do relacionamento entre a Cambridge Analytica, a SCLE e a AIQ.²¹⁵ Identificou a existência de "uma permeabilidade" entre as empresas acima e além do que normalmente seria esperado".²¹⁶ O ICO afirma que as preocupações mais amplas com a estreita colaboração das empresas são compreensíveis e cita as seguintes transações e contatos financeiros:

Em 24 de outubro de 2014, a SCLE Elections Limited efetuou pagamentos ao Facebook de aproximadamente US\$ 270.000 numa conta de anúncios da AIQ; em 4 de novembro de 2014, a SCLE efetuou um pagamento de US\$ 14.000 na mesma conta de anúncios da AIQ. Mais tarde, um reembolso de anúncios não utilizados da AIQ foi feito para a SCLE, com a explicação de que a SCLE havia efetuado pré-pagamentos para suas campanhas sob a AIQ. A SCLE foi listada como um dos principais contatos de pelo menos um dos AIQ. As contas do Facebook e o endereço de e-mail desse contato pertenciam a um funcionário da SCLE que também estava

²¹³ [Prohibitive software and extensions](#), LinkedIn's terms of agreement, accessed 2 December 2018.

²¹⁴ [Letter from Borden Ladner Gervais LLP to Damian Collins MP](#), 20 September 2018.

²¹⁵ [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018, p40-43.

²¹⁶ [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018, p40.

envolvido em vários pagamentos.²¹⁷

No entanto, as investigações do ICO mostraram que, embora houvesse uma estreita relação de trabalho, "não temos evidências de que a AIQ tenha deixado de ser uma outra pessoa jurídica".²¹⁸

192. Dos arquivos obtidos por Chris Vickery e das evidências que recebemos, parece que a relação AIQ/Cambridge Analytica/SCL é mais profunda do que normalmente se vê numa relação estritamente contratual. **A AIQ trabalhou tanto nas primárias presidenciais dos EUA como em organizações relacionadas ao Brexit, incluindo a campanha Vote Leave, durante o referendo da UE. O trabalho da AIQ destaca o fato de que os dados foram e ainda estão sendo amplamente utilizados por empresas privadas para atingir pessoas, muitas vezes num contexto político, a fim de influenciar suas decisões. É muito mais comum do que as pessoas imaginam. O próximo capítulo destaca a natureza generalizada desse direcionamento.**

Propaganda e Campanha Política

Introdução

193 A investigação do ICO sobre o uso da análise de dados em campanhas políticas revelou "uma desconsideração preocupante da privacidade pessoal dos eleitores".²¹⁹ O ICO enfatiza que "os cidadãos só podem tomar decisões de forma realmente consciente sobre em quem votar, se tiverem certeza de que essas decisões não foram indevidamente influenciadas".²²⁰ Por esse motivo, quando dados pessoais são usados para direcionar mensagens políticas, esse uso deve ser transparente e legal.

194. O Relatório da Comissão Eleitoral, "Campanha Digital: Aumentando a Transparência para os Eleitores", publicado em junho de 2018, recomenda que a lei precisa ser alterada para garantir "mais clareza sobre quem é o responsável pelos pagamentos, o quê, onde e como está sendo comprado, além de impor punições mais severas para os que descumprirem as regras. O financiamento de campanhas on-line já está coberto pelas leis sobre gastos e doações nas eleições. Mas as leis precisam garantir mais clareza sobre quem está gastando o quê, onde e como e deve prever punições mais severas para os que descumprirem as regras."²²¹ Este capítulo destacará a diferença entre publicidade geral e publicidade política, e as medidas que estão sendo tomadas para aumentar a transparência em relação à publicidade política. Recomenda-se a leitura em conjunto com as recomendações a esse respeito incluída no nosso Relatório Preliminar.

Anúncios online

195. A publicidade não política no Reino Unido é regulamentada pela Agência de Padrões para Publicidade (ASA), que emprega um sistema de autorregulação e co-regulação, financiado pelo setor da publicidade. Guy Parker, CEO da ASA, nos disse que "os padrões que aplicamos através dos nossos códigos de publicidade são, quase sem exceção, os mesmos para publicidade de rádio e TV e para outros tipos de publicidade, incluindo online".²²²

²¹⁷ Mesma referência acima, p. 41.

²¹⁸ [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018, p41.

²¹⁹ [Investigation into the use of data analytics in political campaigning: a report to Parliament](#), ICO, 6 November 2018, p6.

²²⁰ Mesma referência acima.

²²¹ [Digital Campaigning: increasing transparency for votes](#), Electoral Commission, June 2018, p3.

²²² [Q4101](#)

196. Qualquer publicidade fora da rádio e TV, incluindo em sites, e-mails e redes sociais, está sujeita a autorregulação. A co-regulação é promovida conjuntamente pela ASA e a Ofcom, a agência regulatória de comunicações e a autoridade de licenciamento de rádio e TV. Dessa forma, a ASA regula a publicidade de rádio e TV tomando por base os regulamentos de transmissão emitidos pela Ofcom.²²³

197. Anunciantes que descumprem os padrões da ASA estão sujeitos a sanção. No entanto, o ASA não tem competência para iniciar um processo judicial contra anunciantes que se recusam a cumprir os Códigos. Além de julgar as reclamações, a ASA pode exercer pressão sobre as empresas do setor de publicidade que reconhecem seus Códigos, e a mídia, os prestadores de serviço podem decidir recusar o trabalho ou negar acesso ao espaço, além da publicidade negativa que o caso pode gerar.²²⁴

198. Devido ao fato de a ASA ser a agência reguladora de publicidade do Reino Unido, Guy Parker nos disse que apenas os anúncios do Reino Unido estão sob seu controle, definindo um anúncio do Reino Unido como "um anúncio direcionado aos consumidores do Reino Unido". No entanto, ele disse que o ASA "levaria em conta o país de origem da empresa que enviou o anúncio, por exemplo, por envio direto de mensagens. Podemos trabalhar com nosso contraparte no país dessa empresa se tivermos um acordo de tratamento conjunto de denúncias transnacionais com esse país."²²⁵ Existem dificuldades óbvias relacionadas a essa definição, já que esses anúncios podem ter origem no exterior ou podem ter origem desconhecida.

199. Guy Parker disse que o Facebook, o Google e outras empresas digitais que ganham dinheiro com anúncios on-line devem trabalhar para remover anúncios enganosos e fraudulentos, e devem contribuir financeiramente para a ASA, para melhorar os sistemas e processos de regulação da publicidade on-line.²²⁶

Propaganda política online

200. A Sociedade de Reforma Eleitoral publicou recentemente "Combatendo o 'Oeste Selvagem' Político: regras de campanha para o século XXI", coincidindo com o 15º aniversário do lançamento do Facebook e 19 anos após a criação das principais regras eleitorais. Fez propostas para garantir transparência adequada nas campanhas: "a capacidade de transmitir rapidamente desinformação e canalizar milhões de libras em campanhas sem escrutínio representa um enorme desafio. Muita coisa mudou — mas nossas regras de campanha permaneceram na era analógica".²²⁷ O relatório descreve o aumento dos gastos dos partidos políticos em anúncios no Facebook nas duas últimas eleições gerais: em 2015, foram cerca de £1,3 milhão; em 2017, havia crescido para cerca de £3,2 milhões.²²⁸ Esse foi o gasto em nível nacional, sem considerar o gasto com campanhas locais.

201. Em junho de 2018, a Comissão Eleitoral publicou um gráfico, destacando a proporção de dinheiro que os candidatos alegaram gastar em publicidade digital como porcentual do total gastos com publicidade.²²⁹ Eles explicaram que o gráfico não mostra o quadro completo da publicidade digital

²²³ [ASA website](#), accessed 5 February 2019.

²²⁴ [Self-regulation and co-regulation, ASA website](#), accessed 5 February 2019.

²²⁵ [Q4108](#)

²²⁶ [Q4112](#)

²²⁷ [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.

²²⁸ Mesma citação acima, Dr. Jess Garland, Diretor de Política e Pesquisa, ERS.

²²⁹ [Digital campaigning: increasing transparency for voters](#), The Electoral Commission, June 2018, p4.

nas eleições e referendos: “Contém apenas dados de gastos nas plataformas digitais mais conhecidas, informadas pelos candidatos registrados”. Assim como outros anunciantes digitais, os candidatos também podem 'curtir', 'compartilhar' e 'postar' mensagens gratuitamente, com o potencial de atingir um público maior.²³⁰

202. A publicidade política na televisão está sujeita a regulação estrita, e os partidos ou organizações políticas não podem ser donos de canais de TV ou rádio, nem podem administrar uma emissora ou canal. As transmissões políticas do partido têm regras e regulamentos claros, supervisionados pela Ofcom, durante os períodos eleitorais.²³¹ A publicidade política fora da TV e da rádio permanece sem regulamentação e, como dissemos em nosso Relatório Preliminar, a capacidade das empresas de mídia social de direcionar conteúdo para indivíduos, inclusive de forma privada, é um fenômeno novo, que cria problemas em relação à regulamentação das eleições.²³²

203. A Comissão Eleitoral descreveu a natureza perniciosa dos anúncios políticos micro-direcionados: “Somente o eleitor, o candidato e a plataforma sabem quem foi o alvo das mensagens. Somente a empresa e o candidato sabem por que um eleitor foi selecionado e quanto foi gasto numa campanha específica”.²³³ Guy Parker, CEO da ASA, esclareceu a posição em torno da regulamentação dessa publicidade política on-line:

Não cobrimos publicidade política, que também definimos como publicidade, independentemente do momento em que é veiculada — ela também é veiculada fora do período eleitoral — cujo principal objetivo é influenciar os eleitores numa eleição ou referendo.

[...] Nosso sistema de regulação depende da adesão das pessoas que serão objeto da nossa regulação. Os partidos políticos e os grandes grupos de campanha nunca concordaram em cumprir os nossos códigos de publicidade.²³⁴

204. É importante reconhecer o fato de que nem todos os anúncios políticos são promovidos por partidos políticos; eles podem ser promovidos por grupos e contatos pessoais, alguns não são nem pagos. Os Grupos do Facebook são onde pessoas e organizações podem compartilhar seus interesses e expressar uma opinião e podem ser: públicos, quando qualquer pessoa pode ver quem são os membros do Grupo e o que foi publicado; fechado, quando somente os convidados a participar do grupo podem ver e compartilhar o conteúdo; ou oculto, quando ninguém no Facebook sabe da existência do grupo, somente os membros do próprio grupo. As páginas do Facebook são sempre públicas, criadas por organizações para interagir com seu público e publicar conteúdo, mas apenas os administradores das páginas podem postar na conta.²³⁵

205. Em 5 de fevereiro de 2019, o Facebook proibiu quatro grupos do Facebook na Birmânia, classificando-os como "organizações perigosas": o Exército Arakan, o Exército da Aliança Democrática Nacional de Mianmar, o Exército da Independência de Kachin e o Exército de Libertação Nacional de Ta'ang. Eles também banirão “todos os elogios, apoios e declarações relacionados a esses grupos” assim que “tomarem ciência da publicação”.²³⁶

²³⁰ Mesma referência acima.

²³¹ [Q3790](#), Sharon White, CEO, Ofcom.

²³² [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017-19, HC 363, 29 July 2018, para 137.

²³³ [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017-19, HC 363, 29 July 2018, para 140.

²³⁴ [Q4102](#)

²³⁵ [Using Facebook Groups](#), Tiffany Black, lifewire, 16 December 2018.

²³⁶ [Banning more dangerous organizations from Facebook in Myanmar](#), Facebook newsroom, 5 February 2019.

206. Por escrito, a Dra. Kate Dommett, University of Sheffield, recomendou a criação de um registro público de toda a publicidade política, diferenciando entre campanhas formalmente afiliadas (um partido político e as empresas que pagam para realizar publicidade digital) e campanhas de informação, promovidas sem influência direta da parte. Isso "estabeleceria um entendimento sobre o cenário político"²³⁷

207. Nosso Relatório Preliminar defendeu a sugestão da Comissão Eleitoral de que todas as campanhas eletrônicas deveriam trazer marcas digitais facilmente identificáveis, incluindo informações sobre a organização responsável pela publicação e quem seria legalmente responsável pelo gasto.²³⁸ Essas recomendações foram semelhantes às feitas pelo Comitê de Normas da Vida Pública.²³⁹

208. É especialmente importante conhecer a origem dos anúncios políticos ao considerar a questão da interferência no exterior nas eleições. A fonte geográfica de um anúncio deve facilmente identificável. Também é necessário agir rapidamente durante o curto período de uma campanha, quando ocorre publicidade política falsa, enganosa ou ilegal. A demora em agir aumenta a possibilidade de que a desinformação possa influenciar o resultado.

209. A Coalizão de Reforma na Publicidade Política, que inclui representação da Sociedade Incorporada de Anunciantes Britânicos (ISBA), Comissão da Internet e Econsultancy, desenvolveu um plano composto por quatro pontos para o futuro dos anúncios políticos. O plano recomenda que: todas as alegações de fato usadas em anúncios políticos sejam verificadas previamente; um organismo novo ou existente deve ter o poder de regular o conteúdo político da publicidade; todos os anúncios políticos pagos devem estar disponíveis para exibição pública, em um único site pesquisável; e anúncios políticos devem ter uma marca ou marca d'água para identificar o patrocinador do anúncio.²⁴⁰

210. *Repetimos a recomendação do nosso Relatório Preliminar, de que o governo deve examinar as maneiras pelas quais a lei do Reino Unido deve definir a campanha digital, incluindo definições sobre o que constitui a publicidade política on-line, como os tipos pré-definidos de palavras que normalmente surgem em anúncios que não são patrocinados por um partido político específico. Também é preciso reconhecer o papel e o poder das campanhas não pagas e dos Grupos do Facebook que influenciam as eleições e os referendos (dentro e fora do período eleitoral).*

211. *A lei eleitoral não é adequada para fazer esse controle e precisa ser alterada para refletir as mudanças técnicas de campanha e a migração de folhetos e outdoors físicos para campanhas políticas on-line com micro-direcionamento. Precisamos de transparência absoluta das campanhas políticas online, incluindo faixas claras e persistentes em todos os anúncios e vídeos políticos pagos, indicando a fonte e o anunciante; uma categoria introduzida para gastos digitais em campanhas; e regras explícitas que envolvem o papel e as responsabilidades dos candidatos.*

212. *Esperamos que a consulta do Gabinete leve à conclusão, por parte do governo, de que a publicidade política paga deve ser acessível ao público de forma clara e facilmente reconhecível. Os destinatários devem poder identificar a fonte, quem fez o upload, quem o patrocinou e o país de origem.*

213. *O governo deve realizar uma revisão abrangente das regras e regulamentos atuais em torno do*

²³⁷ [FKN0104](#)

²³⁸ [Disinformation and 'fake news': Interim Report](#), DCMS Committee, Fifth Report of Session 2017-19, HC 363, 29 July 2018, para 41.

²³⁹ [Intimidation in Public Life: a review by the Committee on Standards in Public Life](#), December 2017.

²⁴⁰ [The Coalition for Reform in Political Advertising blog](#), accessed 3 February 2019.

trabalho político durante as eleições e referendos, incluindo: aumento da duração do período sujeito a regulação; definir o que constitui campanha política; e reduzir o tempo para apresentar declarações de gastos à Comissão Eleitoral.

214. O governo deve buscar maneiras pelas quais a Comissão Eleitoral possa ter mais poderes para realizar seu trabalho de modo mais abrangente, incluindo as seguintes medidas:

- a competência legal para obrigar as organizações que atualmente não estão sujeitas a regulação, incluindo empresas de mídia social, a repassar informações mediante consulta;*
- O valor máximo de multa da Comissão Eleitoral, que atualmente é de £20.000, deveria ser aumentado e ajustado como um percentual fixo do retorno, como já ocorre com outros órgãos reguladores;*
- Possibilidade de a Comissão Eleitoral representar contra uma eleição devido a ações ilegais, o que atualmente só pode ser feito por indivíduos;*
- Possibilidade de a Comissão Eleitoral intervir ou impedir que alguém atue ilegalmente numa campanha, se essa pessoa mora fora do Reino Unido.*

215. Os anúncios políticos devem ter acesso público num repositório pesquisável - quem está pagando pelos anúncios, quais organizações estão patrocinando o anúncio e que está sendo direcionado pelos anúncios - para que as pessoas possam entender o comportamento de cada anunciante. Deve ser operado de forma independente do setor de publicidade e dos partidos políticos. Esta recomendação toma por base o parágrafo 144 do nosso Relatório Preliminar.

216. Concordamos com a proposta do ICO de que um Código de Prática, que destaca o uso de informações pessoais em campanhas políticas e se aplica a todos os controladores de dados que processam dados pessoais para fins de campanhas políticas, deve ser sustentado pela legislação principal. Recomendamos fortemente que Governo siga as recomendações do ICO e apresente a legislação principal para converter esses Códigos de Prática em lei.

217. Apoiamos a recomendação do ICO de que todos os partidos políticos trabalhem com o ICO, a Secretaria de Governo e a Comissão Eleitoral, para identificar e implementar uma solução entre partidos para melhorar a transparência sobre o uso de dados comuns. Esta seria uma solução prática para garantir que o uso de dados durante eleições e referendos seja tratado legalmente. Esperamos que o governo trabalhe para que essa colaboração aconteça. Esperamos que o governo resolva todas essas questões quando responder à consulta que lhe foi encaminhada: “Protegendo o Debate: Intimidação, Influência e Informação” e ao relatório da Comissão Eleitoral, “Campanha Digital: Aumentando a Transparência para os Eleitores”. Um aspecto crucial da publicidade e da influência política é o da interferência estrangeira nas eleições, que esperamos que também seja enfrentado fortemente.

