FACING DOWN FACEBOOK

RECLAIMING DEMOCRACY IN THE AGE OF (ANTI) SOCIAL MEDIA

A REPORT FOR THE OFFICE OF MOLLY SCOTT CATO MEP BY TOM SCOTT

THE GREENS/EFA in the European Parliament

Green Party


searchable
ways
countries
years
model
regulators
disinformation
companies
regulatory
Brexit
linked
heavy
campaigns
number
social
media
personal
inquiry
power
report
light
privacy
easily
practice
also
advertising
recentusers
use
referenda
parties
people
networks
bodies
Facebook
platforms
role
Users
data
set
user
ahead
code
spread
elections
abuses
ensure
inquiries
breaches
required
information
penalties

CONTENTS

FOREWORD BY MOLLY SCOTT CATO MEP

Facebook is the social network turned antisocial network. It was supposed to bring us closer together but now stands accused of stealing our imaginations, fostering social divisions, inciting self-harm and failing to control hate speech, extremism and pornography. Facebook has found a way to monetise humanity, extracting monetary value from our creativity. Far from being shared fairly for social good, this creativity has been enclosed, privatised and its value funnelled into the pockets of a small number of shareholders.

These are all serious accusations, but from the perspective of a parliamentarian, the most destructive singular impact of Facebook is its impact on democracy.

Mark Zuckerberg, the founder of this global information behemoth, famously used the mission statement 'Move fast and break things' to drive his company's expansion. Unfortunately, one of the things that seems to have been broken is democracy itself. From voter suppression ads used during the 2016 US Presidential election, to the deceitful propaganda used to persuade British people to vote for Brexit, and on to the WhatsApp lies that enabled Bolsonaro to become president of Brazil, Facebook is being used to undermine democratic standards across the world. And, while actors on both the right and the left could be using Facebook for propaganda purposes, evidence is growing that this anti-social network has now become a major tool of the far right.

I was able to question Richard Allan, Facebook's Vice President of Public Policy, when he gave evidence at the European Parliament inquiry into Facebook and Cambridge Analytica. Like Nick Clegg, who has since joined the company to brush up its image, Allan is a PR man, not a technical expert. He observed that 'one person's fake news is another person's political speech'. This throwaway line demonstrates the dangerous level of complacency we are dealing with. As an information business, Facebook must understand that there is the world of difference between evidence-based policy-making and political propaganda. Perhaps we should not be surprised that Allan, as a PR man, cannot distinguish between the two.

In spite of repeated pleas that it can be trusted, it is clear that Facebook has neither the will nor the humility to reform itself. Regulation is overdue, and urgently so, in view of the fact that the UK may soon hold a People's Vote and the whole of the EU will soon be holding elections to the European Parliament.

There is a vast array of evidence on the appalling and destructive behaviour of Facebook, but I am delighted that in this report Tom Scott has been able to summarise this information and make it accessible. The report also includes suggestions about how regulation might work. It is vital that policy-makers act swiftly on this issue. It is no exaggeration to say that the survival of our democracies depends on it.

EXECUTIVE SUMMARY

This report examines the role of Facebook in abuses of personal data for political purposes and the spread of disinformation in recent years – and particularly during the Brexit referendum campaign in 2016.

It describes how the company has, from its earliest years, abused the trust placed in it by users of its platform and based its business model on the sharing of their personal data with third parties, with scant regard for the uses to which this data has been put. It also details the ways in which Facebook has consistently lied to the public and to regulators in order to conceal or misrepresent the ongoing abuses to which it has been party.

After giving a history of Facebook that describes how the company has come to occupy a massively dominant role in the social media landscape globally, the report summarises three recent inquiries that have shed light on such abuses: the inquiry into disinformation and fake news by the UK parliament's Digital, Culture, Media and Sport Committee; the investigation into the use of data analytics in political campaigns by the UK Information Commissioner's Office; and the inquiry into abuses of personal data involving Facebook and Cambridge Analytica by the Canadian parliament's Standing Committee on Access to Information, Privacy and Ethics. We also look at the testimony given by Mark Zuckerberg and other Facebook executives to EU parliamentarians in the summer of 2018, along with that of a number of expert witnesses.

Each of these inquiries has shone a light on the ways in which Facebook has enabled shadowy political actors to micro-target voters with disinformation ahead of key votes, not least the UK's Brexit referendum. They have also revealed the extent of Facebook's dissembling about its role in these abuses, and the company's determined efforts to resist transparency and accountability.

We conclude that Facebook cannot be trusted to regulate itself. To ensure that such abuses are curtailed in future, we offer a number of policy recommendations.

To ensure user data is better protected we propose:

- Coordination of data protection regulation across different national jurisdictions, using the EU's General Data Protection Regulation (GDPR) as a model framework and with sanctions that represent much more than the mere 'cost of business' for Facebook and other such companies;
- Framing of regulations so that companies basing any part of their data operations in countries not covered by equivalent legislation are deemed to be automatically in breach.
- Specification by regulators of standard, simple and easily understandable privacy settings set by default to 'no sharing of personal data with other organisations'.

To address the spread of disinformation and dishonest/covert political advertising, we propose that:

- The EU make adherence to its new Code of Practice on Disinformation a legal requirement for social media firms, with heavy penalties for any breaches and for concealment of such breaches;
- The Code itself be tightened up to define more precisely what is required of its signatories.
- All signatories to the Code be required to place all political advertisements that run on their platforms in easily searchable databases to which both regulators and members of the public have access, including information on the sponsor of each ad, the amount spent on it and the basis on which any targeting was carried out.

- During political campaigns ahead of elections or referenda, all political advertising – whether from parties or non-party campaigning organisations – should be labelled as such and all such parties and campaigners should be required to register with Facebook and other social media platforms that they use.
- Users of social media platforms should be easily able to opt out of all political advertising and an opt-out link enabling them to do this should be included prominently with all political ads.
- Political advertising related to elections and referenda in particular countries but that originates from and/or is paid for by sources from outside these countries should be banned under the Code.
- The Code be amended to specify clear requirements on identity verification and the prohibition of automated posts by non-human agents.
- Personal social media accounts should always be clearly linked to accountable people, who should be limited in the number of such accounts they can hold. Organisational and group pages should be linked to legally founded organisations or associations with responsible (named) people behind them.

To curb Facebook's monopoly power and foster a healthier social media ecosystem, we propose that:

- Users of social media networks be treated as core stakeholders who should be meaningfully represented both in the ownership of the network and at board level. This could also potentially be a requirement of an internationally applied code of practice
- National governments, including that of the UK, set up dedicated regulatory bodies equivalent to existing regulators that oversee the behaviour of the print and broadcast media and the energy utility industries. Such bodies should be responsible for ensuring that platforms adhere to regulations and codes of practice, with powers to impose heavy fines for breaches and, ultimately, the power to withdraw an offending company's licence to operate.
- Money raised from penalties imposed by regulators on companies such as Facebook should be earmarked for:

  1) fhe funding of organisations developing social media networks that take a transparent and responsible attitude to user data, and that are under the control of fully accountable trusts operated in the interests of users and employees, and

  2) funding for regulatory bodies specifically tasked with the oversight of social media platforms, focusing on transparency, privacy and combating the spread of disinformation online.

1.0 INTRODUCTION

'With great power comes great responsibility.' **The first recorded instance of this phrase, or a close variant of it, was in 1817, when the British parliamentarian William Lamb reminded the press of:**

'… their duty to apply to themselves a maxim which they never neglected to urge on the consideration of government – "that the possession of great power necessarily implies great responsibility". They stood in a high situation, and ought to consider justice and truth the great objects of their labours.' [1]

Anxiety at what has been seen as the grossly irresponsible behaviour from some elements of the media is not new, and has often been amply justified. Racism, sexism and distortion of the truth for the purposes of political propaganda has been evident in the tabloid press for years and – more recently – this tone and style has infected some of the mass broadcast media, where we have seen a decline in concern for truth and justice. The excesses of networks such as Fox News in the US and British newspapers such as The Daily Mail, The Daily Telegraph and The Sun (not least during and after the Brexit referendum campaign) show that people have had good reason to distrust the long-established mass media and to regard much of its output with scepticism if not outright contempt.[2] 'Fake news' may be a recent coinage, but it is not a recent invention.

But as distrust of the 'mainstream media' has grown, so too has the power of a new and highly pervasive form of communication: so-called 'social' media.

The start of the new millennium saw a wave of optimism that these new media could be a powerfully democratising force, and that by bypassing the entrenched power structures of the established media they could help open up space for voices that would otherwise go unheard. This optimism was tied up with the emerging notion of a 'sharing economy'. In an influential article of 2006, Yochai Benkler and Helen Nissenbaum framed this as 'commons-based peer production', in which large numbers of people would use the Internet cooperatively 'to provide information, knowledge or cultural goods without relying on either market pricing or managerial hierarchies to coordinate their common enterprise.'[3] Social media, which enabled anyone to create content and to share it online with others in their networks for free, seemed to many to provide a wonderful set of tools with which to build this utopian vision.

Fast forward to November 2018, when parliamentarians from around the world convened in London to form an International Grand Committee on Disinformation and Fake News. On 27 November the committee's members, which included representatives from Argentina, Belgium, Brazil, Canada, France, Ireland, Latvia, Singapore and the UK, signed a Declaration on the Principles of the Law Governing the Internet. Its preamble noted that:

'…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.'[4]

The declaration clearly spelled out the threat to democracy from 'aggressive campaigns of disinformation launched from one country against citizens in another, and the coordinated activity of fake accounts using data-targeting methods to try manipulate the information that

1 The Parliamentary Debates from the Year 1803 to the Present Time, Hansard, London, 1817

2 In December 2017, a survey by Pew Research Center found that only 32% of people in the UK placed trust in the news media; the average for the Western European countries surveyed was 41%. See: 'Trust in the military exceeds trust in other institutions in Western Europe and U.S.', Courtney Johnson, Pew Research Center, 4 September 2018.

3 Yochai Benckler and Helen Nissenbaum, 'Commons-based Peer Production and Virtue', The Journal of Political Philosophy: Volume 14, Number 4, 2006.

4 'Parliamentarians from across the world sign declaration on the Principles of the Law Governing the Internet', UK Parliament website, 27 November 2018.

people see on social media'. It called for the creation of 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'.

Even as the Grand Committee was deliberating, the destructive power of fake news spread by social media was dramatically illustrated once again when the so-called Gilets Jaunes (Yellow Jackets) unleashed a wave of mob violence on the streets of Paris and other French cities. Their actions had been organised almost entirely via Facebook pages, and the inchoate anger that fuelled them had been stoked in large part via fake news in the form of memes and viral videos.[5]

A protestor of the 'Gele Vestjes'(Yellow jackets) denouncing the NOS news broadcasting channel as 'Fake news' in the city of Groningen.
Wikimedia Commons/Donald Trung

As noted above, 'fake news' and propaganda are in themselves nothing new. What is new, and extraordinarily dangerous, is the way in which weaponised lies and disinformation can be disseminated at tremendous speed and targeted with great precision on groups and individuals who are most likely to be susceptible to them. What's more, this sort of activity is much less visible than propaganda disseminated via more traditional media channels, because of the way in which it is distributed at an individual level, out of public view and often by actors who are not what they claim to be.

As this report will show, one social media company has played a central role in the rise of this insidious threat to democracy, while greatly enriching its owners and investors in the process: Facebook, Inc.

On the same day the Grand Committee issued its declaration, its members had an opportunity to address questions about Facebook's role to the company's Vice President of Policy Solutions, Richard Allan. His answers ranged from the anodyne and uninformative to the evasive and misleading. But perhaps more significant than anything Allan had to say was an empty place at the table in the committee's meeting room – a place labelled with the name of Facebook's co-founder and CEO, Mark Zuckerberg.

Despite repeated requests from the UK parliament's Digital, Culture, Media and Sport (DCMS) Committee, which had convened the international gathering of parliamentarians, Zuckerberg had refused to appear in person to answer questions on the abuses his platform had facilitated.

As Canadian lawmaker Charlie Angus observed: *'We've never seen anything quite like Facebook, where, while we were playing on our phones and apps, our democratic institutions ... seem to have been upended by frat-boy billionaires from California. So Mr Zuckerberg's decision not to appear here at Westminster (Britain's parliament) to me speaks volumes'.*[6]

What had happened to turn the utopian vision of social media as a force for positive collaboration and democratic empowerment into a dystopian nightmare of industrialised hate-speech and

5 'The 'Yellow Jackets' Riots In France Are What Happens When Facebook Gets Involved With Local News', Ryan Broderick, Buzzfeed News, 5 December 2018.

6 'Upended by frat boys: International lawmakers slam Facebook's effect on politics', Alistair Smout, Reuters, 27 November 2018.

divisive propaganda? And what can be done to hold to account the corporation that more than any other has enabled this, and to prevent further damage to our democratic processes and institutions? These are the questions examined in this report.

It starts by describing Facebook's rise to global dominance in the social media sphere, showing how decisions made with a view to maximising the company's market share and the monetisation of personal data can be directly linked to the abuses that have come to light recently.