Facebook e as Redes Tradicionais

218. O Facebook e o Twitter afirmam ter trabalhado para diminuir o espaço para disseminação de desinformação em seus sites. No entanto, durante a nossa investigação, quando encomendamos trabalhos do 89up, eles também analisaram o trabalho do 'Mainstream Network', site sofisticado pró-Brexit, promovido no Facebook, com um gasto de publicidade estimado em £257.000 em apenas 10

meses em 2018.²⁴¹ Usando as ferramentas do Facebook para acessar anúncios, a 89up encontrou mais de 70 anúncios que o site estava executando ao mesmo tempo. Descobriram que a Mainstream Network estava direcionando anúncios para eleitores específicos, incentivando-os a enviar e-mails padronizados para o seu MP. Os anúncios incluíam, por exemplo, um para rejeitar o chamado "Chequers Deal" do Primeiro Ministro. Sempre que um usuário envia um email para o seu MP pelo site, a Mainstream Network coloca seu próprio email no campo BCC. Significa que os dados do usuário estão sendo armazenados pelo proprietário do site e podem ser utilizados para fins de marketing, usando o recurso de 'Público Personalizado' do Facebook.²⁴²

219. No depoimento, a 89up informou que o conteúdo da Mainstream Network havia atingido 10,9 milhões de usuários apenas no Facebook:

O site é altamente enganador e não contém informações sobre os autores do conteúdo, nem informações exigidas por lei para cumprir com o GDPR. Com o nível estimado de gastos, é possível que esse site tenha descumprido as regras do GDPR e da Comissão Eleitoral para promotores políticos não vinculados a um partido.²⁴³

220. É preocupante que esse site esteja sendo executado de forma anônima, para que não seja possível verificar as origens da organização, quem está pagando pelos anúncios e em que moeda, e por que campanhas políticas estão sendo realizadas sem qualquer transparência sobre quem os está executando. O Facebook exige que as campanhas políticas nos EUA e na Índia sejam registradas como "anúncios políticos ou questões de relevância nacional", mas esse não é o caso no Reino Unido.²⁴⁴ Atualmente, o ICO está investigando as atividades da Mainstream Network e se houve uma infração ao GDPR na distribuição de tais comunicações.²⁴⁵

221. Em outubro de 2018, o Facebook anunciou novos requisitos para organizações e indivíduos que promovem anúncios que apresentam figuras políticas, partidos, eleições, legislação no Parlamento ou referendos anteriores. Esses requisitos representam um novo processo de verificação, em que as pessoas que promovem anúncios políticos devem comprovar sua identidade (por meio de passaporte, carteira de motorista ou visto de residência), que será verificada por uma instituição independente. Anúncios políticos suspeitos de promover informação enganosa ou desinformação podem ser denunciados e, se o anúncio trouxer elementos falsos, poderá ser eliminado.

222. Quando Richard Allan, vice-presidente de Políticas Públicas EMEA no Facebook, foi perguntado sobre a Mainstream Network, durante o seu depoimento perante o "Comitê Internacional" em novembro de 2018, ele disse que não havia nada de ilegal em um site que exibia esses anúncios, mas que a nova política do Facebook agora fará com que "qualquer organização que queira exibir anúncios como esse terá que autorizar. Nós vamos registrar as suas informações de identificação. Terão que fazer uma declaração adequada de responsabilidade. Os anúncios serão arquivados". Quando perguntado quem estava por trás da conta da Mainstream Network, Richard Allan disse:

Os dados do proprietário da conta no Facebook seria divulgado no curso de um processo regular, se houvesse uma investigação por alguma entidade com competência legal para fazê-lo.²⁴⁶

²⁴¹ [Written evidence on Mainstream network.co.uk](#) submitted by 89up, October 2018.

²⁴² Facebook's 'Custom Audiences' was explained in Chapter 4.

²⁴³ 89up evidence, October 2018.

²⁴⁴ [Written evidence on Mainstreamnetwork.co.uk](#), submitted by 89up, 20 October 2018.

²⁴⁵ [Q3913](#), Elizabeth Denham.

²⁴⁶ [Q4218](#)

Nossas próprias investigações mostraram que a Mainstream Network não está mais exibindo anúncios políticos no Facebook. No entanto, também não existe acesso aos anúncios publicados antes de 16 de outubro de 2018, pois os anúncios políticos exibidos antes dessa data não estão mais visíveis. Richard Allan foi questionado se informaria ao Comitê os dados que quem está por trás da conta, e por que ele não o faria, se fosse o caso. ²⁴⁷**A Mainstream Network é outro exemplo mais recente de uma organização on-line que busca influenciar o debate político usando métodos semelhantes aos que despertaram preocupação com o referendo da UE, e não há boas razões para a Mainstream Network se esconder atrás do anonimato. Esperamos receber informações do Facebook sobre a Mainstream Network, que não recebemos até agora, apesar das promessas de Richard Allan de que encaminharia essas informações. Consideramos a resposta do Facebook, de modo geral, como falsa, mais um exemplo de má-fé do Facebook. O Comissário de Informação confirmou que está atualmente investigando as atividades deste site e o Facebook, em qualquer caso, terá que cooperar com o ICO.**

223. As empresas de tecnologia devem combater o uso de empresas de fachada e outras tentativas profissionais de ocultar a identidade na compra de anúncios, especialmente em torno da publicidade política - dentro e fora dos períodos de campanha. Deve haver uma divulgação completa do direcionamento usado como parte da transparência da publicidade. O governo deve explorar formas de regulamentar o uso do direcionamento externo em redes sociais, como o Público Personalizado do Facebook.

224. A rápida ascensão de novos sites de notícia populistas de direita está promovendo conteúdo conspiratório e heterodoxo para fora dos canais da mídia tradicional. Isso pode ser visto no sucesso, por exemplo, do site PoliticalUK.co.uk, que funciona em uma rede de sites, páginas de redes sociais e contas de vídeo. Desde a sua criação, no final de abril de 2018, de acordo com Tom McTague, PoliticalUK ganhou mais de 3 milhões de interações nas redes sociais, com uma média de 5.000 'envolvimentos' para cada história publicada. ²⁴⁸

225. McTague observou em sua investigação que a notícia do PoliticalUK.co.uk "A imprensa se cala diante de milhares de protestos contra a traição do Brexit", sobre uma manifestação em Westminster em dezembro de 2018, liderada pelo ativista de extrema-direita Stephen Yaxley-Lennon, também conhecido como Tommy Robinson, recebeu 20.351 interações no Facebook. Para efeito de comparação, um artigo mais crítico sobre o mesmo evento, divulgado pelo Daily Mail, recebeu apenas 3.481 interações. O conteúdo do PoliticalUK.co.uk está sendo promovido por grupos do Facebook, incluindo 'EU-I Voted Leave', seguida por mais de 220.000 pessoas. O próprio Robinson tem mais de 1 milhão de seguidores no Facebook, fazendo dele a segunda figura política britânica mais popular do site, depois do líder do Partido Trabalhista, Jeremy Corbyn.

226. No entanto, ferramentas que permitem ao público ver a maneira pela qual os usuários do Facebook estão sendo direcionados pelos anunciantes foram bloqueadas recentemente pelo Facebook. Evidência que recebemos do Who Targets Me? levanta dúvidas sobre a disposição do Facebook em ter mais transparência em seu site. Who Targets Me? foi criado em 2017 para ajudar o público a entender como eles estavam sendo alcançados por anúncios on-line durante as eleições gerais. Ele explica o seu trabalho, em colaboração com a London School of Economics, o Oxford Internet Institute e a Sheffield University:

²⁴⁷ [Q4219](#)

²⁴⁸ [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.

Nossa ferramenta pode ser instalada como uma extensão do navegador e, em seguida, coleta dados dos usuários do Facebook e mostra estatísticas personalizadas de quantos anúncios eles viram. Os dados também são armazenados num banco de dados mestre, compartilhado exclusivamente com pesquisadores e jornalistas interessados em expor informação enganosa, gastos excessivos nas eleições e microdirecionamento, entre outras questões. Nossa ferramenta pode ser instalada como uma extensão do navegador e, em seguida, coleta dados dos usuários do Facebook e mostra estatísticas personalizadas de quantos anúncios eles viram. Os dados também são armazenados num banco de dados mestre, compartilhado exclusivamente com pesquisadores e jornalistas interessados em expor informação enganosa, gastos excessivos nas eleições e microdirecionamento, entre outras questões.

227. Em 9 de janeiro de 2014, Who Targets Me? e todas as outras instituições que operam nesse espaço, incluindo ProPublica e Mozilla, perderam o acesso a esses dados. O Facebook fez essa alteração com o objetivo de bloquear ferramentas que funcionam para destacar o conteúdo e o direcionamento dos anúncios no Facebook. Atualmente, não existe como os pesquisadores auditarem a publicidade no Facebook.²⁴⁹

228. O ICO solicitou que um Código de Prática seja instituído como lei, para ressaltar o uso de informações pessoais em campanhas políticas — seguindo os mesmos códigos estabelecidos na Lei de Proteção de Dados²⁵⁰ — incluindo regras de conduta apropriadas para cada idade, regras de proteção de dados e código de conduta jornalística.²⁵¹ O ICO prevê que essas regras se aplicariam a todos os controladores de dados que processam dados pessoais para fins de campanha política. O ICO possui poderes, nos termos do Regulamento Geral de Proteção de Dados (GDPR), para produzir códigos de práticas relacionados às atribuições do Comissário, sendo que eles pretendem fazer isso antes das próximas eleições gerais.²⁵² Mas o ICO também considera que esses códigos devem ter uma base legal na legislação principal, e foi feita uma consulta sobre esta proposta em 21 de dezembro de 2018. Entendemos também que apenas somente depois que esses códigos de prática estiverem em funcionamento é que o processamento de dados pessoais será levado a sério.

Conselho Constitucional de Pesquisa (CRC)

229. Essa falta de transparência na publicidade política foi ilustrada pela doação do Conselho Constitucional de Pesquisa (CRC) durante o referendo da UE. O CRC é uma organização de financiamento sem personalidade jurídica sediada na Escócia, que contribuiu para a campanha a favor do Brexit promovida pelo Partido Sindicalista Democrático na Irlanda do Norte e na Inglaterra, durante o referendo da UE. Doou £435.000 para o DUP, a maior doação política da história da Irlanda do Norte, dos quais £425.000 foram gastos em publicidade na campanha do referendo. Seu único representante identificado é o seu presidente, Richard Cook. Surgiram alegações de que o Vote Leave e o DUP faziam parte de uma campanha coordenada no referendo da UE, e que as atividades financeiras de Richard Cook envolviam fraudes relacionadas à gestão de resíduos.²⁵³ O Comitê escreveu duas vezes para Richard Cook, perguntando a origem da doação de £435.000 e como se esperava que o dinheiro seria gasto. Recebemos uma resposta em 5 de novembro de 2018. Richard Cook alegou estar “muito satisfeito” em receber a carta do Comitê. Logo, acusou o comitê de

²⁴⁹ Mesma referência acima.

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.

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.

disseminar “notícias falsas e desinformação” sobre ele. No entanto, ele se recusou a revelar a origem do dinheiro ou a dizer como o Conselho Constitucional de Pesquisa acreditava que seria gasto.²⁵⁴

230. A Comissão Eleitoral apresentou provas em 6 de novembro de 2018, e foi questionada sobre essa doação do CRC. A então CEO, Claire Bassett, explicou que "a própria lei nos impõe restrições sobre o que podemos dizer sobre qualquer doação realizada antes de 2017", e que não "gostariam de se colocar nessa situação, infelizmente".²⁵⁵ As doações feitas a partidos políticos na Irlanda do Norte até julho de 2017 estão protegidas contra divulgação, de acordo com a Seção 71E da Lei de Partidos Políticos, Eleições e Referendos de 2000. Louise Edwards, Chefe de Regulamentos da Comissão Eleitoral, explicou a situação:

O Partido Sindicalista Democrático, um partido registrado na Irlanda do Norte, tinha o dever de nos apresentar relatórios trimestrais sobre doações ao longo do período do referendo, o que foi feito. Temos a atribuição de verificar o conteúdo dos relatórios de doações para as partes da Irlanda do Norte, e esse é um trabalho que levamos muito a sério e que cumprimos. Se entendemos que alguma doação desses relatórios é inadmissível, as restrições [...] deixam de se aplicar e podemos tratar dessa doação específica. Não podemos tratar de doações para o DUP além desse período, porque, esses relatórios foram verificados e os doadores eram regulares.²⁵⁶

231. Quando indagada se haveria um plano comum entre o Conselho Constitucional de Pesquisa ao doar £435.000 para o DUP e reservar um anúncio de £280.000 no jornal Metro, em Londres, a favor do Vote Leave (poucos dias antes da votação), Louise Edwards respondeu que “não posso responder essa pergunta sem descumprir a legislação, infelizmente”.²⁵⁷ Quando indagada se o dinheiro do CRC doado para o DUP era do Reino Unido e não de origem estrangeira (o que tornaria a doação inaceitável pela legislação do Reino Unido), Claire Bassett respondeu que "estávamos convencidos de que os doadores eram regulares".²⁵⁸ Quando indagada se a instituição havia sido informada sobre a origem do dinheiro, Louise Edwards e Claire Bassett disseram: "não podemos mais discutir esse assunto" ²⁵⁹e "estávamos convencidos de que os doadores eram regulares de acordo com a legislação do Reino Unido", ²⁶⁰levando-se em conta “várias fontes”. ²⁶¹Elas também foram incapazes, por lei, de confirmar se conheciam a identidade da pessoa que doou o dinheiro.²⁶²

232. As doações feitas a partidos políticos na Irlanda do Norte até julho de 2017 estão protegidas contra divulgação, de acordo com a Seção 71E da Lei de Partidos Políticos, Eleições e Referendos de 2000. Esse dispositivo impede que a Comissão Eleitoral divulgue qualquer informação relacionada a essas doações antes de julho de 2017. Concordamos com a Comissão Eleitoral que é "profundamente lamentável" que eles estejam impedidos, por lei, de informar aos membros do Parlamento e ao público os detalhes sobre a origem da doação de £435.000 que foi dada pelo Conselho Constitucional de Pesquisa (CRC) para o DUP ou o processo de *due diligence* que foi realizado. Mas diante da lei vigente, este Comitê e o público em geral não têm como investigar a origem da doação de £435.000 ao DUP feita em nome do CRC e estão impedidos de saber se vieram de uma instituição cujos membros aprovaram a doação, ou se não foi esse o caso, ou se

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

²⁵⁵ [Q4068](#)

²⁵⁶ [Q4068](#)

²⁵⁷ [Q4081](#), Louise Edwards

²⁵⁸ [Q4069](#), Claire Bassett

²⁵⁹ [Q4070](#), Louise Edwards

²⁶⁰ [Q4069](#), Louise Edwards

²⁶¹ [Q4072](#), Louise Edwards

²⁶² [Q4075](#), Claire Bassett

veio de algum indivíduo rico.

233. *Existe uma falta de transparência em torno da relação entre o Conselho Constitucional de Pesquisa, o DUP e o movimento Vote Leave. Acreditamos que, para evitar ter que divulgar a fonte dessa doação de £435.000, o CRC, de forma deliberada e conscientemente, explorou uma brecha na lei eleitoral para direcionar dinheiro para o Partido Sindicalista Democrático na Irlanda do Norte. Esse dinheiro foi utilizado para custear a publicidade em jornais pró-Brexit fora da Irlanda do Norte e para pagar à empresa de análise de dados canadense Aggregate IQ.*

234. *Apoiamos a Comissão Eleitoral em seu pedido de que o governo estenda as regras de transparência em torno de doações feitas a partidos políticos na Irlanda do Norte a partir de 2014. Esse período abrangeria duas eleições gerais do Reino Unido, duas eleições para a Assembleia da Irlanda do Norte, o referendo da independência da Escócia, o referendo da UE e as eleições da UE e do governo local. Instamos o governo a implementar essa mudança na lei o mais rápido possível para garantir total transparência sobre essas eleições e referendos.*

Relatório Cairncross: um futuro sustentável para o jornalismo

235. Como dissemos em nosso Relatório Preliminar, o então Secretário de Estado, Rt Hon Matthew Hancock MP, nos disse que a avaliação Cairncross examinaria o papel da cadeia de suprimentos de publicidade digital, dentro de um contexto mais amplo do futuro da imprensa britânica, para indicar o quão justa e transparente é e se "incentiva a proliferação de notícias imprecisas e/ou enganosas". A consulta foi encerrada em setembro de 2018 ²⁶³ e o Relatório Cairncross foi publicado em 12 de fevereiro de 2019.

236. *Parabenizamos pelo relatório do Dame Frances Cairncross sobre a proteção do futuro do jornalismo e o estabelecimento de um código de conduta para reequilibrar o relacionamento entre provedores de notícias e redes sociais. Em particular, nós o parabenizamos com a recomendação de que jornais e revistas digitais on-line alcancem taxa zero de IVA, como ocorre com as versões impressas. Essa medida eliminaria o falso incentivo para as empresas de notícias se posicionarem contra o desenvolvimento de mais serviços digitais pagos. Concordamos com a recomendação de que nós deveríamos investigar a publicidade on-line, principalmente com o foco na principal empresa de pesquisa e rede social, pela Autoridade de Defesa da Concorrência e de Mercados.*

6 Influência estrangeira em campanhas políticas

Introdução

237. A velocidade do desenvolvimento tecnológico coincidiu com uma crise de confiança nas instituições e na mídia no Ocidente. Isso permitiu que países estrangeiros com intenção de desestabilizar instituições democráticas se aproveitassem dessa crise. Claramente, houve influência da Rússia nas eleições em eleições no exterior, esse fato foi comprovado. Em nosso Relatório Preliminar, destacamos as provas de tais tentativas sobre o referendo da UE; ²⁶⁴

238. É interessante notar que, em 30 de novembro de 2018, a resposta on-line do governo ao nosso relatório recebeu um total de 1.290 visualizações exclusivas e o PDF foi recebido 396 visitas

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

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

independentes no site.²⁶⁵ No mês seguinte à sua publicação, mais de 63% das visualizações do relatório on-line eram de endereços IP estrangeiros (enquanto, em média, 80% dos visualizadores de relatórios estão baseados no Reino Unido) e, destes, mais da metade era da Rússia. Além disso, dois terços dos leitores eram novos visitantes, o que significa que nunca haviam visitado o site parliament.uk antes (em comparação com o que ocorre com a maioria dos relatórios, em que apenas cerca de 30% são de novos visitantes). A tabela a seguir mostra as visualizações de página exclusivas por cidade, ilustrando essa alta proporção da Rússia:

	Cidade	Visualizações Únicas
1.	Moscou	19,79%
2.	Londres	17,3%
3.	São Petersburgo	2,94%
4.	Cambridge	2,25%
5.	Kiev	1,9%
6.	Sheffield	1,56%
7.	Bristol	1,38%
8.	Edinburgh	1,38%
9.	Novosibirsk	1,21%
10	Ottawa	1,21%

Fonte: Unidade de Publicações e Web, Câmara dos Comuns do Reino Unido

O mapa a seguir mostra a concentração desses leitores na resposta do governo ao Relatório Preliminar, por país:

[Imagem]

1 427

Isso por si só demonstra um interesse muito claro da Rússia no que tínhamos a dizer sobre suas atividades em campanhas políticas no exterior.

239. Neste capítulo, atualizaremos as informações incluídas em nosso Relatório Preliminar, incluindo o conhecimento do Facebook sobre a interferência russa em seus dados. Também completamos as recomendações que já havíamos apresentado.

Interferência russa nas eleições do Reino Unido

²⁶⁵ Essas estatísticas foram fornecidas pela Unidades de Publicações e Web, da Casa dos Comuns do Reino Unido. 'Único' significa que, se a mesma pessoa visitou uma página HTML/PDF várias vezes em uma sessão, ela contaria apenas como uma visualização. Não é possível acompanhar as leituras do PDF que tiveram origem fora do site Parliament.uk (por exemplo, quando o link para o PDF é compartilhado no Twitter), portanto esse número está sub-representado.

240. Como dissemos em nosso Relatório Preliminar, a primeira-ministra Theresa May acusou a Rússia de se intrometer nas eleições e disseminar desinformação, na tentativa de "armar informações" e semear discórdia no Ocidente.²⁶⁶ Em sua resposta ao Relatório, o governo declarou que, após o ataque com agente nervoso em Salisbury em março de 2018, o governo “constatou que o estado russo promoveu pelo menos 38 narrativas de desinformação falsas em torno desse ato criminoso”.²⁶⁷ No entanto, o governo deixou claro que “não viu evidências de uso bem-sucedido da desinformação por atores estrangeiros, incluindo a Rússia, para influenciar os processos democráticos do Reino Unido”.²⁶⁸

241. Quando o Secretário de Estado foi questionado sobre o que quer dizer o termo “bem-sucedido”, o deputado Hon Jeremy Wright, respondeu em seu depoimento: “Não encontramos nada que nos convença de que a interferência russa tenha tido um impacto significativo na maneira como as pessoas escolhem votar nas eleições. Não é que eles não tenham tentado, mas não encontramos evidências desse impacto significativo”²⁶⁹. Certamente é motivo de preocupação suficiente que o Governo tenha reconhecido que houve interferência, independentemente da falta de evidência acerca do impacto. O governo deve conduzir análises para entender a extensão do direcionamento de conteúdo pela Rússia aos eleitores durante as eleições.

242. O governo também não pode afirmar categoricamente que “não houve comprovação de que essa interferência tenha sido bem-sucedida” em nossos processos democráticos, pois não é possível definir o termo “bem-sucedido” de forma retroativa. No entanto, existem fortes evidências que apontam para atores estatais hostis influenciando processos democráticos. Cardiff University e o Digital Forensics Lab do Atlantic Council detalharam a forma em que o Kremlin tentou influenciar as atitudes na política do Reino Unido.²⁷⁰

243. A mídia alinhada ao Kremlin publicou um número significativo de artigos exclusivos sobre o referendo da UE. Os pesquisadores da 89Up analisaram o artigo mais compartilhado e identificaram 261 com um claro viés anti-UE para o relatório. As duas principais agências foram RT e Sputnik, com vídeo produzido por Ruptly.²⁷¹ Os artigos que mais viralizaram tiveram o maior viés anti-UE.²⁷² O alcance social desses artigos anti-UE publicados pelos canais de propriedade do Kremlin foi de 134 milhões de impressões em potencial, comparado com um alcance total de apenas 33 milhões e 11 milhões de impressões em potencial para todo o conteúdo compartilhado nos sites Vote Leave e [Leave.EU](#), respectivamente.²⁷³ O valor de uma campanha de mídia social paga comparável seria entre £1,4 e 4,14 milhões.

244. Em 17 de janeiro de 2019, o Facebook removeu 289 páginas e 75 contas do seu site, contas que tinham cerca de 790.000 seguidores e gastaram cerca de US\$ 135.000 em anúncios entre outubro de

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 Mesma referência acima.

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 é uma agência de notícias em vídeo pertencente à rede de notícias de televisão RT.

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.

2013 e janeiro de 2019. Os sites tinham sido administrados por funcionários da agência de notícias estatal russa Sputnik, que se apresentavam como um portal independente de notícias ou de interesse geral. Cerca de 190 eventos foram hospedados por essas páginas (a primeira foi agendada para agosto de 2015 e a mais recente, agendada para janeiro de 2019).²⁷⁴

245. Nathaniel Gleicher, chefe da política de segurança cibernética do Facebook, escreveu: “Apesar das deturpações das identidades, descobrimos que essas páginas e contas estavam vinculadas a funcionários da Sputnik, uma agência de notícias com sede em Moscou, e que algumas das páginas frequentemente postavam sobre assuntos como sentimentos anti-OTAN, protestos e combate à corrupção.”²⁷⁵ O Facebook também removeu 107 páginas, grupos e contas que foram criadas para parecer que foram executados a partir da Ucrânia, mas que faziam parte de uma rede com base na Rússia.

246. Ben Nimmo, do Digital Forensics Lab do Atlantic Council, detalhou as tentativas de influenciar as atitudes em relação ao referendo escocês, por exemplo, que inclui um observador eleitoral russo dizendo que o referendo não está de acordo com os padrões internacionais, e contas do Twitter que questionam sua legitimidade. Nimmo argumenta que o comportamento dessas contas é pró-Kremlin e é consistente com o comportamento das contas conhecidas, que são administradas pela chamada “fábrica de trolls” em São Petersburgo, na Rússia, durante as eleições presidenciais dos Estados Unidos a partir de 2016. No entanto, não é possível determinar a partir de fontes abertas se algumas ou todas as contas são atores independentes ou estão vinculadas a operações dos serviços de inteligência da Rússia.²⁷⁶

247. Como o Secretário de Estado disse, a Rússia também usou campanhas de influência digital maligna para minar a comunicação de evidências do governo após o envenenamento de Sergei Skripal e da sua filha.²⁷⁷ Uma pesquisa do Centro de Pesquisa e Evidência de Ameaças à Segurança da Cardiff University mostrou como as contas do Twitter de ‘marionetes’,²⁷⁸ controladas pela Agência de Pesquisa da Internet de São Petersburgo, tentaram alimentar divisões sociais, incluindo tensões religiosas, depois dos ataques terroristas de Westminster, Manchester, London Bridge e Finsbury Park.²⁷⁹ Além disso, os métodos pelos quais a influência maligna pode ser empregada também estão sendo constantemente expandidos. Embora o Twitter tenha sido se movido para encerrar contas abusivas e falsas, o Facebook continua resistindo a fazê-lo. Uma pesquisa do Instituto para Diálogo Estratégico do Programa Arena da LSE sobre as eleições da Alemanha em 2017 descobriu que os Grupos do Facebook foram criados por administradores não verificáveis, direcionando a mídia apoiada pelo Estado russo durante o período eleitoral, com regularidade, nas mídias sociais.²⁸⁰

248. O governo está muito disposto a aceitar as evidências da atividade russa no caso envolvendo Sergei Skripal, o que é razoável, diante das provas coletadas. No entanto, resiste em aceitar as evidências sobre a interferência no referendo de 2016 no Reino Unido. Se o governo deseja que o

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

²⁷⁵ Mesma referência acima.

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 Marionete é uma identidade online usada com a finalidade de promover enganação.

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.

público leve suas declarações a sério a respeito desses assuntos importantes para a segurança nacional e a nossa democracia, ele deve tratar a questão de forma imparcial, sem influência das implicações políticas de qualquer relatório.

249. Como ocorre com outros países, o Reino Unido está claramente vulnerável a campanhas secretas de influência digital, e o governo deve promover análises para entender a extensão do direcionamento dos eleitores por agentes estrangeiros, durante as últimas eleições. Perguntamos ao governo se a legislação atual seria suficiente para proteger o processo eleitoral da influência maligna. A legislação deve estar alinhada com os mais recentes desenvolvimentos tecnológicos e deve ser explícita sobre a influência ilegal sobre o processo democrático por atores estrangeiros. Instamos o governo a analisar esta questão e a responder em seu White Paper.

Facebook e a Campanha de Desinformação da Rússia

250. O Comitê perguntou repetidamente ao Facebook, por escrita e durante os depoimentos, sobre a atividade russa no Facebook e, em particular, sobre os anúncios russos exibidos durante as eleições presidenciais nos EUA em 2016. De acordo com um artigo do New York Times publicado em novembro de 2018, o ²⁸¹Facebook descobriu atividades suspeitas ligadas à Rússia em seu site no início de 2016, em uma tentativa de interromper as eleições presidenciais. Em setembro de 2017, Alex Stamos, o então Diretor de Segurança, disse aos membros do Conselho Executivo do Facebook que a atividade russa ainda não estava sob controle. O artigo afirmava que os executivos do Facebook, incluindo Mark Zuckerberg e Sheryl Sandberg, tentaram livrar a empresa deles desviando a atenção para outras empresas de tecnologia, contratando uma consultoria política, a Definers Public Affairs, supostamente para espalhar informações anti-semitas sobre George Soros e sua campanha. Soros chamou o Facebook de "uma ameaça à sociedade" no início de 2018.²⁸²

251. Quando Simon Milner, Diretor de Políticas para o Reino Unido, Oriente Médio e África, no Facebook, depôs em fevereiro de 2018, ele foi questionado especificamente se o Facebook havia identificado pessoas de um país que tentavam fazer anúncios políticos em outro país. Ele respondeu:

Não identificamos nas últimas eleições gerais, durante a votação do Brexit nem durante as eleições gerais de 2015, por jornalismo investigativo, por exemplo, que levou à sugestão de que muitas campanhas estão sendo realizadas, financiadas por pessoas de fora. [...] Não há indicação de que isso esteja acontecendo.²⁸³

252. Dadas as informações contidas no artigo do New York Times e as informações que recebemos da Six4Three, acreditamos que o Facebook sabia da existência de evidências de interferência no exterior e que o Simon Milner nos enganou quando testemunhou em fevereiro de 2018. O Diretor de Tecnologia do Facebook, Mike Schroepfer, também disse ao Comitê, com relação ao conhecimento da empresa sobre interferência russa nas eleições presidenciais de 2016, direcionando conteúdo para as contas de usuário no site: “Demoramos a entender o impacto disso na época”.²⁸⁴ Novamente, isso parece ser uma resposta enganosa, com base no que os executivos seniores do Facebook sabiam em 2016. Agora sabemos que essa afirmação simplesmente não era verdadeira. **Ficamos com a impressão de que Simon Milner e Mike Schroepfer enganaram o Comitê de forma deliberada, ou que eles**

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 a 425](#)

²⁸⁴ [Q2122](#)

não foram deliberadamente informados pelos executivos seniores do Facebook sobre a extensão da interferência russa nas eleições estrangeiras.

Endereços IP russos no Facebook

253. Os documentos da Six4Three revelaram que “um engenheiro do Facebook informou à empresa em outubro de 2014 que entidades com endereços IP russos estavam usando uma chave de API do Pinterest para obter mais de 3 bilhões de pontos de dados por dia por meio do sistema pago de API de amigos. Essa atividade não foi relatada a nenhum órgão externo na época”.²⁸⁵

254. Quando questionado sobre esses e-mails, Richard Allan se recusou a responder, afirmando que essas informações eram baseadas em mensagens de e-mail "não verificadas, a partir de levantamento parcial feito por uma fonte que tem uma inclinação particular".²⁸⁶ No entanto, na mesma noite de 27 de novembro de 2018, o próprio Facebook escolheu enviar as mesmas mensagens de e-mails a um repórter da CNN, apesar da descrição de Richard Allan.²⁸⁷ O Facebook queria mostrar que a investigação havia provado que não houve interferência russa. No entanto, a troca de e-mails mostra que a declaração do engenheiro de que não houve interferência russa foi dada dentro de uma hora, e é questionável se os engenheiros do Facebook teriam conseguido verificar tudo dentro desse curto prazo de modo a constatar que a interferência russa não teria ocorrido.

Dados do Facebook de propriedade do Centro de Psicometria da Cambridge University que foram compartilhados com APIs Russos

255. O ICO está investigando até que ponto os dados foram compartilhados entre a GSR - a empresa criada pelo Dr. Kogan, antes do seu trabalho envolvendo o aplicativo 'thisisyourdigitallife' — Cambridge University e APIs russas.²⁸⁸ Quando perguntado se o ICO ainda estava investigando para saber se os dados do Dr. Kogan foram acessados por pessoas na Rússia, a Comissária para Informação, Elizabeth Denham, afirmou:

Essa é uma linha ativa de investigação. O que dissemos em julho foi que havia alguns endereços de IP encontrados nesses dados e naquele servidor associado a Aleksandr Kogan que foram atribuídos a Rússia e estados associados. Essas são as informações que passamos às autoridades. Não é nosso objetivo investigar mais do que isso, mas repassamos isso para as autoridades competentes.²⁸⁹

Mais tarde, ela nos disse que o ICO havia encaminhado o assunto à Agência Nacional de Crimes.²⁹⁰

256. O Comissário Adjunto de Informações, James Dipple-Johnston, trouxe esclarecimentos adicionais. Destacou o fato de que os endereços IP originários da Rússia estavam conectados a um aplicativo anterior no Centro de Psicometria da Cambridge University. Os endereços IP também foram vinculados a supostos ataques cibernéticos no passado e a um "ponto de entrada do Tor" - um dispositivo para as pessoas esconderem sua identidade online.²⁹¹

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

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 e 3969](#)

Interferência russa por de outras redes sociais

257. A intromissão russa nas eleições no exterior, claramente, não se limitou apenas ao Facebook. Em outubro de 2018, o Twitter lançou um arquivo de tweets compartilhados por contas da Agência de Pesquisa na Internet, com o objetivo de "incentivar a pesquisa aberta e a investigação desses comportamentos de pesquisadores e acadêmicos de todo o mundo".²⁹² Os conjuntos de dados consistiam em 3.841 contas afiliadas à Agência de Pesquisa da Internet e com origem na Rússia, e 770 outras contas, "possivelmente com origem no Irã". As contas incluíram mais de 10 milhões de tweets e mais de 2 milhões de imagens.²⁹³ As contas do Twitter foram usadas para influenciar a eleição presidencial dos EUA de 2016, bem como eleições e referendos em vários outros países, incluindo o Reino Unido. As contas também foram usadas para influenciar o sentimento do público em torno de várias questões de importância nacional em outros países, incluindo a Ucrânia.

258. O Instituto para a Internet de Oxford e o Comitê Especializado em Inteligência do Senado trabalharam juntos para investigar as atividades da Agência de Pesquisa da Internet (IRA), estudando os dados fornecidos pelas empresas de tecnologia no verão de 2017.²⁹⁴ As investigações revelaram que: a campanha russa para polarizar o eleitorado dos EUA e desestabilizar a confiança na mídia começou em 2013, mais cedo do que se pensava anteriormente; e a IRA posteriormente acelerou a produção de conteúdo num conjunto completo de empresas de mídia social, com comportamentos similares no Twitter, Facebook, Instagram e YouTube.

259. Observamos também os comentários feitos por Vladislav Surkov, consultor sênior do Presidente Putin, em um artigo publicado no diário russo Nezavisimaya Gazeta, em 11 de fevereiro de 2019. Ele disse que "os políticos estrangeiros culpam a Rússia por se intrometer nas eleições e referendos em todo o planeta. De fato, é mais sério do que isso: A Rússia está se intrometendo em seus cérebros e eles não sabem o que fazer com a mudança de consciência".²⁹⁵

Leave.EU, Arron Banks, os EUA e a Rússia

Nosso Relatório Preliminar destacou o fato de que Arron Banks é, até o momento, a pessoa que, supostamente, fez a maior doação a uma campanha política na história britânica, anunciada como de £8,4 milhões, mas essas questões ainda se aplicam tanto sobre as fontes dessa doação como sobre a extensão da riqueza de Arron Banks.²⁹⁶

261. O Relatório registrou o fato de que Arron Banks tratou de empreendimentos comerciais na Rússia e em outros países, numa série de reuniões com funcionários da Embaixada da Rússia:

Arron Banks e Andy Wigmore enganaram o Comitê sobre o número de reuniões que ocorreram na Embaixada da Rússia, e saíram da audiência do Comitê para evitar o escrutínio do conteúdo das discussões travadas na Embaixada da Rússia. [...] Não está claro se Arron Banks obteve

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

²⁹³ Mesma referência acima.

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.

lucros com negócios resultantes de reuniões organizadas por autoridades russas.²⁹⁷

262. Nosso Relatório Preliminar recomendou que a Comissão Eleitoral buscasse investigações as doações que os Bancos Arron fizeram à campanha Leave, para verificar se o dinheiro não veio do exterior e que, “se houver alguma dúvida, o assunto deve ser encaminhado à Agência Nacional de Combate ao Crime”²⁹⁸ Em 1º de novembro de 2018, a Comissão Eleitoral encaminhou as seguintes organizações e indivíduos à Agência Nacional de Combate ao Crime: Better for the Country (a empresa que realizou a campanha do referendo Leave.EU); Arron Banks; Leave.EU; Elizabeth Bilney; e outras empresas e indivíduos associados. A investigação da Comissão Eleitoral centrou-se em £2 milhões que foram emprestados por Arron Banks e seu grupo de seguradoras para a Better for the Country, e outros £6 milhões foram dados para a organização, em nome do Leave.EU, individualmente por Arron Banks.²⁹⁹ A NCA abriu agora uma investigação criminal.

263. Pedimos à Agência Nacional de Combate ao Crime uma atualização sobre suas investigações, e eles responderam:

A NCA iniciou uma investigação sobre as entidades Better for the Country (BFTC) e Leave.EU; bem como Arron Banks, Elizabeth Bilney e outros indivíduos. Essa resposta veio depois da aceitação dos materiais encaminhados pela Comissão Eleitoral. Agora, essa é uma investigação em andamento e não podemos discutir detalhes operacionais.³⁰⁰

264. Na primavera de 2018, soubemos que Steve Bannon havia apresentado Arron Banks à Cambridge Analytica.³⁰¹ Em novembro de 2018, recebemos provas sobre a existência de um relacionamento entre o Leave.EU e Steve Bannon em 2015, evidenciado por um e-mail de Arron Banks para Andy Wigmore, com cópia para Steve Bannon e Elizabeth Bilney, mostrando que o Leave.EU queria que a Cambridge Analytica estabelecesse uma estratégia de financiamento nos EUA:

Gostaríamos que a Cambridge Analytica apresentasse uma estratégia para arrecadação de fundos nos Estados [...] e como poderíamos nos conectar com pessoas com laços familiares no Reino Unido, arrecadar dinheiro e criar atividades nas redes sociais.³⁰²

Arron Banks e Leave.EU não miravam apenas a Rússia, mas os EUA também.

265. O documento da Comissão Eleitoral, “Campanha Digital”, publicado em junho de 2018, destaca o fato de que as regras atuais sobre gastos foram estabelecidas em um período pré-digital:

As regras do Reino Unido estabelecem quantias mínimas para os gastos da campanha antes que pessoas ou organizações tenham que se registrar como promotores políticos não vinculados a um partido. Isso significa que um indivíduo ou organização estrangeiro que desembolsa esses valores não descumpra qualquer lei eleitoral específica no Reino Unido. [...] Não enxergava a possibilidade de fontes estrangeiras direcionarem publicidade de campanha paga para o Reino Unido”.³⁰³

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 Mesma referência acima, parágrafo 191.

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.

266. Estamos seguros de que a nossa recomendação que consta do Relatório Preliminar, de julho de 2018, a respeito de Arron Banks e sua doação, tenha sido aceita pela Comissão Eleitoral — que teme que Banks não seja a 'verdadeira origem' da doação — e pela Agência Nacional de Combate ao Crime, que atualmente está investigando a origem da doação.

267. Existe um princípio geral de que, sujeito a certos limites de gastos, o financiamento estrangeiro não é permitido nas eleições no Reino Unido. No entanto, como a Comissão Eleitoral deixou claro, as regras atuais não proíbem explicitamente os gastos no exterior. Recomendamos que, na primeira oportunidade, o Governo revise as regras atuais sobre o envolvimento estrangeiro em nossas eleições no Reino Unido para garantir que a interferência estrangeira nas eleições no Reino Unido, na forma de doações, não ocorra. Também precisamos deixar claro que o Facebook e todas as plataformas têm a responsabilidade de cumprir a lei e não facilitar atividades ilegais.