The next section of the report summarises a large body of evidence gathered by three inquiries that have looked into Facebook's role in recent political events around the world: the inquiry into disinformation and fake news by the UK parliament's Digital, Culture, Media and Sport Committee; the investigation into the use of data analytics in political campaigns by the UK Information Commissioner's Office (ICO); and the inquiry into abuses of personal data involving Facebook and Cambridge Analytica by the Canadian parliament's Standing Committee on Access to Information, Privacy and Ethics. This section also covers the testimony given by Mark Zuckerberg and other Facebook executives to EU parliamentarians in the summer of 2018, along with that of a number of expert witnesses.

We conclude by proposing some recommendations aimed at making companies such as Facebook more accountable, at fostering more democratic models of ownership and control in the social media sphere, and at reviving some of the more positive possibilities that, just a few years ago, this had seemed to hold out. Given the possibility that we may be engaged in a second EU referendum within months, it is essential that proposals for legal changes as well as changes of corporate policy at Facebook are implemented swiftly and decisively.

2.0 FACEBOOK'S RISE TO GLOBAL DOMINANCE

2.1 'MOVE FAST AND BREAK THINGS'

At the same time as Harvard Professor Yochai Benkler was gestating his thoughts on commons-based peer production, a student at the same university was developing a very different take on social media – and one that was to make him, over the next decade, one of the world's richest men.

In 2003, Mark Zuckerberg, a second-year Harvard student, wrote a programme he called 'Facemash', which compiled photos of female Harvard students and invited users to choose which of these was 'hotter'. It proved a hit with many male students but not with the university authorities, who charged Zuckerberg with offences including violation of individual privacy and copyright infringement.

Zuckerberg, true to his later form, was undeterred. In 2004 he and three male collaborators launched 'TheFacebook', a website that functioned as a directory of students at Harvard and allowed them easily to contact each other. Within a month, more than half the undergraduates at Harvard had registered, and soon after the site was opened to students at other universities. More controversy followed the site's launch, however, with Zuckerberg accused of having misappropriated the ideas of other Harvard students and put them to his own use (a case that was eventually settled out of court for $9.5 million in 2008).

Zuckerberg was not slow to grasp the commercial possibilities of the site, and in 2004 he and entrepreneur Sean Parker (now president of the nascent corporation) moved to Palo Alto, California. They rapidly secured an infusion of venture capital from PayPal co-founder and right-wing libertarian, Peter Thiel.[7]

A TELLING EXCHANGE

Shortly after launching TheFacebook, Mark Zuckerberg had an instant messenger exchange with a college friend which showed an attitude to privacy that was to characterise Facebook's approach to personal data over the next decade and a half.

Zuck: Yeah so if you ever need info about anyone at Harvard

Zuck: Just ask.

Zuck: I have over 4,000 emails, pictures, addresses, SNS

[Redacted Friend's Name]: What? How'd you manage that one?

Zuck: People just submitted it.

Zuck: I don't know why.

Zuck: They 'trust me'

Zuck: Dumb fucks.[8]

In 2004, the company unveiled a new feature that would become one of the defining characteristics of its platform: the Facebook Wall, which offered users a place to post messages to their friends. By December of that year there were over one million active users of the site. After further injections of venture capital, in 2005 Facebook launched a version of the site

7 Thiel, who is still on Facebook's board, was a major donor to Donald Trump's election campaign and is reported to have assembled a Silicon Valley 'brains trust' to supply ideas to the Trump presidency. His company Palantir Technologies supplies big-data services to corporations, intelligence and law enforcement agencies, and Palantir staff are said by whistleblower Christopher Wylie to have been frequent visitors to Cambridge Analytica's London headquarters. Thiel is on record expressing the view that democracy and freedom (by which he means unfettered capitalism) are incompatible; see 'Donald Trump, Peter Thiel and the death of democracy', Ben Tarnoff, The Guardian, 21 July 2016.

8 'Well, These New Zuckerberg IMs Won't Help Facebook's Privacy Problems', Nicholas Carlson, Business Insider, 13 May 2010.

aimed at high-school students and by the end of the year its user base had grown to six million.

The following year, Facebook was opened to anyone over the age of 13 and began promoting itself as a vehicle for business advertising. By October 2007 it had around 50 million users and had overtaken MySpace as the most widely used social media site in world. This was no doubt one reason why Microsoft bought a 1.6% stake in the company that same month for $240 million, implying a market value of around $15 billion.

Two other developments in 2007 were critical to the company's exponential growth – and to the abuses of personal data for which it was to become notorious. One was the launch of Facebook's application programming interface (API); the other was a move towards forming data-sharing partnerships with device manufacturers, eventually including Apple, Amazon, BlackBerry, Microsoft and Samsung (the true nature of these partnerships was not publicly reported till 2018).[9]

'Move fast and break things' was Facebook's motto for developers working on its platform until 2014. *(Image: Facebook)*

2.2 RHETORIC OF OPENNESS AND INCLUSIVITY

In May 2007 at Facebook's inaugural developers' conference in San Francisco, Zuckerberg's keynote address described, in messianic terms, how Facebook intended to transform the social media landscape:

'Right now, social networks are closed platforms. And today, we're going to end that. With this evolution of Facebook Platform, any developer worldwide is going to be able to build full applications on top of the social graph, inside the Facebook framework.'[10]

The rhetoric was of openness and inclusivity. The reality that emerged over the next few years was very different, as observers soon began to point out. One such was Tim Berners-Lee, often credited as the inventor of the World Wide Web, who in 2010 wrote[11] in Scientific American:

'The Web evolved into a powerful, ubiquitous tool because it was built on egalitarian principles and because thousands of individuals, universities and companies have worked, both independently and together as part of the World Wide Web Consortium, to expand its capabilities based on those principles. The Web as we know it, however, is being threatened in different ways. Some of its most successful inhabitants have begun to chip away at its principles. Large social networking sites are walling off information posted by their users from the rest of the Web.'

Berners-Lee was also concerned by the growing threat from online surveillance technologies used to profile Web users:

9 'Facebook Gave Device Makers Deep Access to Data on Users and Friends', Gabriel Dance, Nicholas Confessore and Michael LaForcia, The New York Times, 3 June 2018

10 'Did Facebook miss a massive opportunity by building a walled garden instead of a truly open platform?', Mathew Ingram, GigaOM, 24 July 2013.

11 'Long Live the Web: A Call for Continued Open Standards and Neutrality', Tim Berners-Lee, Scientific American, December 2010.

'Other threats to the web result from meddling with the Internet, including snooping […] The URIs that people use reveal a good deal about them. A company that bought URI profiles of job applicants could use them to discriminate in hiring people with certain political views, for example. Life insurance companies could discriminate against people who have looked up cardiac symptoms on the Web. Predators could use the profiles to stalk individuals. We would all use the Web very differently if we knew that our clicks can be monitored and the data shared with third parties.'

Berners-Lee had correctly identified the main factors that have fed into the attacks on democracy that Facebook's platform was to facilitate a few years down the line. What he could not have predicted at the time is quite how these factors would come together to cause havoc around the world.

2.3 MONETISING PERSONAL DATA

The key to this was that at the same time as 'walling off' data collected from its users through their use of its own and other sites, Facebook was also devising ways in which this data could be monetised by making it available to third parties.

The principal way in which Facebook does this is not to sell data directly to advertisers, but to use its own wealth of data harvested from users to place targeted ads on its users' feeds. Zuckerberg explained this succinctly in testimony to a hearing of the joint Senate Judiciary and Commerce Committees in April 2018:

'What we allow is for advertisers to tell us who they want to reach, and then we do the placement. So, if an advertiser comes to us and says, 'All right, I am a ski shop and I want to sell skis to women,' then we might have some sense, because people shared skiing-related content, or said they were interested in that, they shared whether they're a woman, and then we can show the ads to the right people without that data ever changing hands and going to the advertiser.'[12]

But there is another way in which Facebook has exploited user data, and it was this that was to prove central to the Cambridge Analytica affair and other data breaches: by making it available to third-party app developers. This was not done to raise revenue directly – developers were not paying for access to the data – but rather to increase Facebook's own market share by making itself an environment rich in platform-specific apps that could be used both by regular Facebook subscribers and by businesses as vectors for delivering ads.

As the tech-industry news website TechCrunch reported in 2007 when the Facebook API was launched, the new technology gave enormous scope to third parties to exploit not just the Facebook platform but also the personal data of its users:

'Facebook is giving an unprecedented amount of access to developers […] Applications can serve their own ads and/or conduct transactions with users […] The payoff is two way. Not only do developers get deep access to Facebook's twenty million users, Facebook also becomes a rich platform for third party applications.'[13]

Within six months of the API being introduced, more than 10,000 apps had launched on the Facebook platform.

2.4 THE SOCIAL GRAPH: TURNING PEOPLE INTO 'INVENTORY'

For both app designers and device manufacturers, what Facebook offered above all else was access to what the company calls its 'social graph'. This is essentially a model of the social network that maps the interconnections and activities of all its users, and has been described as 'the global mapping of everybody and how they're related'.[14]

12 Zuckerberg Senate Transcript 2018, Wikisource.org, 2018.

13 'Facebook Launches Facebook Platform; They are the Anti-MySpace', Michael Arrington, TechCrunch, 24 May 2007.

14 'Facebook: One Social Graph to Rule Them All?', CBS News, 21 April 2010.

The social graph was and is an extraordinarily powerful tool for the targeting of personalised advertising. Advertising industry magazine AdAge reported in 2007: 'While Google knows what millions of people are searching for, Facebook has something the search giant hasn't been able to grow: a network of connections between people that creates a viral distribution platform unrivalled by any portal or search engine.'[15]

As Facebook's then Chief Operating Officer, Owen Van Natta, explained to the magazine:

'A visit to Amazon.com will uncover all the product recommendations one might want but the value can be limited in the anonymity of the people posting the reviews. On the other hand, if you take your online activities and put them through the filter of the people you know well, those actions take on greater meaning.'

In terms that now seem heavily laden with historical irony, Van Natta stressed that it was the authenticity of these social connections that gave them such value:

There's not a lot of utility for it outside of using it to connect with real friends. If you put up a fake profile on Facebook, people won't connect to it.

In its drive to become an app-rich platform that could dominate the social media space, Facebook allowed and indeed encouraged app developers to monetise their apps through subscription services, e-commerce and advertising. As its Senior VP Sales helpfully explained in 2007:

'In order to get great applications built, we needed to make sure developers could be rewarded and have a business model around it.' He said with 29 million users, there's plenty of inventory for him to sell and that he envisions the better the applications are, the more time people will spend on the site and the more he can sell to marketers.'[16]

The description of people who use Facebook as 'inventory' could hardly be a clearer indication of the way in which Facebook has based its entire business model on the commodification of users and their personal data, bearing out with a vengeance the old ad industry maxim: 'If you're not paying for the product, you are the product.'

For app developers, the social graph that underpinned the Facebook API offered easy access to user data that allowed them to personalise these users' experience – and to target them with ads for their own products and those of others. Facebook did require developers using its API to sign an agreement not to sell user data and to delete it if requested, but as one developer who made extensive use of the API has explained, for years it was extremely easy to obtain not just the personal data of app users but also those of their Facebook friends, and the agreement to use this data responsibly was all but impossible to enforce, even if Facebook had wanted to:

It was all an agreement, there's no way they could have policed that. Thousands will have retrieved data that consumers had allowed, but their friends had not knowingly [allowed]. Thousands will have broken the agreements they had with Facebook, and used data or derived data in ways contrary to the intent and interpretation of that developer agreement.[17]

App companies were often unscrupulous in the way that they used the Facebook platform to maximise their revenues, for instance by spamming an app users' friends with posts in the name of the user. The hugely successful (and highly addictive) Farmville app, a game from developer Zynga that encouraged users to spend real money on in-game currency to buy virtual items, was notorious for this. *'I did every horrible thing in the book,'* admitted Marc Pincus, Zynga's co-founder and an early Facebook investor, in 2009.[18] By the end of that year, Facebook's user base was well on the way to half a billion users.

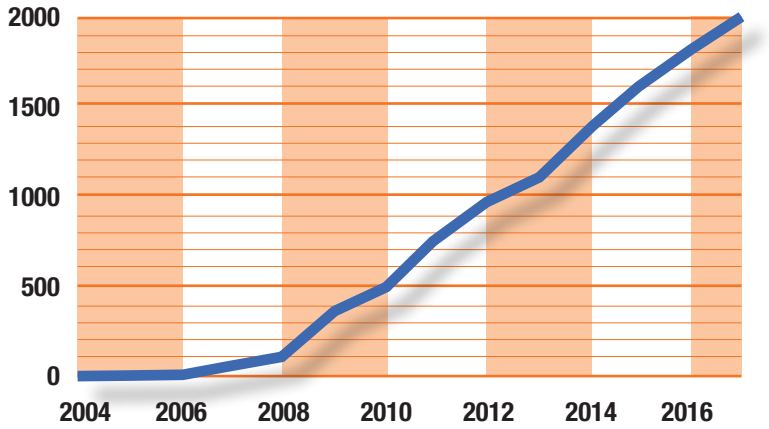
15 '23-year-old Mark Zuckerberg has Google Sweating', Abbey Klaasen, AdAge, 9 July 2007.

16 AdAge, ibid.

17 'A developer built a Facebook app as a 'thought experiment' to see how much data people would give up – and got almost 1 million users', Shona Gosh, Business Insider, 20 March 2018.

18 'How Facebook's platform made it worth billions – and set it up for a fall', Owen Thomas, The San Francisco Chronicle, 21 March 2018.