Outras investigações em andamento e denúncias criminais

268. Recentemente, fomos informados por Clint Watts, um especialista que conhecemos em Nova York em fevereiro de 2018, que as contas do Twitter monitoradas durante 2015 estavam discutindo o Brexit e a influência da campanha presidencial dos EUA.³⁰⁴ Além disso, no mesmo mês em que o Twitter divulgou seu arquivo de tweets compartilhados por contas da Agência de Pesquisa na Internet, o Departamento de Justiça dos EUA apresentou acusações criminais contra uma cidadã russa, Elena Alekseevna Khusyaynova, por supostos crimes relacionados à interferência entre o período da eleição presidencial dos EUA de 2016 e as eleições minoritárias de 2018.³⁰⁵

269. O FBI também apresentou uma queixa criminal em 28 de setembro de 2018. Descreveu o trabalho do 'Projeto Lakhta', em qual indivíduos supostamente “se envolveram em operações de interferência política e eleitoral direcionada a populações dentro da Federação Russa e em vários outros países, incluindo, entre outros, os Estados Unidos, membros da União Europeia e Ucrânia”.³⁰⁶ Desde pelo menos maio de 2014, o objetivo declarado do Projeto Lakhta nos Estados Unidos era espalhar desconfiança em relação aos candidatos a cargos políticos e ao sistema político em geral”.³⁰⁷ A queixa também abrangeu 14 empresas — que se acredita serem empresas de fachada — envolvidas na conspiração³⁰⁸

270. Em 31 de janeiro de 2018, o Facebook anunciou a suspensão de uma rede de contas — 783 páginas, grupos e contas — que, segundo a empresa, apresentava comportamento não autêntico coordenado no Facebook e no Instagram “controlado a partir do Irã”. Quase simultaneamente, o Twitter anunciou que havia suspenso redes de contas que chamou de “operações de agências estrangeiras de inteligência”, potencialmente conectadas ao Irã, Venezuela e Rússia.³⁰⁹

271. As operações de inteligência fazem parte de um grupo complexo e inter-relacionado de ações que promovem confusão e agitação por meio de sistemas de informação, como empresas de mídia social. Essas empresas, em particular o Facebook, precisam agir contra administradores de

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 Mesma referência acima.

³⁰⁸ Mesma referência acima.

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

grupos não transparentes, que estão sendo usados para campanhas políticas. Eles também precisam impor uma punição muito mais rigorosa aos usuários que abusam do sistema. Apenas ter uma conta falsa de desinformação encerrada, mas ser capaz de abrir outra no momento seguinte, dificilmente será suficiente para evitar que volte a ocorrer.

272. O governo deve pressionar as empresas de mídia social para divulgar quaisquer casos de desinformação. O governo precisa garantir que as empresas de mídia social compartilhem as informações que têm sobre interferência estrangeira em seus sites — incluindo quem pagou por anúncios políticos, quem visualizou os anúncios e quem clicou nos anúncios — sob pena de serem responsabilizados financeiramente se essas informações não forem disponibilizadas. Os certificados de segurança, contas autenticadas nas redes sociais, garantiriam que uma pessoa real estivesse por trás das opiniões expressas na conta.

273. Renovamos nosso pedido ao governo para informar quantas investigações estão sendo realizadas atualmente sobre interferência russa na política do Reino Unido. Recomendamos ainda que o Governo inicie uma investigação independente sobre eleições passadas — incluindo a eleição do Reino Unido de 2017, o Referendo do Reino Unido de 2016 e o Referendo da Escócia de 2014 — para esclarecer o que realmente aconteceu com relação à influência estrangeira, desinformação, financiamento, manipulação de eleitores e compartilhamento de dados, para que as mudanças cabíveis na lei possam ser promovidas e as lições possam ser aprendidas para futuras eleições e referendos.

7. Influência da SCL em eleições estrangeiras

Introdução

274. As empresas de análise de dados têm desempenhado um papel fundamental nas eleições em todo o mundo. As empresas de comunicação estratégica frequentemente realizam campanhas em nível internacional, que são financiadas por meios menos transparentes e empregam métodos legalmente duvidosos. Como escrevemos em nosso Relatório Preliminar, levantamos preocupações sobre a complexa rede de relacionamentos entre o grupo de empresas SCL (Strategic Communications Laboratories) e "essas preocupações só aumentadas pelos vínculos existentes entre Alexander Nix e SCL com organizações envolvidas nas forças armadas e nos setores de defesa, inteligência e segurança".³¹⁰

275. Destacamos as seguintes campanhas eleitorais e referendos em que a SCL Elections e empresas associadas estiveram envolvidas: Austrália; Brasil; República Checa; França; Gâmbia; Alemanha; Gana (2013); Guiana; Índia; Indonésia; Itália; Quênia (campanhas Kenyatta de 2013 e 2017); Kosovo; Malásia; México; Mongólia; Níger; Nigéria; Paquistão; Peru; Filipinas; Eslováquia; São Cristóvão e Neves; Santa Lúcia; São Vicente e Granadinas; Tailândia; Trinidad e Tobago; e o Reino Unido. De acordo com os depoimentos que ouvimos, a SCL também pode ter trabalhado nas campanhas eleitorais para prefeito em Buenos Aires em 2015, para Mauricio Macri.³¹¹

276. Após a publicação do nosso Relatório Preliminar, tanto o Alto Comissário de Malta quanto a empresa de RP de Chelgate escreveram ao Comitê, negando as declarações que constavam do Relatório Preliminar de que o Partido Trabalhista de Malta mantinha relações com o Grupo SCL "por

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](#)).

vários anos antes das eleições de 2013". Entendemos, no entanto, que a SCL com certeza realizou reuniões em Malta, que Christian Kalin, da Henley & Partners, foi apresentado por Joseph Muscat pela SCL em 2011, e que Christian Kalin se reuniu com os dois partidos antes de 2013.³¹²

Mais informações sobre o trabalho da SCL

277. Como dissemos em nosso Relatório Preliminar, as Eleições da SCL e suas empresas associadas, incluindo a Cambridge Analytica, trabalharam em campanhas que não eram financiadas de maneira transparente, ultrapassando as fronteiras legais e éticas.

278. Nosso Relatório Preliminar descreveu a relação entre o trabalho de campanha da SCL Elections e Christian Kalin, presidente da Henley & Partners:

Fomos informados de que, por trás de grande parte do trabalho de campanha da SCL Elections estava a mão oculta de Christian Kalin, Presidente da Henley & Partners, que fez com que investidores financiassem as campanhas e, em seguida, preparou a SCL para escrever seu manifesto e supervisionar todo o processo da campanha. Em troca, Alexander Nix nos disse que a Henley & Partners obteria direitos de passaporte exclusivos daquele país, sob um programa de cidadania por investimento (CBI). A relação entre Alexander Nix e Christian Kalin foi descrita como um 'pacto faustiano'. Com os direitos exclusivos de passaporte, veio um governo que seria favorável ao Sr. Kalin e seus clientes.³¹³

Oportunidades de cidadania por investimento

279. Atualmente, a Henley & Partners gerencia esquemas de 'cidadania por investimento' em vários países, incluindo Malta, Moldávia, Santa Lúcia, São Cristóvão e Neves e Granada. Os passaportes do Caribe permitem o acesso sem visto a 130 países, incluindo o Reino Unido e a muitos estados europeus. Os passaportes emitidos por Malta permitem o acesso a todos os países europeus — o Programa de Investidores Individuais (IIP) de Malta foi inaugurado no início de 2014, o primeiro desse tipo a ser reconhecido pela Comissão Europeia.³¹⁴ Muitos desses passaportes são emitidos para residentes da Rússia, China e do Oriente Médio. Um artigo recente do Guardian descreveu o trabalho da Henley & Partners, descrevendo a maneira pela qual estrangeiros podem se tornar cidadãos de um país em que nunca viveram, em troca de doações para um fundo nacional:

Henley ganhou dezenas de milhões de dólares com esse comércio, e seu primeiro grande cliente foi o governo de São Cristóvão. E enquanto caía a estrela de Nix, Kalin e sua indústria estão em alta — e estão sendo cada vez mais investigados. [...] Por algumas centenas de milhares de dólares, o passaporte certo, do lugar certo, pode levar seu dono a quase qualquer país. Pelo valor, comerciantes legítimos acham que vale a pena. Mas, além disso, a polícia receia que criminosos e empresários buscam esse caminho para fugir de sanções³¹⁵

280. Houve uma pressão renovada da União Europeia para regulamentar os esquemas de residência por investimento (descritos como 'golden visas') e cidadania por investimento (descritos como 'golden passports'). A concessão de residência a investidores estrangeiros, em troca de passaportes, está sujeita a “riscos de segurança, riscos de lavagem de dinheiro e corrupção e sonegação de impostos. Tais riscos

³¹² Confidential evidence shown to the Committee.

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](#), MaltaImmigration.com, accessed 3 February 2019.

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

são ampliados pelos direitos transnacionais associados a cidadania na União Europeia.³¹⁶ Em janeiro de 2019, a Comissão Europeia publicou um relatório, “Cidadania dos investidores e regimes de residência na União Europeia”, levantando essas preocupações.³¹⁷

281. Em nosso Relatório Preliminar, destacamos o trabalho realizado pela SCL para vencer as eleições gerais de 2010 em São Cristóvão e Neves, que incluíram uma operação contundente, com a Líder da Oposição, Lindsay Grant, sendo oferecido suborno por um agente disfarçado que se apresentava como investidor imobiliário. Alexander Nix nos disse que Christian Kalin também estava executando um programa de cidadania por investimento em São Cristóvão e Neves na época.³¹⁸

282. Em 2014, o Reino Unido emitiu um aviso de que 'atores ilegais' estavam comprando passaportes “com o objetivo de evitar sanções americanas ou internacionais ou para se envolver em outros crimes financeiros”.³¹⁹ Esse anúncio teve origem, em parte, no fato de São Cristóvão e Neves terem removido a informação sobre o "Local de Nascimento" dos seus passaportes, e os EUA estavam preocupados com o esquema. Entre as pessoas que adquiriram passaportes de São Cristóvão e Neves estão as seguintes pessoas:

- Ali Sadr Hasheminejad: iraniano, adquiriu o passaporte SKN por intermédio da Henley & Partners em 2009; preso pelos EUA em março de 2017 por irregularidades envolvendo sanções a lavagem de dinheiro e pagou fiança em maio; atualmente sujeito a monitoramento eletrônico e toque de recolher; seu banco maltês, Pilatus, teve sua licença revogada em outubro de 2018, por lavagem de dinheiro.³²⁰
- Houshang Hosseinpour, Houshang Farsoudeh e Pourya Nayebi: iranianos, adquiriram passaportes SKN em novembro de 2011, dezembro de 2011 e novembro de 2012, respectivamente; usaram seus passaportes SKN para adquirir um banco na Geórgia; todos os três homens foram alvo de sanção dos EUA em 2014;³²¹
- Ren Biao: chinês que obteve seu passaporte SKN em setembro de 2013; mudou-se para a SKN com sua família em 2014, depois que a China emitiu um aviso vermelho da Interpol. Era procurado por supostamente ter obtido US\$ 100 milhões por fraude a instituições estatais;³²²
- John Babikian, fugiu do Canadá em 2012, acusado de sonegação de impostos, portador de um passaporte SKN, processado pela Securities and Exchange Commission dos EUA em 2014 por fraude em ações, multado em US\$ 3 milhões.³²³

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.

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.

283. A Henley & Partners esteve envolvida em ajudar a financiar as eleições em São Cristóvão e Neves, oferecendo e pagando pelos serviços da SCL e executando a parceria de cidadania econômica do governo.³²⁴ A SCL fazia parte do pacote, oferecido pela Henley & Partners, que questiona se a Lei de Suborno do Reino Unido é suficiente para promover um freio regulatório sobre o mau comportamento no exterior. Segundo uma fonte sênior do Partido Trabalhista de São Cristóvão e Neves, o Sr. Nix afirmou que, embora a empresa SCL tenha entrado em processo de falência, as pessoas que trabalham lá são as mesmas e estavam disponíveis para prestar serviços ao gerenciamento de campanhas.³²⁵

284. A Henley & Partners nega o financiamento direto de qualquer campanha eleitoral no Caribe envolvendo cidadania por investimento enquanto a SCL mantinha atividade na região. Uma carta da Global Citizens, em nome da Henley & Partners, foi enviada ao Comitê em dezembro de 2018, declarando: “É natural que haja uma certa interação entre os inúmeros assessores e consultores. É totalmente incorreto, no entanto, sugerir que a Henley & Partners tivesse qualquer tipo de envolvimento formal com a SCL”.³²⁶

285. No final de julho de 2018, quando publicamos nosso Relatório Preliminar, Alexander Nix renunciou ao cargo de diretor do grupo de empresas SCL/Cambridge Analytica, que haviam ingressado com pedido de falência no Reino Unido e falência sob o Capítulo 7 nos EUA.

286. No entanto, Alexander Nix permanece como acionista da Emerdata, sua matriz britânica — constituída em agosto de 2017, como parte de uma reorganização do grupo. A Emerdata não está em processo de falência. Continua sendo uma empresa ativa e possui uma ampla base de acionistas. De acordo com os últimos registros, por sua vez, é de propriedade majoritária da Cambridge Analytica Holdings LLC, uma empresa sediada em Delaware.³²⁷

287. Surgiram poucas informações novas e substanciais no processo de falência, exceto a preocupação causada pelo fato de que - após o escândalo - os administradores não conseguiram resgatar as empresas do Reino Unido. A Emerdata continua sendo de longe o maior credor, ocupa o primeiro lugar no comitê oficial de credores e vem pagando valores elevados pela sua administração.³²⁸

288. Da mesma forma, poucas informações novas surgiram dos processos sob o Capítulo 7 envolvendo as antigas empresas operacionais dos EUA. Desde então, um grupo de usuários do Facebook ingressou com uma ação coletiva na justiça por violação de privacidade. Em janeiro deste ano, um tribunal de Nova York determinou que Julian Wheatland - ex-presidente do grupo SCL e atual diretor de operações da Emerdata - entregasse os documentos solicitados no processo.³²⁹

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.

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

³²⁷ Os registros apresentados à Junta de Registro Comercial em nome da Emerdata Limited. Os atuais diretores da empresa são Jennifer e Rebekah Mercer (filhas do capitalista Robert Mercer, que atua em círculos políticos conservadores dos EUA), Gary Ka Chun Tiu, com sede em Hong Kong, e Julian Wheatland, com sede no Reino Unido. Em 10 de agosto de 2018, os acionistas eram Cambridge Analytica Holding LLC; Alexander Tayler; Julian Wheatley; trust tendo como beneficiários de Rebekah, Jennifer e Heather Mercer; Alexander e Catherine Nix; Jonathan, Domenica, Allegra, Marcus e Hugo Marland; JP Marland & Sons Ltd; Henry e Roger Gabb; Nigel e 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; e 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

289. Assim como a Emerdata (e sua empresa mãe de Delaware), uma antiga empresa do grupo SCL no Reino Unido - SCL Insight Limited - também permanece ativa. Com sede em Londres, pertence ao co-fundador do grupo, Nigel Oakes, passando por um processo de cisão durante a reorganização em 2017.

290. Seguindo as instruções do Secretário de Estado dos Negócios, Energia e Estratégia Industrial (BEIS), o Serviço de Falência atualmente está investigando as ações dos diretores da SCL Elections Ltd, SCL Group Ltd, SCL Analytics Ltd, SCL Commercial Ltd, SCL Social Ltd e Cambridge Analytica (UK) Ltd, de acordo com os dispositivos da Lei de Desqualificação de Diretores de Empresas de 1986.

Conflitos de interesse

291. O problema com muitas empresas de comunicação estratégica é o fato de elas trabalharem em campanhas não apenas antiéticas e possivelmente ilegais, mas também o fato de trabalharem contra os interesses nacionais da segurança do Reino Unido com campanhas para atores estatais privados ou hostis, que estão em conflito, ou que discordam com a política externa do Reino Unido. As evidências nos dados da AIQ enviados por Chris Vickery sugerem que a AIQ estava trabalhando ou planejando trabalhar numa campanha política para o partido Osnova na Ucrânia. O Partido Osnova foi criado pelo político e empresário Serhiy Taruta. De acordo com um artigo do Atlantic Council, Serhiy Taruta afirmou que a maioria dos ucranianos não apoia a OTAN, contrariando o resultado de outras pesquisas. O mesmo artigo diz que Osnova defende "concessões" aos vizinhos da Ucrânia.³³⁰

292. Quando perguntamos a Jeff Silvester, CEO da AIQ, sobre Osnova e se a AIQ estava trabalhando nas eleições ucranianas de 2019, Silvester respondeu: “Osnova é um partido político na Ucrânia. Temos um cliente para quem criamos um aplicativo Android e iOS, e eles estão trabalhando com o Osnova ”.³³¹ A Ucrânia é um país profundamente importante para o Ministério da Defesa do Reino Unido e o Ministério das Relações Exteriores e de Assuntos do Commonwealth. O interesse é o de proteger a sua segurança nacional diante da agressão russa.

293. Em nosso Relatório Preliminar, declaramos:

Igualmente preocupante é o fato de o Grupo SCL ter realizado trabalhos “para o governo britânico, o governo dos EUA e outros governos aliados”. Significava que Alexander Nix e o grupo SCL e empresas associadas estavam trabalhando para o governo do Reino Unido, além de trabalhar em campanhas para outros países. Alexander Nix também nos disse que Christian Kalin estava trabalhando para o governo do Reino Unido ao mesmo tempo. Publicamos uma aprovação da SCL pelo Ministério da Defesa, depois que a SCL ofereceu treinamento em operações psicológicas para a equipe do MOD, que revelou que a SCL recebeu informações sigilosas sobre operações em Helmand, Afeganistão, baseado nas suas credenciais de segurança. Alexander Nix explicou que a SCL “é uma empresa que atua no setor governamental e de defesa, atua como empresa detentora de credenciais para trabalhos sigilosos”.³³²

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).

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

³³¹ [Q3130](#) e [Q3131](#).

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

Esse fato fundamenta um profundo questionamento. As empresas que trabalham em campanhas eleitorais no exterior dessa maneira também devem desenvolver projetos do Ministério da Defesa do Reino Unido e do Ministério de Relações Exteriores e de Assuntos do Commonwealth?

294. Quando Brittany Kaiser presetou seu depoimento na primavera de 2018, ela discutiu a natureza porosa entre as ações comerciais, políticas e de defesa da SCL. Disse que, antes de 2015, a metodologia de 'análise do público-alvo' (TAA) era considerada uma arma - "táticas de comunicação como armas" - e tinham que ter informado ao governo do Reino Unido se seria implantado em outro país.³³³

295. Emma Briant, professora sênior da University of Essex, apoia uma regulação mais rigorosa das empresas de comunicações estratégicas, com o estabelecimento de licenças profissionais que podem ser revogadas, se necessário. Esse licenciamento “protegeria comercialmente o próprio setor, criando um benefício econômico resultante de 'soft power' para o setor e para os governos ocidentais”.³³⁴ Ela deu dois exemplos dos conflitos de interesses identificados no caso da Cambridge Analytica: A Cambridge Analytica trabalhou para a Lukoil, uma empresa petrolífera russa com conexões políticas bem abrangentes, enquanto, ao mesmo tempo, o Grupo SCL estava fornecendo treinamento contra propaganda russa para a OTAN. “Na mesma época, Alexander Nix, da Cambridge Analytica, entrou em contato com Julian Assange, do Wikileaks, ampliando a liberação de emails nocivos; a Rússia foi acusada de ter hackeado essas mensagens, mas nega”.³³⁵

296. Conforme declaramos, a Emerdata é o principal credor da SCL Elections Ltd e tem pagado valores elevados pela sua administração.³³⁶ Visto que muitos funcionários seniores da SCL Elections Ltd/Cambridge Analytica possuem posição de destaque na Emerdata, existe o receio de que o trabalho da Cambridge Analytica continue, embora com nome diferente. ***Declaramos em nosso Relatório Preliminar que “o Grupo SCL e as empresas associadas entrarem em processo de falência, mas outras empresas estão realizando trabalhos semelhantes. Executivos seniores envolvidos com a SCL e a Cambridge Analytica parecem ter mudado para novos veículos corporativos”.***³³⁷ ***Recomendamos que “a Agência Nacional de Combate ao Crime, se ainda não o estiver fazendo, investigue as conexões entre a empresa SCL Elections Ltd e a Emerdata Ltd.”***³³⁸ ***Repetimos essas recomendações neste relatório.***

297. Em outubro de 2018, o Secretário de Estado do DCMS, Rt Hon Jeremy Wright MP, foi questionado pelo Comitê se a legislação atual do Reino Unido relativa a empresas de lobby como a SCL era adequada para esse fim. Ele não foi sincero em sua resposta, afirmando que o ICO deveria investigar o trabalho da SCL. “Penso que essa investigação nos trará uma indicação, primeiramente, se algo saiu errado neste caso, além de indicar, em caso afirmativo, se isso indica uma fraqueza estrutural que precisamos resolver”.³³⁹ Ele não respondeu ao questionamento específico, não disse se a lei relativa a empresas de lobby, como a SCL, era adequada para esse fim. Acreditamos que ela não é adequada; a atual autorregulação das empresas de lobby não está funcionando.

³³³ [Q1560](#)

³³⁴ [FKN0099](#)

³³⁵ Mesma referência acima.

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.

298. *Recomendamos que o governo busque maneiras pelas quais as empresas de relações públicas e comunicações estratégicas sejam auditadas, possivelmente por um órgão independente, para garantir que suas campanhas não entrem em conflito com os interesses nacionais do Reino Unido e com as questões de segurança, e não obstruam a imposição de sanções legítimas, como é o caso atual da venda legal de passaportes. É necessário impor barreiras para garantir que essas empresas não possam trabalhar em projetos sensíveis do governo do Reino Unido e com clientes cuja intenção possa ser o enfraquecimento desses interesses.*

299. *A transformação da Cambridge Analytica em Emerdata ilustra como é fácil para empresas desacreditadas se reinventarem e preservarem sua capacidade de fazer uso dos mesmos dados e de empregar as mesmas táticas para enfraquecer os governos, inclusive no Reino Unido. O setor precisa de uma limpeza minuciosa. É o que revelou o escândalo da SCL/Cambridge Analytica, exemplos de práticas irregulares praticadas no exterior ou para clientes estrangeiros, com o risco de ingressar na política britânica. Atualmente, o setor de comunicações estratégicas está sujeito, basicamente, a auto-regulação. O governo do Reino Unido deve considerar novas leis que reduzam o comportamento irregular nesse setor.*

300. *É preciso haver transparência nessas empresas estratégicas de comunicação, com um registro público de todas as campanhas para as quais trabalham, tanto nacionais como no exterior. Elas precisam ser responsabilizadas por descumprir as leis durante campanhas em qualquer lugar do mundo, ou por trabalhar em campanhas não transparentes do ponto de vista financeiro. Recomendamos que o governo enfrente essa questão, quando responder à sua consulta, 'Protegendo o Debate: Intimidação, Influência e Informação*

301. *Recomendamos que o governo reveja a Lei de Suborno do Reino Unido, para avaliar se a legislação é suficiente para impor um freio regulatório sobre o mau comportamento no exterior. Também buscamos o governo para explorar a viabilidade de adotar uma versão no Reino Unido da Lei de Registro e Representação Estrangeira dos EUA (FARA), que exige que “pessoas que atuam como representantes de entidades estrangeiras com capacidade política ou quase-política devem elaborar uma divulgação pública periódica acerca dos seus relacionamentos com o seu contratante estrangeiro, bem como as atividades, recebimentos e gastos relacionados a tais atividades”.*

8 Educação digital

Introdução

302. É difícil estabelecer a diferença, no mundo das redes sociais, entre conteúdo verdadeiro, enganoso ou falso, especialmente quando essas mensagens são enviadas em nível individual. Crianças e adultos precisam estar equipados com as informações e capacidade crítica necessárias para entender o conteúdo das redes sociais, descobrir o que é correto e confiável e o que não é. Além disso, as pessoas precisam estar cientes dos direitos que possuem sobre seus próprios dados pessoais e o que devem fazer quando quiserem que seus dados sejam removidos.

303. A maioria das nossas testemunhas enfatizou a necessidade de mais educação digital entre os usuários das redes sociais. Por lei, a Ofcom tem a atribuição de promover a educação sobre uso de mídias, para ampliar “a capacidade de usar, compreender e criar mídia e comunicação em diversos contextos”. Sharon White nos disse que as ações de educação digital realizadas se baseiam principalmente em pesquisas, “sobre como as crianças usam e entendem a Internet, e o mesmo vale

para os adultos".³⁴⁰ Nunca é demais enfatizar a importância de uma maior compreensão pública sobre a informação digital - seu uso, escala, importância e influência.

304. Uma maior compreensão do público sobre o que as pessoas leem nas redes sociais tem sido ajudada por organizações que trabalham para alcançar uma maior transparência no conteúdo. Por exemplo, os jornalistas da empresa NewsGuard avaliam os websites de notícias e informações com base em nove critérios - uma forma de 'Tabelas de Valor Nutricional', explicando a história de cada site, quem são os donos, de onde vem o financiamento e o nível de transparência. Em janeiro de 2019, a Microsoft integrou as avaliações do NewsGuard em seu navegador móvel Edge.³⁴¹

305. Ouvimos também os representantes da Disinformation Index, uma organização que atribui uma nota para cada canal, indicando a probabilidade de que esse canal esteja promovendo desinformação: "Da mesma maneira que as agências de classificação de risco classificam países e produtos financeiros com AAA como de baixo risco, até o nível de Lixo, para os investimentos mais arriscados, o mesmo ocorre com os meios de comunicação".³⁴²

306. A impressão é que o Facebook quer enfrentar a desinformação em seu site. Em janeiro de 2019, o Facebook empregou o Full Fact para revisar e avaliar a precisão das notícias veiculadas no Facebook - incluindo a produção de relatórios de avaliação a cada três meses - como parte do seu programa de verificação independente de fatos, na primeira vez em que essa iniciativa foi realizada no Reino Unido.³⁴³ No entanto, como descrevemos no Capítulo 5, o Facebook também bloqueou recentemente o trabalho de organizações como a Who Targets Me?, que auxiliavam o público a entender como e por que eles estão sendo alcançados com anúncios on-line. **Por um lado, o Facebook dá a impressão de trabalhar em prol da transparência, no que diz respeito à auditoria do seu conteúdo de notícias; por outro lado, porém, ocorre uma ofuscação considerável em relação à auditoria dos seus anúncios, responsável pelo faturamento em constante crescimento do Facebook. Para tomar uma decisão consciente sobre os anúncios que lhes são apresentados no Facebook, os usuários precisam ver a fonte e o objetivo por trás do conteúdo.**

307. Elizabeth Denham descreveu a campanha "Your Data Matters" do ICO, em andamento desde abril de 2018: "É uma campanha em andamento e acho que foi responsável por um aumento de reclamações, feitas por mais pessoas, contra empresas e contra nós".³⁴⁴ Ela também enfatizou a necessidade de o público entender seus direitos e também de se "tornarem cidadãos mais educados digitalmente para que saibam navegar na Internet e possam exercer seus direitos". O Comissário de Informação disse que o ICO tinha um papel a desempenhar, mas não tinha necessariamente os recursos.³⁴⁵

308. Em nosso Relatório Preliminar, recomendamos que o governo apresente propostas em seu White Paper para que uma taxa para educação seja cobrada das empresas de mídia social, para financiar uma estrutura abrangente on-line, garantindo que a educação digital seja tratada como o quarto pilar da educação, ao lado de leitura, escrita e matemática.³⁴⁶ Em sua resposta, o Governo afirmou que ainda estava reunindo informações para tomar uma decisão sobre a melhor abordagem acerca da imposição

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.

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.

de qualquer taxa sobre as empresas, e não gostaria de prejudicar o trabalho atualmente realizado por instituições de caridade e outras organizações que combatem danos praticados on-line. Não concordou que a educação digital deveria ser o quarto pilar da educação, uma vez que "já é ensinado em todo o currículo escolar nacional".³⁴⁷

Atrito no sistema

309. O termo 'atrito' representa qualquer coisa que diminui a velocidade de um processo ou função. Em 2011, Mark Zuckerberg anunciou que os aplicativos não gerariam mais mensagens pop-up, perguntando aos usuários se eles gostariam de publicar suas atividades mais recentes em seu feed do Facebook; em vez disso, o Facebook criou aplicativos capazes de postar diretamente nos feeds dos usuários, sem necessidade de permissão. Zuckerberg disse: "daqui em diante, será uma experiência sem atritos".³⁴⁸

310. Alguns acreditam que o atrito deve ser reintroduzido na experiência on-line, tanto pelas empresas de tecnologia quanto pelos próprios usuários, a fim de reconhecer a necessidade de fazer uma pausa e pensar antes de produzir ou consumir conteúdo. Existe uma tendência de pensar na educação digital como sendo de responsabilidade daqueles que ensinam e dos que aprendem. No entanto, os algoritmos também podem desempenhar um papel importante na educação digital. O 'atrito' pode ser incorporado ao sistema, para dar mais tempo para as pessoas pensarem sobre o que estão escrevendo e o que estão compartilhando, para que possam ter a opção de limitar o tempo que passam online; deveria haver obstáculos para tornar o processo de postagem ou compartilhamento mais ponderado ou mais lento. Por exemplo, esse atrito extra poderia incluir: a opção de compartilhar uma publicação ou um comentário apenas se o usuário escrever sobre a publicação; a opção de compartilhar uma postagem somente depois lê-la na íntegra; e uma maneira de monitorar o que está prestes a ser enviado, antes de ser enviado.³⁴⁹

311. O Centro para a Tecnologia Humana sugere medidas simples que podem ser adotadas pelos próprios usuários, para aumentar o atrito em dispositivos móveis, incluindo: desativar todas as notificações, sem prejudicar o relacionamento com as pessoas; alterar a cor da tela para 'escala de cinza', reduzir a intensidade e a atração de cores brilhantes; manter a tela inicial apenas com ferramentas; digitar o nome dos aplicativos para abrir; manter carregadores fora do quarto; remover redes sociais de dispositivos móveis; e telefonar em vez de enviar mensagens de texto.³⁵⁰

Reguladores e educação digital

312. *Como escrevemos em nosso Relatório Preliminar, a educação digital deve ser o quarto pilar da educação, juntamente com a leitura, escrita e matemática. Na resposta do governo, não avalia a nossa recomendação de impor uma taxa sobre as empresas de mídia social, a ser usada, em parte, para financiar uma estrutura educacional abrangente - desenvolvida por instituições de caridade, ONGs e os próprios reguladores - e promovida de forma online. Essa estrutura seria utilizada para informar as pessoas sobre as implicações de se disporem a compartilhar os seus dados, os direitos das pessoas sobre os dados e as maneiras pelas quais elas podem se engajar e interagir construtivamente com as redes sociais. As pessoas precisam se manter atentas no relacionamento com essas empresas, principalmente sobre o que leem e o que escrevem. Reiteramos esta*

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.

³⁵⁰ Mesma referência acima.

recomendação ao Governo e aguardamos resposta.

313. O público precisa saber mais sobre sua capacidade de denunciar campanhas digitais que acreditem ser enganosas e/ou ilegais. A Ofcom, a ASA, a OIC e a Comissão Eleitoral precisam ter mais visibilidade para que as pessoas conheçam os seus serviços e atribuições. O governo deveria assumir um papel de liderança na coordenação desse serviço crucial para o público. O governo deveria promover o esclarecimento da população sobre os seus direitos no relacionamento com as empresas de mídia social.

314. Os usuários das redes sociais precisam de ferramentas on-line para ajudá-los a distinguir entre jornalismo de qualidade e histórias provenientes de organizações vinculadas à desinformação ou consideradas fontes não confiáveis. As empresas de mídia social devem ser obrigadas a desenvolver ferramentas como essas para si mesmas ou trabalhar com prestadores de serviço existentes, como o Newsguard, para disponibilizar esses serviços para seus usuários. Exigir que as empresas de mídia social adotem essas medidas pode fazer parte de um novo sistema de regulamentação de conteúdo, com base num código legal, e sob supervisão de um regulador independente, como discutimos anteriormente neste relatório.

315. As empresas de mídia social precisam ser mais transparentes sobre seus próprios sites e como eles funcionam. Em vez de se esconder atrás de contratos complexos, elas devem informar aos usuários como seus sites funcionam, incluindo as funções de administração de conteúdo, e a maneira como os algoritmos são usados para priorizar determinadas histórias, notícias e vídeos, dependendo do perfil de cada usuário. Quanto mais as pessoas souberem como os sites funcionam e como os sites usam os dados dos indivíduos, mais informados estaremos, o que, por sua vez, terá mais facilidade para tomar decisões sobre o uso e a privacidade dos sites.

316. A Ofcom, o ICO, a Comissão Eleitoral e a Autoridade de Padronização de Publicidade escreveram separadamente sobre seu papel na promoção da educação digital. Recomendamos que o governo garanta que os quatro principais reguladores produzam uma estratégia mais unificada em relação à educação digital. Incluída nesta abordagem unificada, deve haver uma discussão pública sobre como nós, como indivíduos, concordamos com o uso e compartilhamento dos nossos dados. As pessoas precisam saber como seus dados estão sendo usados (com base nas recomendações estabelecidas no capítulo dois deste Relatório Final). Os usuários precisam saber como definir os limites que desejam e como esses limites devem ser definidos no que diz respeito aos seus dados pessoais. Esse debate deve incluir os argumentos a favor da vontade de os usuários quererem definir uma expectativa básica de privacidade, como ocorre no campo básico da higiene. Os usuários podem optar por abrir mão desse padrão mínimo, se quiserem.

317. Recomendamos que a participação nas redes sociais permita mais pausas para reflexão. Mais obstáculos ou 'atritos' deveriam ser incorporados às redes sociais e nas próprias atividades dos usuários - para dar às pessoas tempo para considerar o que estão escrevendo e compartilhando. Deveriam ser ensinadas técnicas para desacelerar a interação online, para que as próprias pessoas questionem o que escrevem e o que leem - e parem e pensem mais antes de fazer um julgamento online.

Conclusões e recomendações

A regulamentação e o papel, definição e responsabilidade legal das empresas de tecnologia

1. As empresas de mídia social não podem se esconder sob o pretexto de serem meramente

“plataformas”, mantendo o argumento de que não são responsáveis elas mesmas por regular o conteúdo de seus sites. Reiteramos a recomendação do nosso Relatório Intercalar de que uma nova categoria de empresa de tecnologia seja formulada, expandindo suas responsabilidades, e que não seja necessariamente uma "plataforma" nem "editora". Essa abordagem permitiria que as empresas de tecnologia assumissem responsabilidade jurídica por conteúdos identificados como nocivos após sua publicação por usuários. Pedimos ao Governo que considere essa nova categoria de empresa de tecnologia em seu próximo Livro Branco. (Parágrafo 14)

2. Ao optar por não comparecer perante a Comissão e não responder a nenhum dos nossos convites, Mark Zuckerberg mostrou desprezo tanto pelo Parlamento do Reino Unido como pela "Grande Comissão Internacional", que envolve membros de nove legislaturas de todo o mundo. (Parágrafo 29)

3. Nosso Relatório Intercalar recomendou que sejam estabelecidas responsabilidades jurídicas claras para que as empresas de tecnologia atuem contra conteúdos nocivos ou ilegais em seus sites. Há agora uma necessidade urgente de estabelecer uma regulação independente. Acreditamos que deva ser estabelecido um Código de Ética obrigatório, supervisionado por entidade reguladora independente, que estabeleça o que constitui conteúdo nocivo. O órgão regulador independente teria poderes normativos para supervisionar empresas de tecnologia relevantes, o que criaria um sistema regulatório para o conteúdo on-line tão eficaz quanto o de indústrias de conteúdo offline. (Parágrafo 37)

4. Como dissemos em nosso Relatório Intercalar, esse Código de Ética deve ser semelhante ao Código de Radiodifusão publicado pela Ofcom (Departamento de Comunicações do Reino Unido), que se baseia nas diretrizes estabelecidas na seção 319 da Lei das Comunicações. O Código de Ética deve ser desenvolvido por peritos técnicos e supervisionado por entidade reguladora independente, a fim de estabelecer por escrito o que é e o que não é aceitável nas redes sociais, incluindo conteúdo nocivo e ilegal encaminhado para as empresas por seus usuários em pedidos de remoção de conteúdo, ou conteúdo facilmente identificável pelas empresas de tecnologia. (Parágrafo 38)

5. O processo deve estabelecer responsabilidade jurídica clara para que as empresas de tecnologia ajam contra conteúdos nocivos e ilegais acordados na sua plataforma. Essas empresas devem dispor de sistemas relevantes de identificação e remoção desses conteúdos e garantir a existência de estruturas de segurança cibernética. Se as empresas de tecnologia (assim como os engenheiros técnicos envolvidos na criação do software para as empresas) não cumprirem as suas obrigações nos termos desse Código e não agirem contra a distribuição de conteúdo nocivos e ilegais, o regulador independente deve ter a capacidade de abrir processos judiciais contra elas, com a possibilidade de multas elevadas serem administradas como penalidade pelo não cumprimento do Código. (Parágrafo 39)