MONTHLY USERS OF FACEBOOK (MILLION), 2004-17 [19]



2.5 PRIVACY ISSUES PROLIFERATE

Concerns over the uses made of personal data collected by Facebook had emerged even before its new platform was launched in 2007 but began to proliferate rapidly thereafter. Many users were disturbed by a tracking system known as Beacon, launched by Facebook in November of that year. This allowed third-party websites to send data about user behaviour on their sites to Facebook, which in turn used it to display information about purchases, games played, etc. on the user's news feed. Facebook introduced an opt-out of this system for users, but there were well-sourced allegations that the company continued to collect such data even when Facebook users had opted out, and even when they were not logged into Facebook.[20]

Facebook, following a pattern that was by now becoming familiar, simply brushed off such concerns. Asked by a New York Times reporter whether it was collecting data on their purchases from users who had opted out of the system, the company's VP Marketing and Operations replied: 'Absolutely not. One of the things we are still trying to do is dispel a lot of misinformation that is being propagated unnecessarily.'[21]

After a successful class action lawsuit in the US, however, Facebook announced in 2009 that it was withdrawing the Beacon tool. A spokesperson for the company claimed at the time: 'We learned a great deal from the Beacon experience. For one, it was underscored how critical it is to provide extensive user control over how information is shared.' The fact that Facebook had 'learned' from this experience was not borne out by subsequent developments.[22]

In 2008, as criticism of Beacon intensified, Facebook launched a new data-sharing tool, Facebook Connect, which supposedly aimed to correct Beacon's mistakes by requiring Facebook users to take deliberate action before they shared their activities from other websites. However, there was another purpose to Facebook Connect, which was to enable Facebook to more easily partner with major branded content providers. The idea was that Facebook users would be able to log into these providers' sites by using their Facebook IDs; the corollary, of course, was that Facebook would receive data on precisely what content its users were engaging with on partner sites, which soon included many high-profile brands such as CNN and TripAdvisor.

Concerns quickly arose when users who connected with various online services via their Facebook IDs found that they had unwittingly installed apps that linked to Facebook and started posting content, without their knowledge, on their timelines. Many Facebook users were unhappy with their data being used to spam them and their friends in this way.

This was among the factors that led to a major investigation by the Office of the Privacy Commissioner of Canada in 2009. The investigation was launched after a group of law students at the University of Ottawa's Internet Policy and Public Interest Clinic filed a 35-page complaint

19 Wikipedia, 17 December 2018 (based on Facebook data).

20 'Facebook's Beacon More Intrusive Than Previously Thought', Juan Carlos Perez, PC World, 30 November 2007.

21 'Facebook Executive Discusses Beacon Brouhaha', Brad Stone, The New York Times, 29 November 2007.

22 'Facebook to end Beacon tracking tool in settlement', Barbara Ortutay, USA Today, 21 September 2009.

with the Commissioner alleging 22 separate violations of Canadian privacy laws. As one of the students explained:

'To boil it down simply, it's an issue of honesty and an issue of consent. Facebook isn't being completely honest with its users. It presents itself as a social utility site . . . but they are actually involved in a lot of commercial activities.' [23]

The complainants pointed out that Facebook's privacy settings and terms of use were so hard to access and understand that they were likely to be missed by many users (Facebook at the time had some seven million of these in Canada). They also noted that even if users opted for the highest privacy settings, their personal data could still be shared by friends with lower privacy settings, and that Facebook subscribers using third-party apps on the site were – often unwittingly – sharing their data by default with the app developers.[24]

Canada's Privacy Commission published its findings in July 2009. Its report concluded that the allegations were well-founded in four areas: default privacy settings, collection and use of users' personal information for advertising purposes, disclosure of users' personal information to third-party application developers, and collection and use of non-users' personal information. The report's author, Assistant Privacy Commissioner Elizabeth Denham, stressed that the Commission was particularly concerned by the issue of data-sharing with third parties:

Most notably, regarding third-party applications, the Assistant Commissioner determined that Facebook did not have adequate safeguards in place to prevent unauthorised access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers.[25]

2.6 TRUST US, WE'VE CHANGED

In response to these findings, in August 2009 Facebook announced what appeared to be its intention to introduce major new privacy safeguards, including:

'… a new permissions model that will require applications to specify the categories of information they wish to access and obtain express consent from the user before any data is shared. In addition, the user will also have to specifically approve any access to their friends' information, which would still be subject to the friend's privacy and application settings.'[26]

Assistant Privacy Commissioner Elizabeth Denham expressed herself satisfied with Facebook's commitment to meaningful change.[27] Not everyone was convinced, however. David Fewer of the Canadian Internet Policy and Public Interest Clinic, whose complaints against Facebook had led to the original investigation, later commented:

'The privacy commissioner at the time kind of gave the green light to Facebook, and from our perspective that was really problematic, especially the access to third-party content through the API. They reached a resolution which did away with our complaint, and basically gave the green light to Facebook to keep on doing what they do.' [28]

Many, including Elizabeth Denham herself, have also since had reason to reflect on whether Facebook's assurances in 2009 were given far too much credence.

Indications that this might be the case were not long in coming. In 2010, the Wall Street Journal reported that many of the most popular third-party Facebook apps 'have been transmitting identifying information – in effect, providing access to people's names and, in some cases, their friends' names – to dozens of advertising and Internet tracking companies'. The WSJ also noted that despite Facebook's supposed improvements to user privacy controls, the recently launched control panel did not 'detail what information friends' applications have accessed

23 'Ottawa law students file complaint over Facebook', CCTV News Ottawa, 31 May 2009.

24 'Privacy Complaint Filed Against Facebook', Grant Gross, CSO Online, 2 June 2009.

25 'Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act', Office of the Privacy Commissioner of Canada, 16 July 2009.

26 'Facebook Announces Privacy Improvements in Response to Recommendations by Canadian Privacy Commissioner', Facebook Newsroom, 27 August 2009.

27 'Remarks at a Press Conference on the Facebook Investigation', Elizabeth Denham, Office of the Privacy Commissioner of Canada, 27 August 2009.

28 'Canada flagged Facebook's third-party app privacy problem way back in 2009', Patrick Cain, Global News, 5 April 2018.

about a user'. This was later to prove a crucial point in the Cambridge Analytica data scandal.[29]

Writing in The Financial Times in May 2010, John Gapper was also highly critical of Facebook's attitude to protecting its users' privacy and personal data, which he described as 'displaying a disregard bordering on disdain'. Gapper noted that 'Facebook's privacy controls are now so complex and hard to understand that many have been nudged into 'sharing' a lot, just as Mr Zuckerberg wishes.' He also described how the 'improvements' to privacy controls heralded by Facebook had actually involved making a great deal more personal data publicly available by default, including gender, location and users' friends lists.[30]

Gapper observed that Zuckerberg's open letter assuring Facebook users that their privacy would now be better protected contrasted with the approach he outlined at the Facebook developers' conference just a few months later, in which he had proclaimed 'we are building towards a web where the default is social,' and with the 'Orwellian' warning now given to the site's users: 'When you connect with an application or website, it will have access to General Information about you.' The phrase 'General Information' was indeed to prove a remarkable piece of obfuscatory Newspeak.

2.7 THE 'OPEN GRAPH' AND THE GROWING BACKLASH

The 2009 developers' conference that Gapper described had been used by Facebook to announce a major new development, the so called 'open graph'. Zuckerberg's keynote described this as 'one of the most transformative things for the Web we've ever done.' As industry magazine TechCrunch reported:

'Facebook has redesigned its Graph API for developers so that not only can they see the social connections between people, but they can also see and create the connections people have with their interests—things, places, brands, and other sites […] Facebook wants it to be defined by social connections, likes and dislikes, interests that are coded and machine-readable. 'Our goal is to use the open graph so people can have instantly social experiences wherever they go,' he [Zuckerberg] says.'[31]

Who could object to having 'social experiences wherever they go'? Growing numbers of people, it turned out, were none too happy about the level of surveillance tracking that Facebook's 'open graph' was subjecting them to. This was reflected on Facebook itself, where several groups sprang up to demand better privacy controls under titles such as 'Millions Against Facebook's Privacy Policies and Layout Redesigns' and 'Protest: Restoring The Age Of Privacy To Facebook'.

Others concluded that the best way to protest was simply to leave the network: 31 May 2010 saw the first 'Quit Facebook Day'. The campaign had been initiated by two software developers under the slogan: 'Sick of Facebook's lack of respect for your data? Add you name to commit and quit!'

More than 33,000 people renounced their use of the network on that single day, but as commentators pointed out this was a mere pinprick in the company's subscriber base, which had by then grown to some 500 million globally. The Guardian observed, percipiently if optimistically: 'Ultimately, it won't be an unofficial rabble of protesters that bothers Facebook or forces more coherent improvement; it will be US regulators.'[32]

Facebook was indeed supremely unbothered by the protests. But nor was it greatly troubled by further, tentative moves by lawmakers. In May 2010, the Chairman of the US House Judiciary Committee asked Facebook, along with Google, to cooperate with inquiries into privacy practices at the two companies. Facebook's Director of Public Policy, Tim Sparapani, responded with a letter that, in its breezy disregard for the truth, can be seen to epitomise Facebook's trademark approach to such inquiries:

29 'Facebook in Privacy Breach', Emily Steel and Geoffrey Fowler, The Wall Street Journal, 18 October 2010.

30 'Facebook's open disdain for privacy', John Gapper, The Financial Times, 12 May 2010.

31 'Zuckerberg: 'We Are Building A Web Where The Default Is Social'', Erick Schonfeld, TechCrunch, April 2010.

32 'Facebook: Did anyone really quit?', The Guardian, 1 June 2010.

'The question posed in your letter asks whether Facebook shares users' personal information with third parties without the knowledge of users. The answer is simple and straightforward: we do not. We have designed our system and policies so that user information is never shared without our users' knowledge.' [33]

A year after the first Quit Facebook Day, the company launched a disturbingly powerful new facial recognition system, 'Tag Suggestions', which compared newly uploaded photos to those in its database of the user's friends – and was turned on by default for every user. The ostensible purpose was to suggest that the user tagged these friends into the photos, but observers were not slow to point out that the system could, in conjunction with other AI systems, be put to many other, less benign uses.

WHAT'S IN A FACE?

The ability of facial recognition systems to do more than simply identify people was to prove of great interest to Michal Kosinski, a psychologist who has worked extensively with Facebook data.

In 2013, as a PhD student at Cambridge University's Psychometrics Centre, Kosinski co-authored a paper on personality analysis, using behavioural data harvested from some 58,000 people via a Facebook app. It demonstrated a strong relationship between these people's Facebook likes and their psychological and demographic traits. This might seem obvious enough, but Kosinski and his co-authors were able to show that the algorithm they had developed, if supplied with enough data, could make more accurate assessments of a person's personality than their real-life friends. Kosinski claims that Mark Zuckerberg and other Facebook staff were well aware of his research.

Kosinski went on to publish a paper claiming to show how algorithms applied to facial analysis could be used to detect personal characteristics including IQ, a predisposition to commit certain types of crime, and even to distinguish between gay and straight people. He also claims to have used similar techniques to distinguish between the faces of Republicans and Democrats.[34]

This research was plainly of more than academic interest, as was a subsequent paper of Kosinski's in 2017, which described how assessing psychological traits from digital footprints could be used effectively for:

'…psychological mass persuasion—that is, the adaptation of persuasive appeals to the psychological characteristics of large groups of individuals with the goal of influencing their behavior. On the one hand, this form of psychological mass persuasion could be used to help people make better decisions and lead healthier and happier lives. On the other hand, it could be used to covertly exploit weaknesses in their character and persuade them to take action against their own best interest, highlighting the potential need for policy interventions.'[35]

By the time this paper appeared, the world was becoming aware that such techniques had already been put into practice by a company that had shown a keen interest in Kosinski's earlier research and that of his university colleague Aleksandr Kogan: Cambridge Analytica. And the previous year, in the run-up to the US presidential election, Kosinski had accepted an invitation to share his insights with an unusual audience consisting of Russian politicians and state officials, as part of an 'educational day' in Moscow arranged by Sberbank Corporate University, a subsidiary of the sanctioned, Kremlin-linked bank.[36]

33 'Facebook Defends Privacy Policies', Juliana Gruenwald, Benton, 27 July 2010.

34 "I was shocked it was so easy': meet the professor who says facial recognition can tell if you're gay', Paul Lewis, The Guardian, 7 July 2018.

35 ' Psychological targeting as an effective approach to digital mass persuasion', S. C. Matz, M. Kosinski, G. Nave, and D. J. Stillwell, Proceedings of the National Academy of Sciences of the United States of America, 28 November 2018.

36 Paul Lewis, The Guardian, ibid.

2.8 THE 'INSIDER PIG PILE': FACEBOOK GOES PUBLIC

In May 2012, Facebook held its initial public offering (IPO), selling 421 million shares on the US Nasdaq exchange for an initial price of $38 per share, based on a valuation of the company at $104 billion.