6. Esse mesmo órgão público deve ter a capacidade jurídica necessária para obter informações de empresas de mídia social que tenham relevância para seus questionamentos, o que pode incluir a capacidade de verificar quais dados do indivíduo estão sendo guardados, caso tal usuário solicite tais informações. A entidade também deve ter acesso à mecanismos de segurança das empresas de tecnologia e a seus algoritmos para garantir que operam com responsabilidade. Este órgão público deve ser acessível ao público e estar apto a receber queixas de do público a respeito das empresas de redes sociais. Pedimos ao Governo que apresente estas propostas em seu próximo Livro Branco. (Parágrafo 40)

7. Apoiamos a recomendação do Comissariado para Informação do Reino Unido (ICO) de que os dados inferidos devem ser tão protegidos nos termos da lei quanto as informações pessoais. As

proteções da lei de privacidade devem ser estendidas para além das informações pessoais, de forma a incluir modelos usados para fazer inferências sobre um indivíduo. Recomendamos que o Governo estude maneiras de expandir as proteções da lei de privacidade para incluir modelos que são usados para fazer inferências sobre os indivíduos, especialmente durante campanhas políticas. Isso garantirá que essas inferências sejam tratadas com tanta importância quanto as informações pessoais de indivíduos. (Parágrafo 48)

8. Em nosso Relatório Intercalar, recomendamos que uma taxa fosse cobrada das empresas de tecnologia que operam no Reino Unido, para expandir o trabalho do ICO. Nós reiteramos essa recomendação. A decisão do Chanceler, no Orçamento de 2018, de impor um novo imposto de 2% sobre os serviços digitais às receitas das grandes empresas de tecnologia do Reino Unido a partir de abril de 2020, mostra que o Governo está aberto à criação de um imposto às empresas de tecnologia. A resposta do Governo a nosso Relatório Intercalar sugeria que não mais apoiaria financeiramente o ICO, contrariando nossa recomendação. Recomendamos fortemente que o Governo reconsidere essa posição. (Parágrafo 51)

9. O novo sistema e regulamentação independentes que recomendamos devem ser instaurados e financiados adequadamente. Recomendamos que seja cobrado um imposto de empresas de tecnologia que operam no Reino Unido para o financiamento desse trabalho. (Parágrafo 52)

Uso e segmentação de dados

10. O escândalo da Cambridge Analytica foi facilitado pelas políticas do Facebook. Se o acordo da Comissão Federal de Comércio (Federal Trade Commission, ou FTC) houvesse sido integralmente cumprido, isso não teria acontecido. A Queixa da Comissão Federal de Comércio dos EUA (FTC) de 2011 condenou o Facebook — por não proteger os dados dos usuários e por permitir que os desenvolvedores de aplicativos tivessem acesso irrestrito aos dados de usuários — e declarou que a empresa foi construída de forma a facilitar o abuso de dados. Quando questionada sobre o fracasso do Facebook em dar seguimento à queixa da FTC, Elizabeth Denham, a Comissária de Informação, disse-nos: Estou muito desapontada que o Facebook, sendo uma empresa tão inovadora, não tenha dedicado mais foco, atenção e recursos para a proteção de dados pessoais". Nós compartilhamos desse sentimento. (Parágrafo 76)

11. As provas que obtivemos de documentos judiciais do caso da empresa Six4Three indicam que o Facebook estava disposto a ignorar configurações de privacidade de seus usuários para transferir dados para certos desenvolvedores de aplicativos; a cobrar preços altos pela publicidade de alguns desenvolvedores, para que recebessem esses dados; e a deixar outros desenvolvedores, como a Six4Three, sem dados, fazendo com que fechassem seus negócios. É evidente que o Facebook estava, no mínimo, agindo em desconformidade com seu acordo com a Comissão Federal de Comércio. (Parágrafo 135)

12. O Commissariado para Informação (ICO) disse à Comissão que o Facebook precisa mudar significativamente seu modelo de negócio e suas práticas para manter a credibilidade. A partir dos documentos que recebemos da Six4Three, tornou-se claro que o Facebook violou intencionalmente e conscientemente leis de privacidade de dados e concorrência. O ICO deve conduzir uma investigação detalhada sobre as práticas da Plataforma do Facebook, seu uso dos dados de usuários e amigos de usuários e o uso de "reciprocidade" no compartilhamento de dados. (Parágrafo 136)

13. Com o Regulamento Geral sobre a Proteção de Dados irlandês (RGPD), a Irlanda é a principal fonte de informação sobre o Facebook. Esperamos que estes documentos forneçam provas úteis para

Helen Dixon, a Comissária irlandesa para a Proteção de Dados, em suas presentes investigações sobre como o Facebook visou, monitorou e monetizou seus utilizadores. (Parágrafo 137)

14. Em nosso Relatório Intercalar, afirmamos que o domínio do setor por um pequeno número de empresas poderosas de tecnologia fez com que elas agissem como monopólios em sua área específica, e apontamos alguns aspectos sobre os dados utilizados por esses serviços. O Facebook, particularmente, não quer ser responsabilizado frente aos órgãos reguladores mundo afora. O Governo deve considerar o impacto de tais monopólios na esfera política e democrática. (Parágrafo 138)

15. A agência governamental Competitions and Market Authority (CMA) — que fomenta e protege a concorrência no Reino Unido — precisa conduzir uma investigação aprofundada da atuação do mercado publicitário nas mídias sociais. A Comissão fez essa recomendação em seu relatório intercalar e está satisfeita por ela também ter sido apoiada pelo Relatório Cairncross independente encomendado pelo Governo e publicado em fevereiro de 2019. Dado o conteúdo dos documentos que publicamos da Six4Three, a agência também deve investigar se o Facebook especificamente esteve envolvido em quaisquer práticas anticoncorrenciais e conduzir uma análise das práticas comerciais do Facebook com outros desenvolvedores, para decidir se o Facebook está usando injustamente sua posição dominante no mercado de mídias sociais na decisão sobre quais empresas devem ter sucesso ou não. Esperamos que o Governo inclua essas considerações ao reavaliar autoridade do Reino Unido no que tange a concorrência em abril de 2019, conforme indicado na resposta do Governo ao nosso Relatório Intercalar. Não deve ser permitido a empresas como o Facebook se comportar como “gângsteres digitais” no mundo digital, pensando-se à frente e além da lei. (Parágrafo 139)

16. A partir das provas que recebemos, apoiadas pelas conclusões tanto do ICO quanto da Comissão Eleitoral, fica claro que existia uma relação porosa entre a Eldon Insurance e a Leave.EU, com funcionários e dados de uma organização alimentando a outra. Não se tentou criar uma divisão rigorosa entre as duas organizações, o que viola as leis vigentes. Estamos à espera dos resultados das investigações realizadas pela ICO das duas organizações. (Parágrafo 146)

17. Como exposto em nosso Relatório Intercalar, Arron Banks e Andy Wigmore demonstraram total desconsideração e desdém pelo processo parlamentar quando compareceram perante nós em junho de 2018. É agora evidente que também nos deram provas enganosas sobre a relação de cooperação entre a Eldon Insurance e a Leave.EU. Eles se mostraram, sem dúvida, indivíduos com pouco apreço pela verdade. (Parágrafo 147)

AggregateIQ

18. Há provas claras de que houve uma estreita relação de colaboração entre a Cambridge Analytica, SCL e AIQ. Houve certamente uma relação contratual, mas acreditamos que a informação revelada a partir do repositório indicaria algo mais próximo, com troca de dados entre AIQ e SCL, bem como entre AIQ e Cambridge Analytica. (Parágrafo 166)

19. A AIQ trabalhou tanto nas eleições primárias presidenciais dos EUA como em organizações relacionadas com o Brexit, incluindo com o grupo designado "Vote Leave", durante o Referendo da UE. O trabalho do AIQ destaca o fato de os dados terem sido e continuarem a ser amplamente utilizados por empresas privadas a fim de influenciar pessoas em suas decisões, muitas vezes em um contexto político. É uma prática muito mais comum do que se pensaria. O próximo capítulo enfatiza a ampla natureza desse direcionamento. (Parágrafo 192)

A publicidade e as campanhas políticas

20. Reiteramos a recomendação do nosso Relatório Intercalar de que o Governo deve considerar como a legislação britânica deve caracterizar uma campanha digital, com todas as definições acordadas sobre o que constitui publicidade política on-line, como, por exemplo, os tipos de palavras acordados costumam surgir em anúncios e não são patrocinados por nenhum partido político específico. Também é necessário que haja um reconhecimento do papel e do poder de campanhas não remuneradas e de Grupos do Facebook ao influenciar eleições e referendos (dentro e fora do período designado para campanhas). (Parágrafo 210)

21. A lei eleitoral, como está, não se adequa a esse propósito e precisa ser alterada para refletir as mudanças nas práticas de campanha e na substituição dos folhetos físicos e outdoors por campanhas políticas on-line micro-direcionadas. É preciso haver transparência absoluta nas campanhas políticas on-line, incluindo a presença de indicações constantes e claras da fonte e do anunciante de qualquer anúncio e vídeo políticos pagos; a criação de uma categoria para gastos digitais em campanhas; e a criação de regras explícitas sobre o papel e responsabilidades dos anunciantes designados. (Parágrafo 211)

22. Esperamos que a consulta do Cabinet Office resulte no parecer do Governo de que a publicidade política paga deve ser acessível ao público, além de clara e facilmente identificável. Os destinatários devem ser capazes de identificar a fonte da publicidade, quem fez seu upload, quem a patrocinou e seu país de origem. (Parágrafo 212)

23. O Governo deve levar a cabo uma ampla reavaliação das regras e regulamentos vigentes relacionados ao trabalho político durante as eleições e referendos, a saber: aumentar a duração do período regulamentado; definir o que constitui campanha política; e reduzir o tempo para a devolução dos fundos a serem enviados para a Comissão Eleitoral. (Parágrafo 213)

24. O Governo deve explorar maneiras de aumentar os poderes da Comissão Eleitoral, para que realize seu trabalho de forma mais abrangente, incluindo as seguintes medidas:

- O direito legal de obrigar as organizações que não são atualmente reguladas, incluindo as empresas de redes sociais, a fornecer informações relevantes para os seus inquéritos.
- O atual limite máximo da multa da Comissão Eleitoral de £20.000 deve ser aumentado e alterado para uma multa baseada em uma porcentagem fixa do volume de negócios, em conformidade com os poderes já conferidos a outros reguladores da lei.
- Dar a possibilidade de a Comissão Eleitoral apresentar petição contra uma eleição devido a atos ilícitos, que atualmente só pode ser apresentada por indivíduos.
- Dar capacidade à Comissão Eleitoral de intervir ou interromper alguém que atue ilegalmente em uma campanha e more fora do Reino Unido. (Parágrafo 214)

25. A publicidade política deve ser acessível ao público por meio de um repositório pesquisável que indique, por exemplo, quem paga pelos anúncios, que organizações o estão patrocinando e a que público se direciona, para que se possa compreender o comportamento de cada anunciante. Isso deve ser feito independentemente do setor de publicidade e de partidos políticos. Esta recomendação baseia-se no parágrafo 144 do nosso Relatório Intercalar. (Parágrafo 215)

26. Concordamos com a proposta da ICO sobre a criação de um Código de Práticas apoiado por legislação primária que enfatize o uso de informações pessoais em campanhas políticas e se aplique a todos os responsáveis pelo tratamento de dados pessoais para fins de campanhas políticas. Insistimos que o Governo aja de acordo com a recomendação do ICO e que anuncie legislação primária para a inclusão dos Códigos de Prática em leis. (Parágrafo 216)

27. Apoiamos a recomendação do ICO de que todos os partidos políticos devem trabalhar junto a ela, ao Cabinet Office e à Comissão Eleitoral para identificar e implementar uma solução multipartidária que dê maior transparência no uso de dados de indivíduos. Esta seria uma solução prática para garantir que o uso de dados durante as eleições e referendos seja feito de acordo com a lei. Esperamos que o Governo trabalhe no sentido de tornar essa colaboração uma realidade. Esperamos que o Governo aborde todas essas questões quando responder à sua consulta, "Protegendo o Debate: Intimidação, Influência e Informação", e ao relatório da Comissão Eleitoral, "Campanhas Digitais: mais transparência para os eleitores". Um aspecto fundamental da publicidade e da influência política é a interferência estrangeira nas eleições, que esperamos também ser intensamente discutida. (Parágrafo 217)

28. A Mainstream Network é outro exemplo mais recente de organização on-line que procura influenciar o debate político utilizando métodos semelhantes aos que suscitaram preocupações em relação ao referendo da União Europeia, e não deve mais permanecer anônima. Aguardamos informações do Facebook sobre as origens da Mainstream Network, que, até hoje, não recebemos, apesar das promessas de Richard Allan de que forneceria tais informações. Consideramos a resposta do Facebook, no geral, enganosa, sendo outro exemplo da má fé da empresa. O Comissário de Informação confirmou que está atualmente investigando as atividades desse site e que o Facebook terá de cooperar com a ICO. (Parágrafo 222)

29. As empresas de tecnologia devem abordar a questão das empresas-fantasma e outras tentativas de ocultar a identidade na compra de anúncios, especialmente em relação à publicidade política, tanto dentro como fora dos períodos de campanha. Deve haver uma divulgação completa da segmentação do mercado utilizada pela empresa, como parte da transparência na publicidade. O governo deve explorar formas de regulamentar o uso de segmentação em plataformas de mídia social como os Públicos Personalizados do Facebook. (Parágrafo 223)

30. As doações feitas a partidos políticos na Irlanda do Norte antes de julho de 2017 estão protegidas contra divulgação, conforme a Seção 71E da Lei dos Partidos Políticos, Eleições e Referendos de 2000. Isso impede que a Comissão Eleitoral divulgue qualquer informação relacionada a tais doações antes de julho de 2017. Concordamos com a Comissão Eleitoral que é "profundamente lamentável" que não seja possível, por lei, revelar aos Membros do Parlamento e ao público os detalhes acerca da fonte da doação de £435.000 do CRC (Conselho de Pesquisa Constitucional) ao DUP (Partido Democrático Sindicalista da Irlanda do Norte) ou da auditoria que se seguiu. Por causa da lei em sua forma atual, essa Comissão e o público em geral não têm como investigar a fonte da doação de £435.000 para o DUP feita em nome do CRC, e é impedido de saber se ela veio de uma organização — e se seus membros a teriam aprovado ou não — ou de um indivíduo abastado. (Parágrafo 232)

31. Há uma falta de transparência na relação entre o Conselho de Pesquisa Constitucional, o DUP e a facção política Vote Leave. Acreditamos que, para evitar ter que revelar a fonte desta doação de £435.000, o CRC, deliberada e conscientemente, explorou uma brecha na lei eleitoral para direcionar dinheiro para o Partido Democrático Unionista na Irlanda do Norte. Esse dinheiro foi usado para financiar publicidade pró-Brexit em jornais fora da Irlanda do Norte e para pagar a empresa canadense de análise de dados Aggregate IQ. (Parágrafo 233)

32. *Apoiamos a Comissão Eleitoral em seu pedido de que o Governo estenda as regras de transparência em relação às doações feitas a partidos políticos na Irlanda do Norte a partir de 2014. Esse intervalo de tempo abrangeria duas eleições gerais no Reino Unido, duas eleições para a Assembleia da Irlanda do Norte, o referendo sobre a independência da Escócia, o referendo sobre a UE e as eleições para a UE e para o governo local. Pedimos que o Governo faça essa mudança na lei assim que possível para garantir total transparência nessas eleições e referendos. (Parágrafo 234)*

33. *Aplaudimos o relatório de Dame Frances Cairncross sobre a defesa do futuro do jornalismo e a instauração de um código de conduta para reequilibrar a relação entre provedores de notícias e plataformas de mídia social. Em particular, apoiamos a recomendação de que os jornais e revistas digitais on-line tenham taxa zero de IVA, como acontece com as versões impressas. Isso daria fim ao falso incentivo dado a empresas novas contra o desenvolvimento de serviços digitais pagos. Nós apoiamos a recomendação — que concorda com a nossa — de investigar a publicidade on-line por meio da Autoridade de Defesa da Concorrência e de Mercados, com enfoque nas principais empresas digitais de mídia social e ferramentas de busca. (Parágrafo 236)*

Influência estrangeira em campanhas políticas

34. *Assim como outros países, o Reino Unido é nitidamente vulnerável a campanhas encobertas para influência digital, e o Governo deve realizar análises para compreender a dimensão do trabalho de segmentação de eleitores conduzido por atores estrangeiros nas eleições passadas. Questionamos o Governo se a legislação atual para proteger o processo eleitoral de influências danosas é suficiente. A legislação deve estar de acordo com os últimos desenvolvimentos tecnológicos e deve ser explícita quanto à influência ilegal de atores estrangeiros no processo democrático. Exortamos o Governo a analisar esta questão e a respondê-la em seu Livro Branco. (Parágrafo 249)*

35. *Estamos satisfeitos que nossa recomendação estabelecida no Relatório Intercalar em julho de 2018 sobre o Arron Banks e sua doação tenha sido seguida tanto pela Comissão Eleitoral — que tem dúvidas sobre Banks ser a "verdadeira fonte" da doação — quanto pela Agência Nacional de Combate ao Crime, que atualmente investiga a origem da doação. (Parágrafo 266)*

36. *Existe um princípio geral de que, dentro de certos limites de despesa, o financiamento estrangeiro não é permitido nas eleições do Reino Unido. No entanto, como a Comissão Eleitoral deixou claro, as regras atuais não banem explicitamente gastos feitos no exterior. Recomendamos que, assim que possível, o Governo reveja as regras atuais sobre o envolvimento estrangeiro nas eleições do Reino Unido, para garantir que a interferência estrangeira nas eleições do Reino Unido, na forma de doações, não aconteça. Também precisamos deixar claro que o Facebook, assim como todas as outras plataformas, tem a responsabilidade de cumprir a lei e de não facilitar atividades ilegais. (Parágrafo 267)*

37. *As operações de desinformação fazem parte de um grupo complexo e interligado de ações que promovem desordem e instabilidade através de sistemas de informação como empresas de mídia social. Essas empresas, em particular o Facebook, precisam tomar medidas contra administradores de grupos quem não têm transparência e usam os grupos para campanhas políticas. Eles também precisam impor punições muito mais severas aos usuários que abusam do sistema. O simples fato de ter uma conta falsa de desinformação desligada, sendo capaz de abrir outra logo em seguida, não constitui impedimento. (Parágrafo 271)*

38. *O Governo deve pressionar as empresas de redes sociais para que divulguem quaisquer casos de*

desinformação. O Governo precisa garantir que as empresas de mídia social compartilhem informações que tenham sobre a interferência estrangeira em seus sites — incluindo quem pagou por anúncios políticos, quem viu os anúncios e quem clicou nos anúncios — sob ameaça de serem financeiramente responsabilizadas caso as informações não sejam divulgadas. Certificados de segurança com autenticação das contas de mídias sociais assegurariam que uma pessoa real estivesse por trás das opiniões expressas na conta. (Parágrafo 272)