While this was heralded as the biggest ever technology IPO, the stock price fell sharply in the days and weeks following the offering. Commentators noted that the real short-term winners were not investors who'd bought into the IPO, including pension funds and many Facebook employees, but Facebook's founders and venture capital backers. 'Facebook left nothing for the common investor,' commented Forbes publisher Richard Kilgaard. 'The insider pig pile of (private equity) firms and celebrity Silicon Valley angels took it all.' An equity analyst concurred: 'VCs made tons of money. Facebook employees got screwed.' [37]

One reason for the initial slump in Facebook's stock price was that its IPO valuation had been based on a figure of 108 times the company's 2011 earnings, which would require phenomenal revenue growth to be justified. Many observers were sceptical that Facebook advertising could deliver growth at this level. As one wrote:

Facebook may try to wring more revenue from the users it has through more or better advertising, in a bid to meet what will be insatiable investor demand for growth. But the company's users are sensitive to invasive marketing and major advertisers have already raised questions about the effectiveness of ads on the site.[38]

Despite such doubts, Facebook has proved an extremely lucrative investment for its backers. Between its IPO in May 2012 and the end of October 2018, it generated a 373.9% return for shareholders (not accounting for reinvested dividends).[39]

Shareholders of the company before the IPO have made many times this. Zuckerberg alone saw his personal wealth rise to some $19 billion on the day of the IPO, and by July 2018 it had climbed to over $80 billion, reflecting the company's market capitalisation of more than $600 billion.[40]

Three of Facebook's founders – Zuckerberg[41], Dustin Moscovitz and Eduardo Saverin – still hold very substantial stakes in the company. Recent filings with the US Securities and Exchange Commission (SEC) show Zuckerberg to hold 11.92 million Class A shares indirectly through a series of funds, along with 392.71 million Class B shares (which confer voting rights). The company's two-tier share structure means that although Zuckerberg controls around 30% of Facebook stock, he has well over 50% of voting rights in the company.[42]

Other major stakeholders include the WhatsApp founder Jan Koum, who became a Facebook director after WhatsApp was acquired by Facebook in 2014 and remained on its board till April 2018; Facebook's chief operating officer Sheryl Sandberg; and the company's chief technology officer Michael Schroepfer.

FRIENDS WITH BENEFITS?

Several venture capital firms that invested in Facebook before its IPO remain major stakeholders, and there has recently been considerable speculation as to whether some of these may have had other types of gain in mind in addition to the purely financial.

In 2009, the company announced a $200 million investment by the venture capital firm Digital Sky Technologies (DST), with another $100 million in further investment by the company planned. 'DST stood out because of the global perspective they bring,' Zuckerberg explained.

DST was owned by the Russian billionaire investor Yuri Milner, who was also making other multi-million-dollar investments in US tech firms at the time (he went on to become one

37 'Facebook IPO underscores shutting out the masses', James Temple, SFGATE, 22 May 2012.

38 Ibid.

39 'The Top 6 shareholders of Facebook', J. B. Maverick, Investopedia, 30 October 2018.

40 Facebook Market Cap 2009-2018, Macrotrends.net, accessed 4 December 2018.

41 In early July 2018, Zuckerberg's personal wealth was estimated by Forbes at $82.4 billion, though it was dented by the revelations later that month that hit Facebook's stock price. See: 'Mark Zuckerberg's Net Worth Tumbles $18.8 Billion, More In One Day Than Ever Before', Angel Au-Yeung, Forbes, 25 July 2018.

42 Maverick, ibid.

of Twitter's largest investors). It later emerged Mr Milner had close connections with the Kremlin and with oligarchs close to Vladimir Putin, and that DST's Facebook investment was financed in part by Gazprom Investholding, a subsidiary of the state-controlled Russian energy company Gazprom.

Gazprom Investholding is described by Ilya Zaslavskiy of the Kleptocracy Initiative as being 'used for politically important and strategically important deals for the Kremlin'. The Gazprom money flowed into DST via loans to Kanton Services, a company registered in the British Virgin Islands and used as an investment vehicle by the Uzbek-Russian oligarch Alisher Usmanov, who was also a director of Gazprom.[43]

Yuri Milner's career in Russia before moving to Silicon Valley had seen him work closely with Usmanov to build a large stake in one of Russia's largest internet companies, Mail.ru, where Milner served as CEO till 2003 and remained chairman of the board until 2012.

In April 2018, Wired magazine revealed that not only had Mail.ru run hundreds of apps on Facebook that would have enabled it to collect users' data without their consent, but that Facebook had granted it a special extension to allow it to continue doing so even after the company changed its rules in 2014 to stop such third-party data collection. It is not known to what uses the data collected in this way was put, but as former US diplomat Brett Bruen comments: 'If you are a Russian businessperson of a certain scale, you can't escape the requirements Russian intelligence services are going to put on you. This is the reality of doing business in Russia today'.[44]

It is also worth noting that among Facebook's early investors was the app developer Marc Pincus, founder of Zynga – the company whose Farmville app helped set the trend for harvesting of Facebook users' data by third-party apps.[45]

2.9 INSATIABLE DEMAND FOR GROWTH

In response to investors' demand for growth to fulfil the company's price/earnings ratio, Facebook stepped up its efforts to wring revenue out of its operations and to enter new markets – geographical and in terms of online and mobile services – in which to do this. Even before the IPO, it had acquired image-sharing site Instagram in April 2012. Other major acquisitions that followed included facial recognition platform Face.com later that year and instant messenger app WhatsApp in 2014 (the latter purchase was accompanied by a major surge in Facebook's stock price).

Announcing the $19 billion WhatsApp acquisition, Zuckerberg deployed the by-now familiar Facebook rhetoric of inclusivity, framing the takeover as an act of philanthropy:

'Our mission is to make the world more open and connected. We do this by building services that help people share any type of content with any group of people they want. WhatsApp will help us do this by continuing to develop a service that people around the world love to use every day […] We also expect that WhatsApp will add to our efforts for Internet.org, our partnership to make basic internet services affordable for everyone.' [46]

Over the next four years, WhatsApp was indeed to become massively popular in developing countries and by the end of 2017 it had 1.5 billion users worldwide, even more than the 1.3 billion users of Facebook Messenger. 'Now Facebook is finally getting serious about monetising WhatsApp with the recent launch of the WhatsApp for Business app,' reported TechCrunch in early 2018. 'Facebook plans to charge business owners for additional commerce, customer service or broadcasting tools. And with such a massive audience, merchants will be clamouring for them.'[47] So much for philanthropy.

43 ' Kremlin Cash Behind Billionaire's Twitter and Facebook Investments', Jesse Druckernov, The New York Times, 5 November 2017.

44 'Facebook gave a Russian Internet giant a special data extension', Issie Lapowsky, Wired, 10 July 2018.

45 'The Roots of the Cambridge Analytica Scandal: How FarmVille helped users become comfortable giving away their Facebook data', Lila Thulin, Slate, 26 March 2018.

46 'Mark Zuckerberg's full statement on Facebook buying WhatsApp', Mark Zuckerberg, The Guardian, 20 February 2014.

47 'WhatsApp hits 1.5 billion monthly users. $19B? Not so bad', Josh Constine, TechCrunch, February 2018.

WHATSAPP LYNCH MOBS

The effectiveness of WhatsApp in helping people 'share any type of content with any group of people they want' was demonstrated by a spate of mob lynchings in India in 2018, when rumours of child abductions were spread by false messages and doctored videos shared on the messaging service.

In one such incident an innocent man was brutally beaten and his friend killed, with eight police officers who tried to protect them also injured. A BBC reporter spoke to one of the villagers who witnessed the violence:

'I think there were around 1,000 people,' says Vijay Patil, an eyewitness who owns a tea stall in Murki. 'We all received the video on the group,' he says, adding that he left the group that night after seeing what a 'single video on WhatsApp had done'.[48]

Similar WhatsApp lynchings have been reported from other countries. In Mexico, for instance, a mob responded to child abduction rumours spread on WhatsApp in the state of Puebla in August 2018 by burning two men to death. Photos of the incident show a crowd holding up their mobile phones to capture video of the burning victims to share with their friends.[49]

On the advertising front, continued rapid growth in user numbers and aggressive marketing tactics led to steep growth in revenues, rising to nearly 40 billion dollars in 2017 despite a fall in the number of user hours spent on the platform.

Commenting on that year's figures, Zuckerberg appeared to respond to growing concerns over the damaging impacts that content shared via Facebook was having worldwide, and over the phenomenon – by now widely recognised – of social media addiction:

'… we made changes to show fewer viral videos to make sure people's time is well spent. In total, we made changes that reduced time spent on Facebook by roughly 50 million hours every day. By focusing on meaningful connections, our community and business will be stronger over the long term.' [50]

Just what might be concealed by the phrase 'meaningful connections' was about to be revealed by the investigations described in Section 3 of this report.

FALSE IDENTITIES

The potential for Facebook to be used to disseminate disinformation and other damaging material under false or misleading identities has long been evident. In 2008, for example, a university admissions administrator noticed that a number of Facebook Groups purporting to be those of year groups of students at various US universities were in fact nothing of the kind but had been set up as a surreptitious marketing ploy by 'College Prowler', an organisation aiming to market products to these groups of students.[51]

Many of the problems relating to falsification of identities stem from Facebook's lax approach to user verification: in August 2012, the company revealed that more than 83 million Facebook accounts (8.7% of total users) were fakes, many of these used for various types of scam or spam.[52]

While the company has made some efforts to tackle this problem, the number of fake accounts has continued to multiply. In the first quarter of 2018 alone, in the wake of the Cambridge Analytica scandal, Facebook shut down 583 million fake accounts. Although many of these were detected soon after being set up, the company estimated that 3-4% of

48 'How WhatsApp helped turn an Indian village into a lynch mob', Deepthi Bathini, BBC News, 19 July.

49 'Burned to death because of a rumour on WhatsApp', Marcos Martínez, BBC News, 12 November 2018.

50 'Facebook ad revenue up 49% despite user number fall', Emily Tan, Campaign, 1 February 2018,.

51 'Company Created Official-Looking 'Class of 2013' Facebook Groups for Hundreds of Colleges', The Chronicle of Higher Education, 19 December 2008.

52 '83 million Facebook accounts are fakes and dupes', Heather Kelly, CNN, 3 August 2012.

53 'Facebook shuts down 583 million fake accounts as it reveals it is packed with abusive content', Andrew Griffin, The Independent, 15 May 2018.

its more than two billion monthly active users were also fakes.[53]

There have also been several high-profile instances of hackers simply stealing personal data of the sort typically used in identity fraud. In October 2018, for instance, the company revealed that a software vulnerability had allowed the theft of personal data from some 50 million users, in many cases including search history, location data and information about their relationships and religion.

Perhaps even more shocking than the theft itself was Facebook's reaction to it: unlike other major companies whose customers had suffered from similar data breaches, it said it had no plans to provide protection services for concerned users. Instead it referred them to a help page on its website.[54]

2.10 TRUST US, THIS TIME WE'VE REALLY CHANGED

Between 2012 and 2015, the rising clamour over abuse of Facebook users' personal data led to further investigations by regulatory authorities and legal action against the company by user groups. In 2011 and 2012 the Irish Data Protection Commissioner (IDPC) audited Facebook's European headquarters in Ireland and identified various issues related to Facebook users' control over how their own personal data and that of their friends was accessed. This was prompted in part by complaints made by Austrian data protection campaigner Max Schrems, who was by no means satisfied with the IDPC's failure to take strong action against the company. In 2014, Schrems mounted a class action on behalf of some 25,000 Facebook users in Europe, which alleged that Facebook's collection and use of data amounted to illegal mass surveillance.[55]

In response to the ongoing concerns, Facebook announced at its 2014 F8 developers' conference that it would be shutting down access to users' friends' data that had previously been granted to third-party apps, starting with any new apps that were launched. A year later, in April 2015, it stated that all Facebook apps would now be denied such access, and would have to conform with a new log-in system that required apps to get the specific consent of users for any data permissions they sought.

A company spokesman told reporters of Zuckerberg's enthusiasm for a new Facebook slogan, 'People First', because 'if people don't feel comfortable using Facebook and specifically logging into Facebook and using Facebook in apps, we don't have a platform, we don't have developers. When people are confident, they feel happier and use our stuff more, and that's what we're trying to achieve,' he explained.[56]

Once again, the people-friendly rhetoric masked a very different reality.

2.11 TRADING DATA FOR REVENUE

In December 2018 the UK House of Commons Digital, Culture Media and Sport Committee gained access to a dossier of emails and other documents that had been obtained from Facebook by the app developer Six4Three as part of legally required disclosure in a suit the company had brought against Facebook for 'destroying its business'. The documents gave the lie to the assurances Facebook had given in 2014 and 2015, and showed that it had continued to allow favoured app developers access to users' personal data and that of their friends, linking this to revenue that it could reap from the developers. As the committee's chair, Damian Collins, observed:

'Facebook have clearly entered into whitelisting agreements with certain companies, which

54 'Facebook hack victims will not get ID theft protection', Dave Hill, BBC News, 12 October 2012.

55 'Facebook users sue site over data collection, demand compensation for privacy breaches', Andrew Griffin, The Independent, 9 April 2015.

56 'Facebook Is Shutting Down Its API For Giving Your Friends' Data To Apps', Josh Constine, TechCrunch, 28 April 2015.

57 'Note by Damian Collins MP, Chair of the DCMS Committee', UK Parliament, 5 December 2018

meant that after the platform changes in 2014/15 they maintained full access to friends data […] The idea of linking access to friends data to the financial value of the developers relationship with Facebook is a recurring feature of the documents.' [57]

The disclosures also detailed the way in which Facebook had deliberately obscured the level of data harvesting that it was undertaking from users, particularly in regard to changes to its policies on the Android mobile phone system, which enabled the company to amass records of calls and texts sent by users.

Facebook's response to the exposure of these documents was characteristically misleading:

'We stand by the platform changes we made in 2015 to stop a person from sharing their friends' data with developers. Like any business, we had many internal conversations about the various ways we could build a sustainable business model for our platform. But the facts are clear: we've never sold people's data.' [58]

But the simple exchange of data for cash was not what the disclosures had shown. It was, rather, the granting of privileged access to data to developers and business partners who delivered a certain level of revenue to Facebook, even after the company had publicly announced that it was stopping this practice. This was further confirmed later the same month, when it was revealed that Facebook had given some of the world's largest technology companies far more intrusive access to users' personal data than it had disclosed, effectively exempting them from its privacy safeguards. This included enabling Microsoft's Bing search engine to see the names of virtually all Facebook users' friends without consent and allowing Netflix and Spotify to read Facebook users' private messages – a flagrant violation of the agreement that Facebook had made with the US Federal Trade Commission that it would not share user data without explicit permission.[59]

FUELLING INTERCOMMUNAL VIOLENCE IN SRI LANKA

In March 2018, posts spreading misinformation about and inciting violence against the Muslim community in Sri Lanka were made on Facebook pages in Sri Lanka, leading to widespread attacks on Muslims by Buddhist mobs. Videos contained in the posts and widely circulated claimed to show Buddhist temples being torched by Muslims.

Sri Lanka's telecommunications minister, Harin Fernando, said that Facebook had taken far too long to respond to requests to take down the inflammatory posts, pointing for instance to one post that read (in Sinhalese): 'Kill all Muslims, don't even let an infant of the dogs escape.' A Facebook user who alerted Facebook to the post 'received a reply six days later saying the post did not contravene a specific Facebook community standard'.

After days of violence and several deaths, the Sri Lankan government temporarily blocked Facebook, WhatsApp and other platforms in Sri Lanka. 'This whole country could have been burning in hours,' Fernando said. 'Hate speech is not being controlled by these organisations and it has become a critical issue globally.' [60]

2.12 BIGGER THAN ANY RELIGION

In June 2017, Facebook proudly announced that it had 'reached a new milestone: there are now 2 billion people connecting and building communities on Facebook every month'. This gave the company an opportunity to sound, once again, a messianic note:

'This wouldn't have happened without the millions of smaller communities and individuals

58 'Facebook Emails Show How It Sought to Leverage User Data', The New York Times, 5 December 2018

59 'Facebook gave Netflix and Spotify access to users' private messages', The Irish Times, 19 December 2018.

60 'Sri Lanka accuses Facebook over hate speech after deadly riots', Michael Safi, The Guardian, March 2018.

61 'Two Billion People Coming Together on Facebook', Facebook Newsroom, 27 June 2017.

who are sharing and making meaningful contributions every day. Each day, more than 175 million people share a Love reaction, and on average, over 800 million people like something on Facebook. More than 1 billion people use Groups every month […] Every day, people connect with one another, contribute to their local communities and help make the world a better place.[61]

As Christopher Ingraham wrote in The Washington Post, Facebook now had more users than any world religion had adherents, with the exception of Christianity and (it was to overtake Christianity just a few months later). In number terms, Facebook users also now outstripped the speakers of any single language. 'Likes, shares, comments and friend requests are becoming the closest thing humanity has to a universal tongue,' Ingraham enthused.[62]

Ingraham noted some of the many controversies in which the company had become embroiled, but was happy to shrug these off: 'Any service growing that quickly is bound to experience some mishaps.' His piece ended with the words:

'It's easy to forget that none of us – not even Facebook – have any idea what it truly means to have a quarter of humanity plugged into a single product, governed by a single set of rules and norms, uploading deeply personal information to a single database, making a single company the gateway between ourselves and the advertisers who want us to buy stuff. We just go with it, riding the tide of likes and shares into whatever Facebook's future holds for us.'

But Facebook's record over the past decade and a half gave ample reason to resist such a blithe acceptance that the company should be left to create whatever future it saw fit for humanity. And – as the next section of our report describes – all over the world, people were beginning to understand just what kind of a future this might be, and how Facebook had greatly empowered forces that posed a grave threat to the chances of democracy surviving within it.

Maximilian Schrems, an Austrian activist and author, became known for campaigns against Facebook for privacy violation, including its violations of European privacy laws and alleged transfer of personal data to the US National Security Agency as part of the NSA's PRISM program. *Wikimedia Commons/Author Josef Weidenholzer MEP*

62 'If Facebook were a religion, it would be the second largest in the world', Christopher Ingraham, The Washington Post, 30 June 2017.

3.0 THE ATTACK ON DEMOCRACY: RECENT FINDINGS

This section of our report summarises the findings of three recent inquiries that have shed light on the impact of Facebook's activities in the UK and other countries, bringing out common themes that have emerged, particularly in regard to Facebook's role in enabling certain actors to exercise undue political influence by the microtargeting of political advertising and disinformation. It also highlights policy recommendations made by the inquiring bodies that will be returned to in the report's final section.

3.1 DISINFORMATION AND 'FAKE NEWS' INQUIRY BY THE UK HOUSE OF COMMONS DIGITAL, CULTURE, MEDIA AND SPORT COMMITTEE

3.1.1 BACKGROUND

In early 2017, following media reports that Russia had made efforts to influence the result of the Brexit referendum of June 2016 and the subsequent US presidential election, the UK House of Commons Digital, Culture, Media and Sport (DCMS) Committee embarked on a wide-ranging inquiry into disinformation and so called 'fake news'. Its aim was to gain a clearer picture of 'the spread of false, misleading, and persuasive content, and the ways in which malign players, whether automated or human, or both together, distort what is true in order to create influence, to intimidate, to make money, or to influence political elections.'[63]

Throughout 2017 and 2018, the committee heard hundreds of hours of evidence from a wide variety of expert witnesses and from people who had been close to the interface between tech platforms and political propaganda. It also received many thousands of pages of written evidence. In July 2018, it published an interim report, which noted: 'Such has been the impact of this agenda, the focus of our inquiry moved from understanding the phenomenon of 'fake news', distributed largely through social media, to issues concerning the very future of democracy.'

As the inquiry progressed, it found extensive evidence indicating that Facebook's platform and the personal data of Facebook users had been central to efforts to manipulate voters in the UK. Prompted in part by investigative journalism by Carole Cadwalladr of the Observer[64], Channel 4 News and The New York Times, the committee focused in particular on the use of such data by three closely associated companies: SCL Group, Cambridge Analytica and AggregateIQ.

3.1.2 CAMBRIDGE ANALYTICA/SCL

Cambridge Analytica was born out of an existing political consultancy, SCL Group, which had developed 'specialist communications techniques previously developed by the military' and turned these to political purposes for paying clients. It was started with the backing of the US hedge-fund billionaire Robert Mercer and the influential right-wing ideologue Steve Bannon, who served as the company's Vice President (Bannon was also the executive chairman of the 'alt right' website Breitbart and went on to serve as Donald Trump's chief strategist).

The committee found the precise ownership details of SCL and Cambridge Analytica exceptionally hard to establish, due to a complex and shifting web of cross-ownership between closely associated UK and US companies. In August 2017 a new ultimate holding company for Cambridge Analytica and SCL Group companies was set up: Emerdata Limited. Its directors

63 Disinformation and 'fake news': Interim Report, House of Commons Digital, Culture, Media and Sport Committee, UK Parliament, 29 July 2018. All quotes in this section are from this report, unless otherwise noted.

64 Carole Cadwalladr's investigative journalism has since been recognised by several awards. Ahead of her initial report into the harvesting of Facebook data, the Guardian Media Group, which owns The Observer, received a threat of legal action from Facebook in an attempt to prevent its publication. See: 'Facebook says warning to Guardian group 'not our wisest move', Jamie Grierson, The Guardian, 23 March 2018.

included Cambridge Analytica's CEO Alexander Nix and several other directors of SCL Group companies, as well as, from March 2018, Rebekah and Jennifer Mercer, daughters of Robert Mercer. Emerdata is chaired by Erik Prince, founder of the controversial private military group Blackwater USA.

Much of the detailed information on SCL/Cambridge Analytica's activities that the committee took was from two of the companies' former employees, Christopher Wylie and Brittany Kaiser. It was also able to question Cambridge Analytica's CEO Alexander Nix, though much of the evidence he gave was to prove misleading or simply false.

Nix described how psychological profiling underpinned Cambridge Analytica's work, enabling it to target particular voters with messages that would have a strong emotional appeal. He claimed that the information on voters that it used for this purpose was based on 'first-party research, being large, quantitative research instruments, not dissimilar to a poll'. He also claimed that the company did not work with or hold Facebook data, though it uses Facebook as a platform for advertising and 'as a means to gather data' via surveys 'that the public can engage with if they elect to'.

As the committee found, this was far from the truth. Much of the data used by Cambridge Analytica derived in fact from a company called Global Science Research, founded by Aleksandr Kogan, a researcher at Cambridge University's Department of Psychology. Kogan told the committee how he had developed a personality quiz app, 'this is your digital life', to collect data from Facebook users and their friends. As he explained: 'It is not technically challenging in any way. Facebook explains how to do it.'

In 2014 SCL/Cambridge Analytica paid Kogan several hundred thousand dollars for the data itself, then more for personality profiling based on this. His contract with the company required him to match predictive personality scores, including individuals' likely political interests, to named individuals on the electoral register of various US states in which SCL was then involved in political campaigns for Republican candidates. SCL later boasted that it had used behavioural micro-targeting to support 1.5 million advertising impressions during the US mid-term elections in November 2014, achieving 'a 30% uplift in voter turnout, against the predicted turnout, for the targeted groups'.

The committee found that the misuse of Facebook data that Kogan passed to Cambridge Analytica was 'facilitated by Facebook', and that this data had been 'manipulated into micro-targeting [by] Cambridge Analytica and its associated companies, through AIQ' (see below).

Cambridge Analytica and SCL Elections Ltd were wound up in the summer of 2018 in the wake of the scandal that had enveloped them. However, as the committee noted, 'other companies are carrying out very similar work. Many of the individuals involved in SCL and Cambridge Analytica appear to have moved on to new corporate vehicles'.

3.1.3 AGGREGATEIQ (AIQ)

The digital advertising and software development company AggregateIQ (AIQ) was set up in 2013 to create various digital tools to assist Cambridge Analytica's parent company SCL in its political campaigning work in various countries. One of these was the 'Ripon' tool, which Cambridge Analytica whistleblower Christopher Wylie described as 'software that utilised the algorithms from the Facebook data'. Based in Canada, AIQ was supplied with personal data of UK voters by the Vote Leave campaign (the legality of this was a matter of interest to the UK Information Commissioner and to Canada's privacy and information authorities, whose reports are described later in this section). This data was used to target Facebook ads on British voters during the Brexit referendum campaign.

The DCMS committee also saw evidence indicating that AIQ had used an app called 'uCampaign', developed by a company of that name, which was deployed in both the Trump campaign and by Vote Leave's Brexit referendum campaign. This app, which harvested the personal data of Facebook users and their friends and matched this against voter records, had been developed by an Eastern Ukrainian military veteran with the financial backing of American hedge fund magnate Sean Fieler, a close associate of Cambridge Analytica's main backer, Robert Mercer.

The committee noted that 'AIQ had links with Vote Leave and other Brexit campaigns, including Be Leave, Veterans for Britain and the DUP and all used the company in the short period immediately prior to the EU Referendum.' Vote Leave had spent a very large part of its referendum budget with the company and had been referred by the UK Electoral Commission to the Metropolitan Police for illegally co-ordinating such spending with other, supposedly separate Brexit campaign groups in order to circumvent UK laws governing such spending. The DCMS Committee also noted that evidence from Facebook showed that the supposedly separate Brexit campaign group BeLeave used datasets covering the 'exact same audiences' as those addressed by the digital advertising microtargeted by AIQ for Vote Leave.

Despite repeated requests, Vote Leave's campaign director, Dominic Cummings, refused to appear in front of the Committee to give evidence. [65]

3.1.4 DATA ABUSES

The DCMS Committee found Facebook and its users' personal data to have played a central role in efforts by Cambridge Analytica, AIQ and their clients to influence the results of key votes in the US and the UK.

The data in question had been 'scraped' from Facebook users and their friends by the app developed by Dr Kogan. This was technically in breach of the company's then recently revised terms of service. Whistleblower Christopher Wylie described the Facebook data obtained by Dr Kogan's app as Cambridge Analytica's 'foundation dataset', and said the company had collected data on up to 87 million users, the majority in the US but also including over one million in the UK.

As the previous section of this report has shown, Kogan's attitude to Facebook user data was shared by many other app developers and was one that the company itself had done much to foster. This was confirmed to the DCMS committee by former Facebook employee, Sandy Parakilas, who said that in his experience there had been no attempt by Facebook to establish an audit trail of data obtained by third parties, and that 'once the data passed from Facebook servers to the developer, Facebook lost insight into what was being done with the data and lost control over the data'. As the committee and the Information Commissioner's Office were to discover, Cambridge Analytica had not deleted the data when requested to by Facebook.