39. Nós repetimos nosso apelo ao Governo para que faça uma declaração sobre quantas investigações estão sendo realizadas atualmente sobre a interferência russa na política britânica. Recomendamos ainda que o Governo realize uma investigação independente sobre as eleições passadas — incluindo as eleições de 2017 no Reino Unido, o referendo de 2016 no Reino Unido e o referendo na Escócia de 2014 — para verificar o que realmente aconteceu em relação a influência estrangeira, desinformação, financiamento, manipulação de eleitores e compartilhamento de dados, de forma que possam ser feitas alterações adequadas à lei e que esse aprendizado sirva para eleições e referendos futuros. (Parágrafo 273)

A influência do Grupo SCL em eleições estrangeiras

40. Declaramos em nosso Relatório Intercalar que "o Grupo SCL e as empresas associadas entraram em processo de insolvência, mas outras empresas estão realizando um trabalho semelhante. Os executivos seniores envolvidos com a SCL e Cambridge Analytica parecem ter migrado para outros empreendimentos." Recomendamos que Agência Nacional de Combate ao Crime conduza uma investigação — se ainda não houver sido realizada — das conexões entre a empresa SCL Elections Ltda. e a Emerdata Ltda. Reiteramos essas recomendações neste Relatório. (Parágrafo 296)

41. Recomendamos que o Governo estude maneiras de inspecionar empresas de relações públicas e comunicação estratégica, possivelmente por meio de um organismo independente, para garantir que suas campanhas não contrariem o interesse nacional e a segurança do Reino Unido e não obstruam a imposição de sanções legítimas — como acontece atualmente com a venda legalizada de passaportes. É necessário criar barreiras para garantir que essas empresas não trabalhem em projetos sensíveis do Governo britânico nem com clientes cuja intenção possa ser prejudicar esses interesses. (Parágrafo 298)

42. A transformação de Cambridge Analytica em Emerdata ilustra como é fácil para empresas desacreditadas se reinventarem, mantendo a capacidade de uso dos mesmos dados e as mesmas táticas para prejudicar os governos, inclusive no Reino Unido. Esse setor precisa de mudanças. Como mostra o escândalo SCL/Cambridge Analytica, esse tipo de má prática conduzida no exterior ou com clientes estrangeiros corre o risco adentrar a política britânica. Atualmente, o setor de comunicação estratégica é amplamente autorregulado. O Governo do Reino Unido deve considerar novas regras que reduzam o mau comportamento desse setor. (Parágrafo 299)

43. É necessário que haja transparência nas empresas de comunicação estratégica, com registros públicos de todas as campanhas em que trabalham, tanto no país como no exterior. Elas precisam ser responsabilizadas por violações que cometam em campanhas políticas de qualquer lugar do mundo ou por trabalhar para campanhas que não têm transparência financeira. Recomendamos que o Governo aborde todas estas questões quando responder à sua consulta, "Protegendo o Debate: Intimidação, Influência e Informação". (Parágrafo 300)

44. Recomendamos que o Governo reconsidere a lei britânica de combate à corrupção, para avaliar se a legislação é suficiente para refrear a conduta inadequada no exterior. Também esperamos que o

Governo explore a viabilidade da adoção de uma versão britânica da lei estadunidense Foreign Agents and Registration Act (FARA), que exige que "indivíduos que atuam como representantes de atores estrangeiros de forma parcial ou totalmente política divulguem regularmente ao público suas relações com os agentes estrangeiros, bem como as atividades, recibos e dinheiro desembolsado em apoio a essas atividades". (Parágrafo 301)

Alfabetização digital

45. Se, por um lado, o Facebook dá a impressão de estar trabalhando com vistas à transparência no que tange a análise de seu conteúdo jornalístico, por outro, no exame de seu material publicitário — fonte de receitas cada vez maiores — a empresa tem agido de maneira um tanto obscura. Para tomar decisões conscientes sobre a publicidade que se apresenta a eles, os usuários do Facebook precisam ter acesso à fonte e ao propósito do conteúdo. (Parágrafo 306)

47. *Como escrevemos em nosso Relatório Intercalar, a alfabetização digital deve ser o quarto pilar da educação, juntamente com a leitura, a escrita e a matemática. Em sua resposta, o Governo não comentou sobre nossa recomendação de um imposto cobrado de empresas de mídia social, a ser usada, em parte, para financiar uma estrutura educacional abrangente — desenvolvida por instituições de caridade, ONGs e pelos próprios reguladores — disponibilizada on-line. Tal quadro informaria o público sobre as implicações do compartilhamento voluntário de seus dados, seus direitos sobre esses dados e formas pelas quais pode-se estabelecer um envolvimento e uma interação construtiva com as redes sociais. As pessoas precisam se manter atentas no relacionamento com tais sites, particularmente sobre o que leem e escrevem. Reiteramos essa recomendação ao Governo e estamos à espera da sua resposta. (Parágrafo 312)*

47. O público precisa saber mais sobre seu poder de denúncia de campanhas digitais que considerem enganosas e ou ilegais. A Ofcom, a ASA (agência de reguladora da publicidade), a ICO e a Comissão Eleitoral precisam se aprimorar para que as pessoas conheçam seus serviços e funções. O Governo deve assumir um papel de liderança na coordenação desse serviço, fundamental para o público. O Governo deve esclarecer o público sobre os seus direitos no que diz respeito às empresas de mídia social. (Parágrafo 313)

48. Os usuários de mídias sociais precisam de ferramentas on-line que os ajudem a distinguir o jornalismo de qualidade do material proveniente de organizações ligadas à desinformação ou de fontes consideradas não confiáveis. As empresas de mídia social devem ser obrigadas a desenvolver ferramentas como essa para si mesmas ou a trabalhar com provedores já existentes, como a Newsguard, para disponibilizar esses serviços para seus usuários. A exigência da introdução destas medidas por parte das empresas de redes sociais poderia ser parte de um novo sistema de regulação de conteúdo, com base em legislação e supervisionado por um regulador independente, tal como discutido anteriormente neste relatório. (Parágrafo 314)

49. Empresas de mídia social precisam ser mais transparentes sobre seus próprios sites e como eles funcionam. Ao invés de se esconderem por trás de acordos complexos, eles devem informar os usuários sobre como seus sites funcionam, como a sobre as funções de curadoria, por exemplo, e sobre a maneira pela qual algoritmos são utilizados para priorizar certas histórias, notícias e vídeos, de acordo com o perfil de cada usuário. Quanto mais pessoas souberem como os sites funcionam e como os sites usam os dados dos indivíduos, mais informados estaremos, o que por sua vez tornará as escolhas sobre o uso e a privacidade dos sites mais fáceis de serem realizadas. (Parágrafo 315)

50. A Ofcom, a ICO, a Comissão Eleitoral e a ASA escreveram, cada uma separadamente, sobre seu

papel na promoção da alfabetização digital. Recomendamos que o Governo assegure que os quatro principais reguladores produzam uma estratégia conjunta de alfabetização digital. Nessa abordagem conjunta, deve haver uma discussão pública sobre se nós, como indivíduos, estamos satisfeitos com o uso e compartilhamento de nossos dados. O público precisa saber como seus dados estão sendo utilizados (partindo das recomendações que estabelecemos no segundo capítulo deste Relatório Final). Os usuários precisam saber definir os limites desejados e como esses limites devem ser definidos no que diz respeito aos seus dados pessoais. Nesse debate deve-se discutir se os usuários querem um padrão básico de privacidade acordado, da mesma forma que há um padrão básico de higiene, por exemplo. Os usuários também podem optar por não haver padrões básicos, se for o caso. (Parágrafo 316)

51. Recomendamos que a participação nas redes sociais permita mais tempo para consideração. Devem ser incorporados maiores obstáculos nas plataformas das redes sociais e nas próprias atividades dos usuários no sentido de dar às pessoas tempo para que considerem o que estão escrevendo e compartilhando. As técnicas para desacelerar a interação on-line devem ser ensinadas, para que as próprias pessoas questionem tanto o que escrevem quanto o que leem, e que façam uma pausa e reflitam antes de emitir uma opinião na internet. (Parágrafo 317)

Anexo 1 - Participantes do 'Comitê Internacional', terça-feira, 27 de novembro de 2018

Argentina: Leopoldo Moreau, Presidente da Comissão de Liberdade de Expressão, Câmara dos Deputados

Bélgica: Nele Lijnen, membro da Comissão de Infraestrutura, Comunicações e Empresas Públicas, Parlamento da Bélgica

Brasil: Alessandro Molon, membro da Câmara dos Deputados

Canadá: Bob Zimmer, Presidente, Comitê Permanente de Acesso à Informação, Privacidade e Ética, Câmara dos Comuns do Canadá; Nathaniel Erskine-Smith, Vice-Presidente, Comitê Permanente de Acesso à Informação, Privacidade e Ética, Casa dos Comuns; Charlie Angus, Vice-Presidente, Comitê Permanente de Acesso à Informação, Privacidade e Ética, Casa dos Comuns

França: Catherine Morin-Desailly, Presidente, Comitê Permanente de Cultura, Educação e Mídia, Senado Francês

Irlanda: Hildegard Naughton, Presidente, Comitê Conjunto de Comunicações, Ação Climática e Meio Ambiente; Eamon Ryan, membro, Comitê Conjunto de Comunicações, Ação Climática e Meio Ambiente

Letônia: Inese Libina-Egnere, Vice-Presidente

Cingapura: Pritam Singh, Membro, Comitê Seleccionado de Falsidades Online Deliberadas; Edwin Tong, Membro, Comitê Seleccionado de Falsidades Online Deliberadas; Sun Xueling, Membro, Comitê Seleccionado de Falsidades Online Deliberadas

Reino Unido: Damian Collins, Presidente do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns do Reino Unido; Clive Efford, Membro do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns; Julie Elliott, Membro do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns; Paul Farrelly, Membro do

Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns; Simon Hart, Membro do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns; Julian Knight, Membro do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns; Ian C. Lucas, Membro do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns; Brendan O'Hara, Membro do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns; Rebecca Pow, Membro do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns; Jo Stevens, Membro do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns; Giles Watling, Membro do Comitê Digital, da Cultura, dos Meios de Comunicação e Esporte, Câmara dos Comuns.

Anexo 2 - Princípios Internacionais sobre Regulação de Plataformas de Tecnologia

"COMITÊ INTERNACIONAL" DE DESINFORMAÇÃO E NOTÍCIAS FALSAS

Preâmbulo

Nós, os signatários abaixo:---

Membros dos parlamentos nacionais da: República Argentina; Reino da Bélgica; República Federativa do Brasil; Canadá; República Francesa; Irlanda; República da Letônia; República de Cingapura; e o Reino Unido da Grã-Bretanha e Irlanda do Norte,

Observando que - o mundo em que as instituições tradicionais do governo democrático operam está mudando num ritmo sem precedentes; identificamos uma prioridade urgente e crítica para os poderes legislativo e executivo garantirem que os direitos e garantias fundamentais dos seus cidadãos não sejam violados ou prejudicados pela marcha sem controle da tecnologia; a ordem mundial democrática está sofrendo uma crise de confiança com o crescimento da desinformação, a proliferação de agressões on-line e discursos de ódio, ataques conjuntos aos nossos valores democráticos comuns de tolerância e respeito pelas opiniões dos demais, e o uso indevido generalizado de dados de cidadãos para viabilizar tentativas de sabotagem de processos abertos e democráticos, incluindo eleições.

Afirmando que: - a democracia representativa é importante demais e conquistada com muita dificuldade para não ser defendida contra danos on-line, em particular campanhas agressivas de desinformação lançadas por um país contra cidadãos de outro, e a atividade coordenada de contas falsas usando métodos de direcionamento de dados com o objetivo de manipular as informações que as pessoas veem nas redes sociais.

Acreditando que: - temos o dever de criar um sistema de governança global da Internet que possa servir para proteger os direitos e liberdades fundamentais das próximas gerações, com base em códigos de conduta estabelecidos para agências que trabalham para estados, e governar as principais plataformas tecnológicas internacionais que criaram os sistemas que veiculam conteúdo on-line para bilhões de usuários em todo o mundo.

Declaração

No interesse da transparência, responsabilidade e proteção da democracia representativa, declaramos e endossamos os seguintes princípios:

- i. A internet é global e as leis relacionadas a ela devem ser extraídas de princípios mundiais comuns;

- ii. A disseminação intencional da desinformação e promoção de divisão é uma ameaça significativa para a continuidade e crescimento da democracia e para um diálogo global civilizador;
- iii. As empresas globais de tecnologia devem reconhecer seu grande poder e demonstrar sua disposição para aceitar sua grande responsabilidade como detentores de influência;
- iv. As empresas de mídia social devem ser responsabilizadas se não cumprirem determinações emanadas pela justiça, por lei ou por autoridade regulatória para remover conteúdo nocivo ou enganoso das suas plataformas, e devem ser reguladas para garantir que cumpram esse dever;
- v. As empresas de tecnologia devem demonstrar sua responsabilidade para com os usuários, tornando-se plenamente responsáveis perante os parlamentos nacionais e outros órgãos da democracia representativa.

ASSINADO:

[Assinatura] Membro, Congresso Nacional da Argentina	[Assinatura] Membro, Parlamento da Bélgica	[Assinatura] Membro, Congresso Nacional do Brasil
[Assinatura] Membro, Parlamento do Canadá	[Assinatura] Membro, Parlamento da França	[Assinatura] Presidente do Comitê Conjunto de Comunicações, Ação Climática e Meio Ambiente, Parlamento da Irlanda
[Assinatura] Vice-Presidente do Parlamento da República da Letônia	[Assinatura] Membro, Parlamento de Cingapura	[Assinatura] Membro, Parlamento do Reino Unido

Terça-feira, 27 de novembro de MMXVIII, em WESTMINSTER, LONDRES

Ata formal

Quarta-feira, 13 de fevereiro de 2019

Damian Collins, na presidência

Clive Efford Jo Stevens
Paul Farrelly Giles Watling
Ian C Lucas

Minuta do Relatório "*Desinformação e 'fake news': Relatório Final*", proposto pelo Presidente, apresentação e leitura.

Aprovado, Que a minuta do Relatório seja lida por segunda vez, parágrafo por parágrafo. Os parágrafos 1 a 317 foram lidos e aprovados.

Resumo aprovado.

Anexos aprovados.

Aprovado para constituir o Oitavo Relatório do Comitê para a Casa dos Comuns.

Aprovado, Que o Presidente encaminhe o Relatório à Casa.

Aprovado, Que as cópias retidas do Relatório sejam disponibilizadas, de acordo com os dispositivos da Ordem Permanente N. 134.

[Encerrada a sessão, será retomada em 26 de fevereiro de 2019, às 10h00]

Testemunhas

As seguintes testemunhas assinaram. A transcrição estará disponível na [página](#) de [publicações](#) de [inquérito](#) no site do Comitê.

Terça-feira, 19 de dezembro 2017

Samantha Bradshaw, Instituto para Internet de Oxford, e **Professora Kalina Bontcheva**, Professora de Análise Textual, University of Sheffield

[Q1-51](#)

David Alandete, editor do El País, **Francisco de Borja Lasheras**, diretor do escritório de Madri, Conselho Europeu de Relações Exteriores, e **Mira Milosevich-Juaristi**, pesquisadora sênior da Rússia e Eurasia no Elcano Royal Institute e professora associada de História das Relações Internacionais do Instituto de Empresa, Madri

[Q52-85](#)

Terça-feira, 16 de janeiro de 2018

Bethan Crockett, diretor sênior de segurança de marca e risco digital do GroupM EMEA, **Eitan Jankelewitz**, sócio da Sheridans, e **Matt Rogerson**, chefe de políticas públicas, Guardian News and Media

[Q86-159](#)

Tim Elkington, Departamento de Publicidade na Internet, **Phil Smith**, Diretor Gerente da Sociedade de Anunciantes Britânicos (ISBA) e **Ben Williams**, Adblock Plus

[Q160-188](#)

Terça-feira, 23 de janeiro de 2018

Professor Vian Bakir, Bangor University, **Professor Stephan Lewandowsky**, University of Bristol, e **Dra. Caroline Tagg**, Open University

[Q189-237](#)

Matt Breen, Diretor Comercial, Media Chain (parte do Social Chain Group), **Adam Hildreth**, Diretor Executivo, Crisp, e **Dr. Charles Kriel**, Instituto Corsham

[Q238-272](#)

Quinta-feira, 8 de fevereiro de 2018

Richard Gingras, vice-presidente de notícias do Google e **Juniper Downs**, chefe global de políticas públicas do YouTube [Q273-342](#)

Monika Bickert, chefe de gerenciamento de políticas globais, e **Simon Milner**, diretor de políticas, Reino Unido, Oriente Médio e África do Facebook [Q343-478](#)

Carlos Monje, diretor de políticas públicas e filantropia para os EUA e Canadá, e **Nick Pickles**, chefe de políticas públicas e filantropia para o Reino Unido do Twitter [Q479-568](#)

David Carroll, Professor Associado de Design de Mídia, The New School, **Amy Mitchell**, Diretora de Pesquisa em Jornalismo, Centro de Pesquisa Pew, **Frank Sesno**, Diretor, Professor de Mídia e Relações Públicas e Assuntos Internacionais, George Washington University, e **Claire Wardle**, pesquisadora do Shorenstein Centro de Mídia, Política e Políticas Públicas [Q569-600](#)

David Chavern, Presidente e Diretor Executivo, New Media Alliance, **Major Garrett**, Correspondente Chefe da Casa Branca, CBS News, **Tony Maddox**, Vice-Presidente Executivo e Diretor Executivo da CNN Internacional, e **Kinsey Wilson**, Assessor Especial do Presidente e Executivo Chefe do New York Times [Q601-620](#)

Terça-feira, 27 de fevereiro de 2018

Alexander Nix, Diretor Executivo, Cambridge Analytica [Q621-848](#)

Terça-feira, 6 de março de 2018

Bill Browder, fundador e diretor executivo, Hermitage Capital Management, e **Edward Lucas**, vice-presidente sênior do Centro de Análise Política Europeia [Q849-894](#)

Elizabeth Denham, Comissária de Informação [Q895-942](#)

Quarta-feira, 14 de março de 2018

Rt Hon Matt Hancock MP, Secretário de Estado de Conteúdos Digitais, da Cultura, dos Meios de Comunicação e Esporte [Q943-1186](#)

Quarta-feira, 21 de março de 2018

Sandy Parakilas, ex-gerente de operações do Facebook [Q1187—1270](#)

Terça-feira, 27 de março de 2018

Paul-Olivier Dehaye e **Christopher Wylie**, especialistas em redes sociais [Q1271-1461](#)

Terça-feira, 17 de abril de 2018

Brittany Kaiser, ex-diretora de desenvolvimento de programas, Cambridge Analytica [Q1462-1769](#)

Terça-feira, 24 de abril de 2018

Dr. Aleksandr Kogan , pesquisador da Cambridge University	<u>Q1770-2086</u>
Quinta-feira, 26 de abril de 2018	
Mike Schroepfer , Diretor Técnico, Facebook	<u>Q2087-2500</u>
Quarta-feira, 2 de maio de 2018	
Chris Vickery , diretor de Pesquisa de Risco Cibernético, UpGuard	<u>Q2501-2616</u>
Terça-feira, 15 de maio de 2018	
Claire Bassett , diretora executiva, Bob Posner , Diretora de Políticas Financeiras e de Regulação e Consultora Jurídica, e Louise Edwards , Chefe de Legislação da Comissão Eleitoral	<u>Q2617-2760</u>
Quarta-feira, 16 de maio de 2018	
Jeff Silvester , Diretor de Operações, AggregateIQ	<u>Q2761-3145</u>
Terça-feira, 22 de maio de 2018	
Tristan Harris , Co-Fundador e Diretor Executivo do Centro de Tecnologia Humana	<u>Q3146-3190</u>
Quarta-feira, 6 de junho de 2018	
Alexander Nix , ex-CEO da Cambridge Analytica	<u>Q3191-3480</u>
Terça-feira, 12 de junho de 2018	
Arron Banks , e Andy Wigmore	<u>Q3481-3780</u>
Quarta-feira, 31 de outubro de 2018	
Sharon White , Presidente, e Lord Burns , Diretor, Ofcom	<u>Q3781-3893</u>
Terça-feira, 6 de novembro de 2018	
Elizabeth Denham , Comissária de Informação, e James Dipple- Johnstone , Vice-Comissário, Departamento de Informação	<u>Q3894-4018</u>
Claire Bassett , diretora executiva, Bob Posner , Diretora de Políticas Financeiras e de Regulação e Consultora Jurídica, e Louise Edwards , Chefe de Legislação da Comissão Eleitoral	<u>Q4019-4100</u>
Guy Parker , Diretor Executivo, Autoridade de Padronização de Publicidade	<u>Q4101-4130</u>
Terça-feira, 27 de novembro de 2018	
Richard Allan , Vice-Presidente de Soluções de Políticas do Facebook;	<u>Q4131-4273</u>

Terça-feira, 27 de novembro de 2018

Elizabeth Denham, Comissária de Informação, e **Steve Wood**, Vice-Comissário,
Departamento de Informação

[Q4274-4326](#)

Ashkan Soltani, Especialista em Tecnologia

[Q4327-4382](#)

Documentos comprobatórios publicados

A transcrição estará disponível na [página de publicações](#) de [inquérito](#) no site do Comitê.