Tristan Harris of the Center for Humane Technology explained to the committee that the entire premise of Facebook's app platform was to enable third-party developers to have access to people's friends' data, 'to enable as many developers as possible to use that data in creative ways, to build creative new social applications on behalf of Facebook.'

3.1.5 MONOPOLISTIC BUSINESS MODEL

The DCMS committee observed that many of the problems stemming from the spread of disinformation on Facebook could be traced to the company's core business model, which – as one of its former employees testified and as this report has also detailed – focuses above all else on growth in user numbers and revenues.

65 AIQ's website at one point carried a testimonial from Cummings that ran as follows: 'Without a doubt, the Vote Leave campaign owes a great deal of its success to the work of AggregateIQ. We couldn't have done it without them.' See 'Facebook suspends AIQ data firm used by Vote Leave in Brexit campaign', BBC News, 7 April 2018.

The success of Facebook and a handful of other tech companies has, the committee noted, 'resulted in their behaving as if they were monopolies in their specific area'. This has been helped by their providing free access to their services, funded by the exploitation of their users' data to maximise revenues.

The report observed that 'the users become the product of the companies, and this is where issues of mistrust and misuse arise'. While traditional control of monopoly power has focused on consumer pricing, protection of consumers against the power of the tech monopolies is more about the protection of data.

In poorer countries, Facebook's pursuit of market share has led the company to offer free access to services (without data charges) to anyone with a mobile phone, enabling it to become effectively a monopoly provider of online information for many millions of people. In Myanmar, noted the committee, this put it in an ideal position to be exploited by the country's military as a platform for disseminating hatred for the Rohingya Muslim minority, using disinformation and fake accounts.

The committee also observed that, while deploring the torrent of hate speech that had been released upon this minority with horrendous results (massacre, mass rape and the forced displacement of hundreds of thousands), Facebook's CTO 'could not tell us when Facebook had started work on limiting hate speech, he could not tell us how many fake accounts had been identified and removed from Burma, and he could not tell us how much revenue Facebook was making from Facebook users in Burma'.

It concluded that:

'Facebook is releasing a product that is dangerous to consumers and deeply unethical […] This is a further example of Facebook failing to take responsibility for the misuse of its platform.'

3.1.6 PLATFORM OR PUBLISHER?

One strand of the committee's report focused on whether Facebook should be considered as a publisher – with all of the responsibilities that entails – or as a mere channel, with no more responsibility for the content that it carries than a telephone line. Facebook has been keen for itself to be seen as the latter, but, as the committee observed, its algorithms are constantly making decisions on which content to prioritise for particular users, an editorial function more typical of a publisher.

The DCMS committee noted that some countries have taken a much tougher approach than others to regulating the kind of content that Facebook displays, treating it in effect as a publisher. Germany's Network Enforcement Act (NetzDG), for instance, which became law in January 2018, forces tech companies to remove hate speech from their sites within 24 hours or incur fines of up to €20 million. As the committee noted, 'one in six of Facebook's moderators now works in Germany, which is practical evidence that legislation can work'.

The DCMS committee recommended that UK lawmakers consider formulating 'a new category of tech company […] which tightens tech companies' liabilities', and that these should include liability for and responsibility to act against harmful and illegal content on their platforms, so that failure to act 'could leave them open to legal proceedings launched either by a public regulator, and/or by individuals or organisations who have suffered as a result of this content being freely disseminated on a social media platform'.

3.1.7 RUSSIAN USE OF FACEBOOK FOR POLITICAL INTERFERENCE

Aware that the US Congress had uncovered evidence of extensive use of Facebook by the Russian government to interfere in the US presidential election of 2016, using sophisticated targeting techniques and creating customised audiences 'to amplify extreme voices in the campaign, [in] particular those on sensitive topics such as race relations and immigration,' the DCMS Committee sought to investigate whether the same had occurred during the Brexit referendum campaign in the UK and in the Catalonian independence referendum of 2017.

Its efforts to do so ran up against a brick wall. Facebook claimed that payment for political ads in the UK from Russian sources had been minimal, but as the committee reported: 'Time and again, Facebook chose to avoid answering our written and oral questions, to the point of obfuscation.'

Paid ads were anyway not the only way in which Russia may have been able to use Facebook-derived data (see box below). The committee heard that some of the systems that had used the data harvested by Dr Kogan's third-party app and passed on Cambridge Analytica and AIQ 'were accessed from IP addresses that resolve to Russia and other areas of the CIS (Commonwealth of Independent States)'. It expressed its concern that 'people in Russia could have benefitted from the work that Dr Kogan carried out in the UK, in connection with his work for Cambridge Analytica'. Kogan himself had worked on a Russian government-financed project in St Petersburg at the same time as he was working with Cambridge Analytica.

Following publication of its interim report, the committee received evidence showing that a Facebook engineer 'had warned the company in 2014 that users apparently based in Russia were scooping vast amounts of data from the site on a daily basis.' [66]

3.1.8 'DARK ADS'

The DCMS committee also looked more generally at political advertising online, noting that 'this creates new issues in relation to the regulation of elections, including the nature of content and the cost of dissemination'.

It was particularly concerned by so-called 'dark ads' micro-targeted on voters, quoting a recent report from the UK Electoral Commission: 'Only the voter, the campaigner and the platform know who has been targeted with which messages. Only the company and campaigner know why a voter was targeted and how much was spent on a particular campaign.'

It noted evidence from Facebook that the company had no way of categorising which adverts could be classified as political, and therefore no way of monitoring such ads:

'Our systems do not have a perfect or reliable way to classify the category that advertisements (which are developed and distributed by third-parties on our platform) fall in, whether it is political or housing or educational or otherwise.'

The committee recommended an overhaul of UK law around digital campaigning, to cover also online adverts with political intent that are not sponsored by a specific political party:

'There should be public register for political advertising, requiring all political advertising work to be listed for public display so that, even if work is not requiring regulation, it is accountable, clear, and transparent for all to see. There should be a ban on micro-targeted political advertising to lookalikes [i.e. individuals selected on the basis of their resemblance to other profiled individuals] online, and a minimum limit for the number of voters sent individual political messages should be agreed, at a national level.'

66 'Facebook was warned of apparent Russian data trawl in 2014, MPs told', The Guardian, Emma Graham-Harrison and Jim Waterson, 27 November 2018.

RUSSIAN USE OF FACEBOOK AND INSTAGRAM IN THE US

In December 2018, The Oxford Internet Institute's Computational Propaganda Research Project published a report for the US Senate Intelligence Committee on the social media activities of Russia's so-called 'Internet Research Agency' (IRA) in the US between 2013 and 2018.

It found that:

'In total, IRA posts were shared by users just under 31 million times, liked almost 39 million times, reacted to with emojis almost 5.4 million times, and engaged sufficient users to generate almost 3.5 million comments […] On Instagram, a similar pattern is evident. In total, all Instagram posts garnered almost 185 million likes and users commented about 4 million times.'

The report concluded that the IRA had been highly effective in 'spreading sensationalist, conspiratorial, and other forms of junk political news and misinformation to voters across the political spectrum, polarising opinion and supporting Donald Trump's campaign.' [67] It also noted that the impact of these 'organic' posts had been far greater than that of the relatively limited paid advertising from Russian sources that Facebook had (under pressure) identified and disclosed. No similarly in-depth study has been carried out on Russian use of social media to interfere in UK politics.

3.1.9 INADEQUACY OF SELF-REGULATION

Self-regulation by tech and social media companies was not sufficient, in the committee's view:

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

The question of who is paying for political advertising was also addressed:

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

The report called for the UK Electoral Commission to establish a code to govern advertising via social media during election periods, and to consider whether this should be restricted to registered political organisations or campaigns. It also called for closer scrutiny of 'the ethics of Facebook or other relevant social media companies selling lookalike political audiences to advertisers […] using the data they hold on their customers to guess whether their political interests are similar to those profiles held in target audiences already collected by a political campaign'. It suggested that regulation might include a right for users of Facebook and other social media platforms to opt out from being included in such lookalike audiences.

67 The IRA, Social Media and Political Polarization in the United States, 2012-2018, Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly and Camille Francois, University of Oxford, 2018.

3.1.10 LACK OF TRANSPARENCY AND REFUSAL TO TAKE RESPONSIBILITY

The DCMS Committee report expressed frustration at the way in which Facebook had continually stonewalled its efforts to get information about the company and its activities:

Facebook consistently responded to questions by giving the minimal amount of information possible, and routinely failed to offer information relevant to the inquiry, unless it had been expressly asked for. It provided witnesses who have been unwilling or unable to give full answers to the Committee's questions.

The committee's verdict on Facebook's overall role was damning:

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

TOO BIG TO CARE?

Some of the most interesting evidence on Facebook heard by the committee came in December 2018 after it had issued its interim report, from Ashkan Soltani. Having worked as a primary technologist at the US Federal Trade Commission (FTC) on the FTC's investigation into Facebook in 2010-11, Soltani went on to become chief technologist at the FTC. Watching livestreamed evidence taken by the committee from Richard Allan, Facebook's Vice President of Policy Solutions, Soltani had been so disturbed by what he saw as Allan's mendacity that he immediately approached the committee to offer evidence of his own.

He described how Facebook apps were routinely able to bypass user privacy settings to gain access to a wealth of user data, and some were able to access such data even without a user installing them. He observed:

'I do not think Facebook is able to govern itself in this area. From my observations of public data as well as my conversations with multiple stakeholders inside the company, my understanding is that senior leadership simply does not prioritise these issues seriously and they will continue to do the bare minimum necessary to pass through the compliance regimes, but will absolutely continue to make these mistakes as their priority is monetisation of user data.'

Asked whether Facebook had simply grown 'too big to care', Soltani replied:

'If laws are mandated, I think that they will comply with those laws. I think they have a lot of influence, both politically and economically. In the US, a lot of the reticence to pass strong policy has been about killing the golden goose; it is a leading sector in the US economy and there is a lot of worry that regulation will hamper that. I think that is short-sighted. For me, the policy debate is similar to the environmental policy debate 50 years ago, where there was worry about clamping down on companies for emissions and for environmental harm. We found that, actually, by doing so, we incentivised a great deal of innovation around solar energy or renewable fuels. The same is true of this industry.' [68]

68 Oral evidence to the Digital, Culture, Media and Sport International Grand Committee, UK Parliament, 27 November 2018.

3.2 INVESTIGATION INTO THE USE OF DATA ANALYTICS IN POLITICAL CAMPAIGNS BY THE UK INFORMATION COMMISSIONER'S OFFICE

3.2.1 BACKGROUND

In May 2017 the UK Information Commissioner's Office (ICO) launched an investigation into the use of data analytics for political purposes after allegations were made about the 'invisible processing' of personal data and the micro-targeting of political adverts during the EU referendum campaign. The investigation became the largest of its type by any data protection authority and covered several aspects, including the use of personal data by political parties and data analytics companies. However, it is the use of online social media platforms and user data harvested from these, and in particular from Facebook, on which our summary focuses.

The investigation spoke to over 100 'persons of interest' and engaged with 172 organisations. Some 700 terabytes of data – the equivalent of 52.2 billion pages – were examined in the course of the investigation and the ICO made full use of its powers to obtain evidence, including attending premises to seize relevant material. The ICO also worked with several other agencies in the UK, including the Electoral Commission and the National Crime Agency, and with its counterpart authorities in Canada and the United States.

Ahead of publication of the report into its investigation in November 2018[69], in July of that year the ICO brought out a separate report, Democracy Disrupted? Personal Information and Political Influence[70], covering policy recommendations that related to its ongoing investigation. This summary also references the latter report.

3.2.2 TRANSPARENCY

A key focus in the ICO's report on its investigation was transparency. As it noted:

'If voters are unaware of how their data is being used to target them with political messages, then they won't be empowered to exercise their legal rights in relation to that data and the techniques being deployed, or to challenge the messages they are receiving.'

The Information Commissioner found that 'between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information, without sufficiently clear and informed consent.'

The ICO looked in particular at the way in which the data of up to 87 million people worldwide (including at least one million in the UK) had been harvested by the apps developed by Dr Kogan (see Section 3.1 above) and a subset of this data passed on to Cambridge Analytica and other parties for use in political microtargeting. It found that Facebook users had not been made aware:

- that their personal data would be provided to CA;
- that their personal data would be used for the purposes of political campaigning;
- that their personal data would be processed in a manner that involved drawing inferences about their political opinions, preferences and their voting behaviour.

It also found that Facebook 'failed to keep the personal information secure because it failed to make suitable checks on apps and developers using its platform'.

In addition, the ICO found that Facebook had had a close working relationship with academics working on research of the type Dr Kogan developed, and that 'this included many individuals involved in research eventually going on to work at the company'.

Dr Kogan and Alexander Nix both refused requests from the ICO to provide accounts of the events in question.

69 Investigation into the use of data analytics in political campaigns: A report to Parliament, Information Commissioner's Office, 6 November 2018. Quotes in this section are from this source, uncles otherwise noted.

70 Democracy disrupted? Personal information and political influence, Information Commissioner's Office, 11 July 2018.

3.2.3 USES OF DATA FOR POLITICAL ADVERTISING

The ICO looked also at AggregateIQ (AIQ), the Canada-based company closely associated with Cambridge Analytica/SCL (see Section 3.1.3 above) and in particular at its relationship with Vote Leave and other Leave campaign groups during the EU referendum campaign.

It found that AIQ had created and placed advertisements for these Leave campaign groups, targeting these on individuals based on Facebook data and paying Facebook some $2 million for these placements. It found evidence to suggest that there may have been illegal co-ordination between different campaign groups (e.g. sharing of the same datasets). This evidence was passed to the UK Electoral Commission, which has subsequently referred some individuals to the UK police for investigation.

Although it found no evidence to show that the Kogan/Cambridge Analytica Facebook user data had been used for targeting undertaken for these campaign groups, the ICO was concerned by the fact that personal data of UK citizens had been passed to the company by Vote Leave and was still held by AIQ. The ICO issued an enforcement notice to AIQ, ordering the company 'to cease processing any personal data of UK or EU citizens obtained from UK political organisations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes'.

The ICO is continuing to investigate how Vote Leave delivered electronic marketing communications and whether its actions contravened PECR (Privacy and Electronic Communications Regulations).

3.2.4 OUTCOMES AND CONCLUSIONS

The ICO's main recommendations on the uses of online platforms for political campaigning were contained in its 'Democracy Disrupted' report, and included:

- Working with EU data protection authorities to ensure compliance with GDPR, to improve users' understanding of how their data is processed for political advertising, and to ensure that clear and effective privacy controls are easily available to users;
- Urgent roll-out of better transparency features by online platforms;
- Legislation by the UK government to introduce a statutory code of practice for use of personal data in political campaigns;
- Third-party audits after referendum campaigns to ensure personal data held by campaigners is deleted or, if shared, that appropriate consent has been obtained;
- A government review of regulation of online political advertising, to include consideration of requirements for digital political advertising to be archived in an open data repository to enable scrutiny and analysis.[71]

To reflect the seriousness of the breaches of transparency and data protection laws that it had uncovered at Facebook, the ICO issued the company with a penalty of £500,000, the maximum possible under the relevant data protection law at the time of the offences. It also referred outstanding 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, the lead authority in the EU for Facebook (whose European headquarters are in Dublin) under the General Data Protection Regulation (GDPR).

In a message prefacing the report into its investigation, Information Commissioner Elizabeth Denham wrote:

71 Democracy disrupted? Personal information and political influence, ibid.

'When we opened our investigation into the use of data analytics for political purposes in May 2017, we 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 […]'

Parliamentarians, journalists, civil society and citizens have woken up to the fact that transparency is the cornerstone of democracy. Citizens can only make truly informed choices about who to vote for if they are sure that those decisions have not been unduly influenced.

The invisible, 'behind the scenes' use of personal data to target political messages to individuals must be transparent and lawful if we are to preserve the integrity of our election process.

We may never know whether individuals were unknowingly influenced to vote a certain way in either the UK EU referendum or the in US election campaigns. But we do know that personal privacy rights have been compromised by a number of players and that the digital electoral ecosystem needs reform.[72]

Ms Denham stressed that voluntary initiatives by social media platforms were insufficient to address these issues and that 'a self-regulatory approach will not guarantee consistency, rigour or public confidence'. As Section 2 of this report has described, she had good reason not to trust any assurances from Facebook that it would address such issues internally: it had given just such assurances to the Office of the Privacy Commissioner of Canada following an investigation she had supervised while working there in 2009 – and had then completely failed to act on them.

Ms Denham concluded: *'This is a global issue, which requires global solutions.'*

3.3 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 OF THE CANADIAN PARLIAMENT

3.3.1 BACKGROUND

In March 2018, the Standing Committee on Access to Information, Privacy and Ethics of the Canadian Parliament's House of Commons began to investigate abuses of personal data involving Cambridge Analytica, AggregateIQ and Facebook. It soon realised that these breaches were 'the tip of the iceberg' and raised 'broader questions relating to the self-regulation of platform monopolies, the use of these platforms for data harvesting purposes, and their role in the spreading of disinformation and misinformation around the world'.

In June 2018, the committee's interim report noted its concern 'that the Canadian democratic and electoral process is vulnerable to improper acquisition and manipulation of personal data' and made a number of preliminary recommendations regarding Canadian privacy laws. The committee's full report was published in December 2018, and is summarised here.[73]

On some central aspects – particularly the role of AggregateIQ (AIQ) – the committee coordinated its investigation with those being run concurrently by the UK Information Commissioner and the UK Parliament's DCMS Committee (see sections 3.1.3 and 3.2.3 above). Many of its findings drew on and/or corroborated those investigations, so this summary will focus in particular on the Canadian committee's findings in regard to the role of Facebook and to problems associated with social media companies more generally.

72 Investigation into the use of data analytics in political campaigns: A report to Parliament, ibid..

73 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, Canadian Parliament House of Commons, December 2018. All quotes in this section are from this source unless noted otherwise.

3.3.2 AGGREGATEIQ AND FACEBOOK DATA

The committee was able to question Zackary Massingham, CEO of AIQ, as well as Jeff Silvester, the company's Chief Operating Officer. They stated 'that AIQ had no relationship with Cambridge Analytica or SCL Group (SCL), that they had never seen evidence that the organisations Vote Leave and BeLeave coordinated on the Brexit campaign, and that they were unaware that the personal information provided by SCL had been illegally obtained from Facebook'. However, the committee found much reason to doubt these assertions, finding their evidence 'inconsistent, full of contradictions and contrary to the testimony of several other reliable witnesses'.

3.3.3 STRUCTURAL PROBLEMS IN THE 'INFORMATION ECOSYSTEM'

One section of the committee's report was especially interesting in the light it threw on problems that went deeper than the immediate abuses of personal data revealed by the Cambridge Analytica scandal.

A number of expert witnesses drew attention to problems in what the committee referred to as the 'information ecosystem'.

Dr Taylor Owen, Assistant Professor of Digital Media and Global Affairs at the University of British Columbia, explained that 'developments in social media in recent years have created a new structure that determines what is acceptable and sets the boundaries on public debate: the platforms' filtering mechanisms, which decide what people see and whether our content will be seen'. He identified two aspects of this digital infrastructure that are especially damaging.

One is the monetisation of the platforms and their users, which creates a so-called 'attention economy' that:

'…requires commercialising our attention and behavioural changes. Platform algorithms prioritise entertainment, shock, and radicalisation over reliable information. This is embedded in the business model. This is why research shows, for example, that misinformation spreads further and faster than genuine news.'

The other was that the experience of social media users is increasingly determined by unaccountable AI systems which, when set up to drive revenues by maximising user engagement with content, 'filter the most engaging content to us, to know what will rile us up and engage us, to determine what we see as an individual user and whether we are seen and heard inside these platforms.' One result of this is 'fragmentation and the vulnerability of elections', as individual users are exposed to a constant stream of information 'designed to reinforce and harden their views'. This drives polarisation and is 'increasingly leading to actual physical manifestations of individual and collective violence'. It also creates favourable conditions for foreign governments or malign actors wishing to exacerbate social division and influence voter behaviour in other countries.

Reinforcing this point, Claire Wardle, of First Draft, a non-profit organisation focused on the effects of online media, observed that: 'The problem is that deceptive content is often what generates the strongest reactions and is being promoted'.

Ben Scott, Director of Policy and Advocacy at the Omidyar Network, said that in the social media environment *'all of the signals about source credibility and quality that we once had begin to attenuate […] We've lost the normative structure that in the old media environment allowed us as citizens to make implicit judgments about source credibility and, when we're reading digital media, to engage in critical thinking.'*

Tristan Harris, Co-Founder and Executive Director of the Center for Humane Technology, noted that: 'Self-optimising AI systems use algorithms to predict the best content to suggest to a given

individual, and the personalisation of user accounts enables billions of people to be targeted by personalised forms of manipulation.' And, as Dr Elizabeth Dubois, a social media expert at the University of Ottawa, explained, the way social media algorithms operate is currently a black box: 'We don't know how Facebook or Google decides what shows up and what doesn't.'

Like the DCMS committee, Harris called for social media companies to be thought of as publishers responsible for the content they promoted, given that this 'is fuelled by recommendations generated by the platforms, using AI that they have programmed'. This would mean that they became responsible for the social costs as well as the financial profits of their business model:

'Right now we have dirty-burning technology companies that use this perverse business model that pollutes the social fabric. Just as with coal, we need to make that more expensive, so you're paying for the externalities that show up on society's balance sheet, whether those are polarisation, disinformation, epistemic pollution, mental health issues, loneliness or alienation. That has to be on the balance sheets of companies.'

Having heard this and other expert evidence, the committee concluded that:

'The structural problems inherent in social media platforms serve to fuel the attention economy and help in the promotion of disinformation and misinformation to millions of addicted users. The Committee is very concerned about the negative externalities these platforms have.'

3.3.4 TRANSPARENCY IN ONLINE ADVERTISING

Many of the expert witnesses giving evidence to the committee drew attention to the lack of transparency as to who is targeting people with political ads online, and why. As Ben Scott put it, there is 'no reason in the world why every citizen who sees a political ad shouldn't know exactly who bought it, how much they spent, and how many people they paid to reach.' Scott also stressed that people exposed to such advertising should know 'why you got that ad – what the demographic features were that were chosen by the advertiser to make that ad come to you,' and suggested that publicly accessible online databases of such advertising would also improve transparency, with advertisers and tech platforms legally required to include all such ads in these.

The committee recommended that authorising agents should be legally required to submit identification and proof of address when placing political ads online, and that social media platforms should be required to create searchable and machine-readable databases of online political advertising, including information on who funded the ad; the political issue covered; the period during which the ad was online; and the demographics of the target audience. It also recommended that paid political advertising should be clearly labelled as such to the social media users who are exposed to it.

3.3.5 ALGORITHMIC TRANSPARENCY AND RESPONSIBILITY FOR CONTENT

Having heard evidence on the power of algorithms to determine the content delivered to social media users, and on the ability of automated tools such as 'bots' to deliver disinformation and other harmful content, the committee took the firm view that social media platforms should be considered as publishers responsible for the content they delivered.

It recommended that such platforms be legally required to clearly label content produced automatically or algorithmically; to identify and remove inauthentic and fraudulent accounts impersonating others for malicious reasons; and that they should adhere to a code of practice that would forbid deceptive or unfair practices. It also recommended imposing a legal duty on such platforms to swiftly remove harmful content such as hate speech, defamation, harassment,

and incitement to violence 'or risk monetary sanctions commensurate with the dominance and significance of the social platform'.

It also called for Canada to 'enact transparency requirements with respect to algorithms and provide to an existing or a new regulatory body the mandate and the authority to audit algorithms'.

The committee stressed that 'the monetary sanctions imposed by the new proposed legislative measures should represent more than the mere cost of doing business for a company'.

3.3.6 REGULATION OF MONOPOLY POWER

After hearing evidence from Professor Maurice Stucke of the University of Tennessee's College of Law, the committee decided to adopt Professor Stucke's description of highly dominant social data companies such as Facebook as 'data-opolies', which he described as companies that '...control a key platform through which a significant volume and variety of personal data flows. The velocity of acquiring and exploiting this personal data can help these companies obtain significant market power.'

Professor Stucke stressed that:

'…the potential harms from data-opolies can exceed those from monopolies. They can affect not only our wallets. They can affect our privacy, autonomy, democracy and well-being.'

3.3.7 INADEQUACY OF SELF-REGULATION

Canada's Privacy Commissioner, Daniel Thierren, told the committee that he and his international counterparts were alarmed by recent developments:

'There is a crisis in the collection and processing of personal information online. Even tech giants […] are recognising that the status quo cannot continue. Apple CEO Tim Cook spoke of 'a data industrial complex' and warned that 'our own information, from the everyday to the deeply personal, is being weaponised against us with military efficiency' […] Facebook's Mark Zuckerberg admitted that his company committed a serious breach of trust in the Cambridge Analytica matter. Both companies expressed support for a new U.S. law that would be similar to Europe's General Data Protection Regulation or GDPR. When the tech giants have become outspoken supporters of serious regulation, then you know that the ground has shifted and we have reached a crisis point.'

(Any student of Facebook's history might, however, have advised Mr Thierren not to take Zuckerberg's enthusiasm for regulation at face value.)

Several expert witnesses emphasised that social media platforms such as Facebook could not be relied on to regulate themselves.

The committee noted that the EU's General Data Protection Regulation (GDPR) offered European social media users higher levels of protection than are enjoyed by Canadian citizens, particularly with regard to control over how their data is used, and recommended that Canada enact similar legislation.

In its concluding remarks, the committee noted that:

'… if there is one thing that the events of the past year have brought to light, it is that social media platforms should carry out a thorough self-examination, as they have an important choice to make. Do they wish to continue with a business model designed to be addictive while ignoring the harmful effects their platforms can have on the social fabric, and their long-term human impact? Or would they rather make technology more ethical and compatible with the capabilities of the human mind? The Committee sincerely hopes that they will choose the latter'.

While we do not doubt the committee's sincerity, any expectation that Zuckerberg and his fellow tech billionaires will voluntarily 'choose' a more ethical path would, we believe, represent a triumph of hope over experience.