Os números de FKN são gerados pelo sistema de processamento de evidências e, portanto, podem não estar completos.

- 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 AggregateIQ ([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,
66 Argentina ([FKN0117](#))
67 London School of Economics and Political Science ([FKN0119](#))
68 Lucas, Edward ([FKN0052](#))
69 Major Garrett, Chief Whitehouse Correspondent, CBS News ([FKN0042](#))
70 McGrath, M C ([FKN0067](#))
71 McHugh, Mr Alistair ([FKN0020](#))
72 Mercer, Stuart ([FKN0016](#))
73 Miller, Mr C ([FKN0009](#))
74 MoneySavingExpert.com ([FKN0068](#))
75 Morley, Professor Neville ([FKN0091](#))
76 Morris, W ([FKN0085](#))
77 Muslim Engagement and Development (MEND) ([FKN0011](#))
78 National Crime Agency ([FKN0112](#))
79 National Literacy Trust ([FKN0037](#))
80 The Open University ([FKN0026](#))
81 The Open University, supplementary ([FKN0044](#))
82 Penna, Mr Dominic ([FKN0021](#))
83 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](#))

Lista de Relatórios do Comitê durante a Legislatura Atual do Parlamento

Todas as publicações do Comitê estão disponíveis na [página de publicações](#) do site do Comitê. O número de referência da resposta do governo a cada relatório é informado entre colchetes após o número de impressão da Casa dos Comuns.

Legislatura 2017-19

Primeiro Relatório	Nomeação do Presidente da Ofcom	HC 508
Segundo Relatório	O impacto potencial do Brexit nos setores criativos, do turismo e no mercado único digital	HC 365 (HC 1141)
Terceiro Relatório	Nomeação do Presidente da Comissão de Caridade	HC 509 (HC 908)
Quarto Relatório	Combate ao Doping no Esporte	HC 366 (HC 1050)
Quinto Relatório	Desinformação e 'notícias falsas': Relatório Preliminar	HC 363 (HC 1630)
Sexto Relatório	Relatório e Prestação de Contas da BBC 2017-18: Igualdade de Salários na BBC	HC 993
Sétimo Relatório	Relatório e Prestação de Contas da BBC 2017-18: Igualdade de Salários na BBC: Resposta da BBC ao Sexto Relatório do Comitê da Legislatura 2017-19	HC 1875
Primeiro Relatório Especial	Nomeação do Presidente da Comissão de Caridade: Resposta do Governo ao Terceiro Relatório do Comitê da Legislatura 2017-19	HC 908
Segundo Relatório	Combate ao Doping no Esporte: Resposta do Governo ao Quarto	HC 1050

Especial	Relatório do Comitê da Legislatura 2017-19	
Terceiro Relatório Especial	Falha de testemunha em responder a determinação do Comitê: atitude de Dominic Cummings	HC 1115
Quarto Relatório Especial	O impacto potencial do Brexit nos setores criativos, do turismo e no mercado único digital Resposta do Governo ao Segundo Relatório do Comitê da Legislatura 2017-19	HC 1141
Quinto Relatório Especial	Desinformação e 'notícias falsas': Resposta do Governo ao Quinto Relatório do Comitê da Legislatura 2017-19	HC 1630

Traduzido por Klébert Renée Machado Gonçalves e Ariel Daltrozo Munhoz Menezes
DOCUMENTO ENCAMINHADO SEM REVISÃO EM RAZÃO DA URGÊNCIA DO SOLICITANTE
 Serviço de Tradução e Interpretação do Senado – SETRIN/SGIDOC
 03 de outubro de 2019



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*

HC 1791

Published on 18 February 2019
by authority of the House of Commons

The Digital, Culture, Media and Sport Committee

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

Current membership

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

[Clive Efford MP](#) (*Labour, Eltham*)

[Julie Elliott MP](#) (*Labour, Sunderland Central*)

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

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

[Julian Knight MP](#) (*Conservative, Solihull*)

[Ian C. Lucas MP](#) (*Labour, Wrexham*)

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

[Rebecca Pow MP](#) (*Conservative, Taunton Deane*)

[Jo Stevens MP](#) (*Labour, Cardiff Central*)

[Giles Watling MP](#) (*Conservative, Clacton*)

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 additive 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 additive 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 Olivan, 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 owe 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 nekkko [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, [statistica.com](https://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

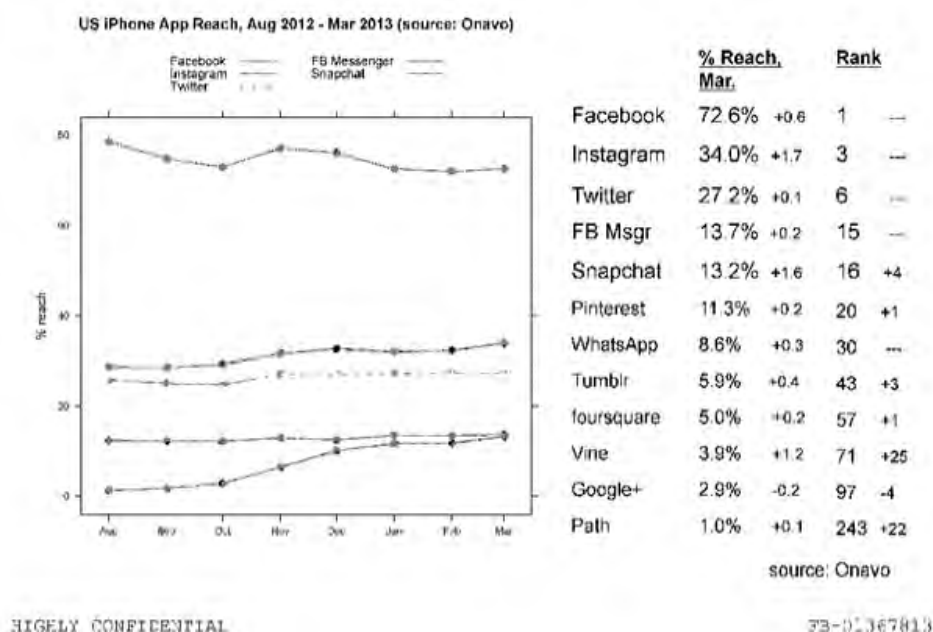
112. The following slides are from a presentation, titled "Industry Update", given on 26 April 2013, showing market analysis driven by Onavo data, comparing data about apps on users' phones and mining that data to analyse Facebook's competitors.

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

128 Ovano 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.



“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 Organizations 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-targeted 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:

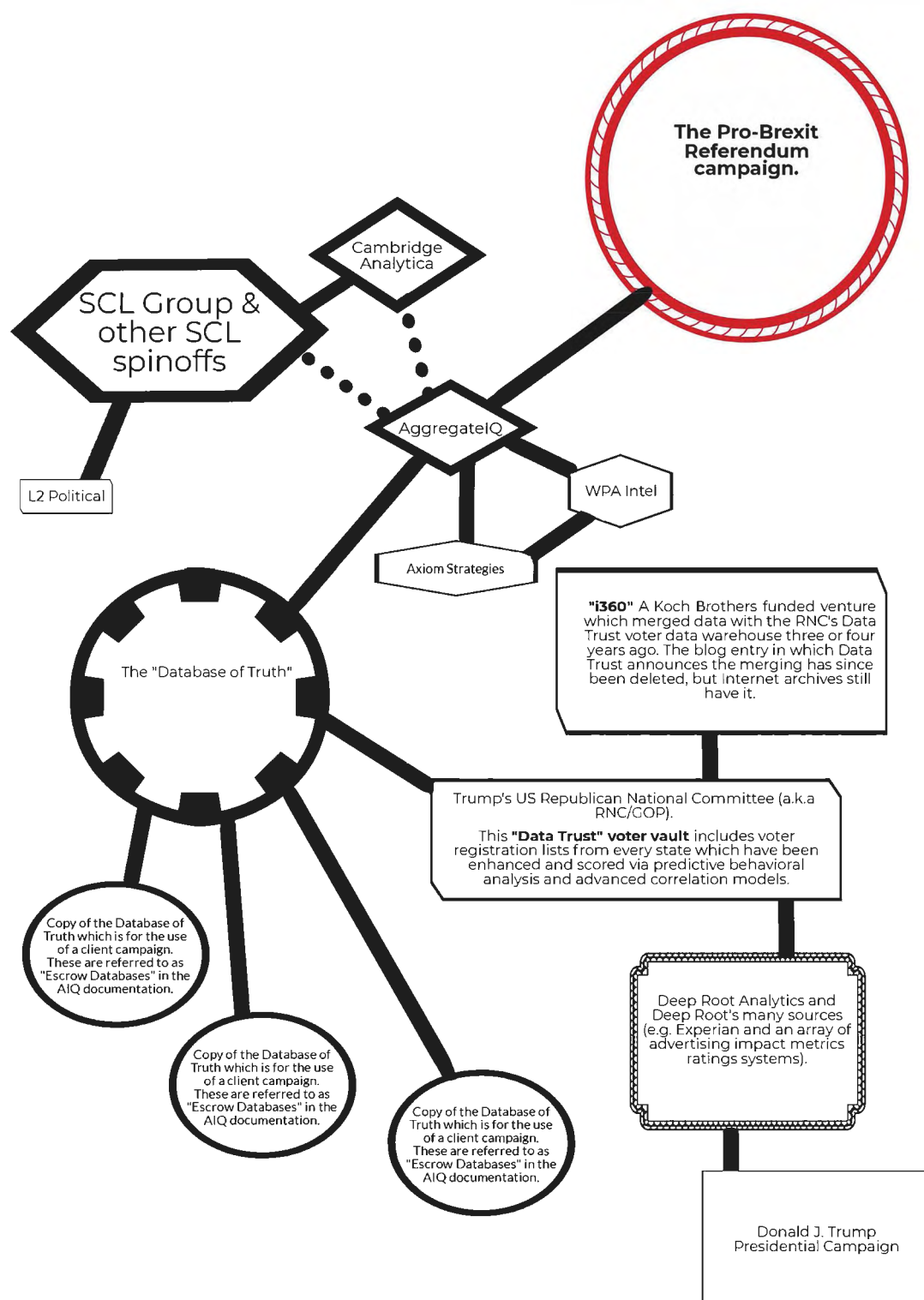
This repository is a set of sophisticated applications, data management programs, advertising trackers, and information databases that collectively could be used to target and influence individuals through a variety of methods, including automated phone calls, emails, political websites, volunteer canvassing,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

171 [The Aggregate IQ Files, Part One: How a political engineering firm exposed their code base](#), 30 April 2018.

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.

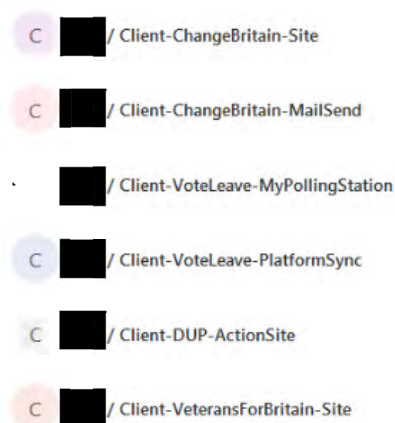
196 Facebook’s explanations of the different custom audiences can be found here: [Letter from Rebecca Stimson, Facebook to Louise Edwards, The Electoral Commission, 14 May 2018, p2.](#)

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:

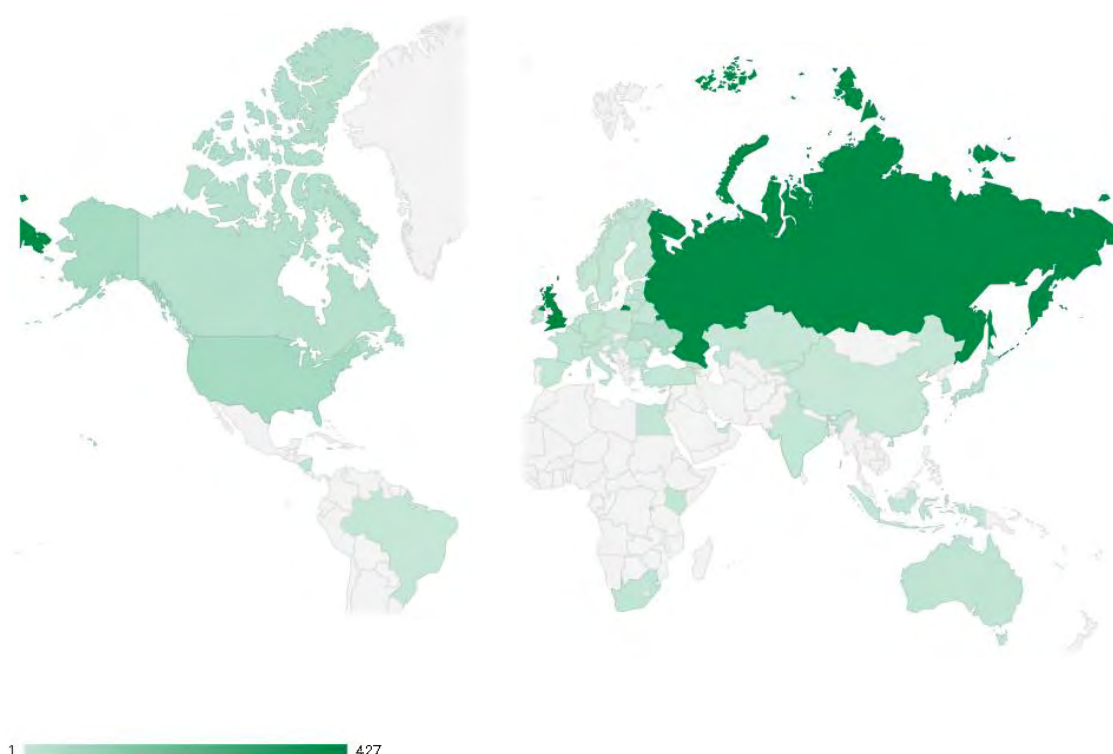
	City	Unique Pageviews *
1.	Moscow	19.79%
2.	London	17.8%
3.	Saint Petersburg	2.94%
4.	Cambridge	2.25%
5.	Kyiv	1.9%
6.	Sheffield	1.56%
7.	Bristol	1.38%
8.	Edinburgh	1.38%
9.	Novosibirsk	1.21%
10.	Ottawa	1.21%

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 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 Nayebe: 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, particular 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.

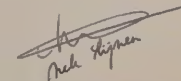
Declaration

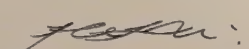
In the interests of transparency, accountability and the protection of representative democracy we hereby declare and endorse the following principles:

- 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.

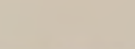
SIGNED:


Member, National Congress of Argentina


Member, Parliament of Belgium

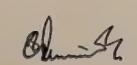

Member, National Congress of Brazil

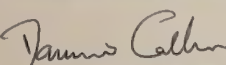

Member, Parliament of Canada


Member, Parliament of France


Chairperson of the Joint Committee on Communications,
Climate Action and Environment, Parliament of Ireland


Deputy Speaker, Parliament of Republic of Latvia


Member, Parliament of Singapore


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 AggregateIQ ([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



CÂMARA DOS DEPUTADOS
Gabinete da Deputada **Lídice da Mata** - PSB/BA

Ofício GDLMAT nº 074/2019

Brasília, 23 de setembro de 2019.

Exmo. Senhor Presidente,

Com meus cumprimentos, requeiro à Vossa Excelência que seja solicitado à Secretaria da Comissão Parlamentar Mista de Inquérito (CPMI) das Fake News providências para imediata e urgente tradução para o Português de dois documentos anexados, que tratam de temas de interesse e que visam instruir os trabalhos dos membros da referida Comissão.

Os documentos referidos são: 1) **“Disinformation and ‘fake news’: Final Report”** - Desinformação e 'notícias falsas': relatório final, produzido pela House of Commons Digital, Culture, Media and Sport Committee (Câmara dos Comuns Comitê Digital, Cultura, Mídia e Esporte), em fevereiro de 2019; e 2) **“Disinformation and the 2020 Election: How the Social Media Industry Should Prepare”** - “Desinformação e eleição de 2020: como a indústria das mídias sociais deve se preparar”, de autoria de Paul M. Barret, publicado por Center for Business and Human Rights (Centro de Negócios e Direitos Humanos) em setembro de 2019.

Dada à relevância desses estudos para os trabalhos da relatoria da referida Comissão, solicitamos urgência na tradução.

Respeitosamente,


Lídice da Mata

Deputada Federal PSB/BA
Relatora da CPMI das Fake News

À Sua Excelência o Senhor
SENADOR ANGELO CORONEL
Presidente da CPMI – Fake News

Recebido em
25/9/19