FACEBOOK TOOLS FOR MICROTARGETING

Facebook provides a number of tools that allow advertisers to define and select particular audiences to target. These include 'Website Custom Audience', which allows advertisers to target Facebook users who have visited their websites (using Facebook Pixel to analyse the behaviour of these audiences while on particular sites) and 'Lookalike Audience', i.e. Facebook users who are likely to be promising targets because their profiles resemble those of existing audiences. Lookalike audiences are created using Facebook's social graph data including demographics, social connections and relationships, income, interests and newsfeed activity. The granularity that these tools provide has increased greatly along with rising data volumes and advances in AI.

The power of tools to influence users' behaviour has also increased apace. An example is Facebook's 'Dynamic Creative', which enables advertisers to rapidly create huge numbers of ads and test multiple variants of these to find those that make most impact on a target audience.

Creating, testing and targeting such ads was one of the things that AIQ was doing for Vote Leave and associated groups during the EU referendum campaign. An example is shown below: a Facebook ad aimed at people who had shown environmental interests. Others were tailored to audiences whose profiles suggested they might be concerned by immigration. Vote Leave's campaign director Dominic Cummings estimates that the campaign ran around one billion targeted ads in the run up to the vote, mostly via Facebook.[74]

One of the 'dark ads' produced and targeted for Vote Leave during the EU referendum campaign in 2016.[75]

Recent analysis by researchers at the University of Southern California has demonstrated how Facebook's audience analysis tools can be used to obtain highly personal information not just on particular audiences but on individuals – including their identities – and to run Facebook-approved campaigns aimed at single users or households. The researchers noted that Facebook's advertising and data use policies 'do not prohibit or discourage microtargeting' and that the company's reaction to being alerted of the ease with which individuals can be identified and targeted showed 'an apathy toward microtargeting and circumventions of the rudimentary microtargeting protections Facebook has put in place' and 'a disregard for the need to limit the ease of targeting marginalised groups'.[76]

74 The Future of Political Campaigning, Jamie Bartlett, Josh Smith and Rose Acton, Demos, 2018. In June 2017, speaking at OgilvyChange's 'Nudgestock' festival of Behavioural Economics, Cummings put the number of ads delivered in this way even higher, at 1.5 billion.

75 'Vote Leave's 'dark' Brexit ads', Channel 4 News Fact Check, 27 July 2018.

76 'Facebook's Advertising Platform: New Attack Vectors and the Need for Interventions', Irfan Faizullabhoy and Aleksandra Korolova, 2018.

3.4 FACEBOOK SCRUTINISED BY EU PARLIAMENTARIANS

3.4.1 BACKGROUND

In May 2018, after repeated requests from the EU Parliament, Mark Zuckerberg agreed to answer questions in person from leaders of the political groups and the Chair and Rapporteur of the Committee on Civil Liberties, Justice and Home Affairs. The Brussels hearing was chaired by EP President Antonio Tajani and, at the insistence of the EU Parliament's Green Group, was livestreamed. Some observers were critical of the format of the session, noting that it did not lend itself well to forensic cross-examination.[77] Nevertheless, the hearings and Facebook's subsequent written answers to follow-up questions were instructive, if only for the very public demonstration of Zuckerberg's reluctance to give straight answers.

This was followed up in June and July 2018 by a series of hearings chaired by Claude Moraes and Josef Weidenhozer of the EU Parliament's Civil Liberties, Justice and Home Affairs Committee. These gave an opportunity for a number of expert witnesses to give some interesting evidence, though the contributions from Facebook executives were somewhat less enlightening.

3.4.2 ZUCKERBERG VAGUE AND EVASIVE

Zuckerberg endeavoured to start his appearance on a contrite note. In a prepared statement, he said:

'Over the last couple of years we haven't done enough to prevent these tools from being used for harm as well: that goes for fake news, foreign interference in elections, and developers misusing people's information. We didn't take a broad enough view of our responsibility and that was a mistake, and I'm sorry for it [...] I want to be clear, keeping people safe will always be more important than maximising our profits.'[78]

Whether from naivety or for other reasons, the Facebook CEO was keen to downplay the political motives underlying the abuses of Facebook's platform, seeking to present these abuses as being motivated largely by commercial considerations and amenable to commercial solutions:

It's worth noting that a lot of fake news is economically motivated not politically motivated. It's much like email spam in that way: the playbook for fighting this is removing the ways that spammers can make money so then they just go and do something else.[79]

Zuckerberg sought to reassure EU lawmakers that Facebook would be making efforts to prevent interference in upcoming elections in Europe: 'This is one of our top priorities … that we prevent anyone from trying to interfere in elections like the Russians were able to do' [in the 2016 U.S. presidential election].[80] He was vague on how his company intended to do this, but suggested that this would involve use of more artificial intelligence (AI) tools to identify and remove fake accounts, as well as closer co-operation with regulators.

Zuckerberg shrugged off questions about Facebook's monopoly position by downplaying Facebook's dominance:

'We exist in a very competitive space where people use a lot of tools for communication. The average person uses a lot of tools for communication… so from where I sit, it feels like there are new competitors coming up every day… We are constantly needing to evolve our services.'[81]

At the end of the hearing, Zuckerberg, seemingly aware of the inadequacy of many of his answers, said: 'I realise there were a lot of specific questions that I didn't get to specifically answer, but going around and hearing the themes of what people are concerned about, had questions about, I think I was able to address the high-level areas in each.' [82]

77 'Mark Zuckerberg let off the hook by shambolic European Parliament grilling', Jon Stone, The Independent, 23 May 2018.

78 The Independent, ibid.

79 The Independent, ibid.

80 'Mark Zuckerberg hearing: As it happened', Politico, 23 May 2018.

81 Politico, ibid.

82 The Independent, ibid.

At the request of President Tajani, Facebook sent written answers to questions posed by MEPs that Zuckerberg had not addressed. These were for the most part equally bland and added little to Zuckerberg's responses, although they did include a commitment to increased transparency in political advertising and to a compulsory system of verification for people managing Facebook pages with large numbers of followers.[83]

3.4.3. EXPERT WITNESSES SHED LIGHT ON MISINFORMATION AND DATA PROTECTION ISSUES

Three subsequent hearings heard from a number of witnesses with first-hand experience of the ways in which Facebook and political disinformation campaigns operate.

At the first of these, Sandy Parakilas, a former Facebook operations manager who since leaving Facebook has become Chief Strategy Officer at the Center for Humane Technology, explained that one of his main responsibilities at Facebook had been data protection. He emphasised that the company had, until 2014/15, allowed developers to access a vast quantity of user data, including (for some developers with 'extended permissions') their private messages – and that it had allowed this to happen without requiring explicit permission from users. He pointed out that even after Facebook had been aware of the abuses of data by Cambridge Analytica, it had continued to allow the company to use its platform for advertising until March 2018.

'This problem is much, much larger than Facebook or Cambridge Analytica,' Parakilas said. 'Regulating such a complicated industry is going to be extraordinarily challenging. The good news is that GDPR is going to be a great first step towards defining rights for users.' However, he stressed that it was important for regulators to 'ensure comprehension, not just consent'. He explained that on Facebook's Terms of Service consent screen, supposedly compliant with GDPR, links to pages on which users can read these terms and see their options 'are tiny, and the button to accept and simply move on without reading anything is very large, so I think it is fair to say that this page is designed to get the user to accept'. He also pointed to recent reports detailing how device manufacturers had been able to access Facebook user data despite the protections supposedly in place to prevent this.

Parakilas suggested that it is crucial to find 'ways to align corporate and user incentives'. Drawing a parallel with the insurance industry, he pointed out that the fact that insurers had to pay out claims whenever a driver was injured had led to the industry caring greatly about passenger safety. He suggested that leveraging a 'cyber-insurance' industry could have similar effects in the online world and help ensure that companies and users are educated to become more aware of best practices, while spreading the risk of large penalties out across many companies. However, he emphasised that 'rules alone will not work' – the companies themselves need to provide users with easy-to-use tools to control usage of their own data. He also stressed that regulation should not curb small companies that drive innovation: 'We do not want to further empower entrenched monopolies through regulation.'

Questioned about whether Facebook was moving user data belonging to non-EU citizens out of the EU in order evade GDPR requirements, Parakilas said that Facebook's approach was neither 'in the spirit of GDPR nor in the spirit of what they have described, which is to apply the protections of GDPR globally. I think were they truly to act in that spirit they would not have moved those accounts.'

Parakilas commented on the 'echo chamber' effect that allowed misinformation to spread unchallenged within certain user communities that Facebook's algorithms help to create, observing that the key to tackling this problem was to make such algorithms more transparent. He acknowledged that Facebook had started to make efforts to achieve greater transparency in political advertising, but stressed that the real problem was with the company's 'surveillance

83 'Follow-up answers from Facebook after the meeting between EP leaders and Zuckerberg', European Parliament, 24 May 2018.

advertising' business model, which 'creates some really dangerous incentives that are bad for society':

'There are two approaches we can take. We can either highly regulate all of the worst cases, for example foreign actors interfering in elections, and we can write a bunch of really complicated rules about how that should or should not happen. Or we could simply remove some of the functionality, so that there is less targeting capability, so that it's harder to do the kinds of things that happened in Brexit and in the US presidential election. Those are the two basic approaches. As regulators, I would encourage you where possible to try to avoid highly specific rules if you can avoid it. If you can try to think about ecosystems and incentives, and wherever you can try to find other actors like I mentioned with the insurance companies – try to find other players in the ecosystem who can provide balance.'

Parakilas also stressed Facebook's highly dominant position in the social media market, the way it has used this to suppress potential competitors such as Snapchat, and the need to prevent data-sharing between Facebook and other platforms under its control such as WhatsApp and Instagram.

Observer journalist Carole Cadwalladr described ongoing investigations into the 2016 EU referendum in the UK (as detailed in earlier sections of this report). She said that these had helped demonstrate that the current laws surrounding campaigning no longer work:

'Everything is running through the black boxes of the tech companies, and we have no idea of what is going on inside those black boxes. What this means, critically, is that we have no idea how much money was spent during the referendum. We don't know who spent it. We don't know where that money came from. We don't know what advertisements people saw. We don't know how people were targeted with those advertisements. We don't know what data that was based upon…We have this situation now where we have a foreign company that played an absolutely pivotal role in that referendum and we have no means of obtaining that information.'

Cadwalladr described how journalists seeking answers from Facebook had been stonewalled and intimidated by threats of legal action by the company. She also described how Facebook had obstructed attempts to discover the extent of efforts by Russian actors to influence UK voters, and deplored the failure of British politicians – some of whom, she said, were directly implicated in some of the abuses that took place around the 2016 referendum – to take action. She said that the EU is the 'one institution that has the authority to stand up to the tech giants […] I really hope that you will hold them to account.'

UK ICO Elizabeth Denham and her deputy, James Dipple-Johnson, updated the hearing on their ongoing investigation into the Cambridge Analytica scandal. Ms Denham emphasised that 'the behavioural advertising ecosystem has been applied across political campaigns to influence how we may vote, and I am deeply concerned at how this has happened without due legal or ethical considerations about the impacts to our democratic system.' She also hailed the progress in data protection made by the EU, and noted that 'online platforms are data controllers under data protection law, and they can be held fully liable for misuse of personal data on their platforms.'

Pointing out the way in which online platforms and their algorithms control the content that users see, Denham stressed that 'they must take responsibility for the provenance of the information that is provided to users'. In response to questions, she acknowledged that similar abuses were happening on other, smaller platforms, but that 'Facebook is a very big player in this field and is the focus of misuse that has been identified in the UK.'

Mr Dipple-Johnson stressed that the new powers that the UK ICO now enjoyed via GDPR had been enormously helpful in allowing it to understand and pursue the data abuses that had taken place.

Asked how data protection authorities could ensure that upcoming European elections would not be affected by similar abuses to those that had been identified in the UK and US, Ms Denham said that, under GDPR, inspection of algorithms and orders to stop processing data would be as effective as administrative fines.

Professor David Carroll, a US academic, described how he had used a Subject Access Request (SAR) under EU law to attempt to obtain his personal data from Cambridge Analytica/SCL, after discovering that this had been processed in the UK, and the ways in which the company had prevented him from obtaining it. His interest was more than personal – Carroll said he wished to find if this data had been used, in combination with psychological profiling, to expose him to malicious information designed to influence his vote in the US presidential election: 'We can understand that their model has the potential to affect a population – even if it's just a tiny slice of the population – because in the US only about 70,000 voters in three states decided the election.' He observed that: 'Unless these political technology machines are built on fundamental rights of access and privacy by design, it strains credulity that democracy can survive uninjured.'

Cambridge Analytica whistleblower Christopher Wylie detailed his experience of the ways in which the firm had acted as 'a corrupting force' in political campaigns in various countries around the world. In particular he described 'Project Ripon', whose purpose was 'to develop and scale psychological profiling algorithms for use on political campaigns'. (see section 3.1.3 above). Wylie emphasised that:

'The work of Cambridge Analytica was not equivalent to traditional marketing, as has been claimed by some…Cambridge Analytica specialised in disinformation, spreading rumours, kompromat and propaganda. CA sought to identify certain mental and emotional vulnerabilities in certain subsets of the population and worked to exploit those vulnerabilities by targeting information designed to activate some of the worst characteristics in people, such as neuroticism, paranoia and racial biases.'

Wylie claimed that Facebook had approved the terms and conditions of the app used to harvest user data that was used as input for these algorithms without even reading these. He said that AIQ had illegally shared data between supposedly separate Leave campaigns during the EU referendum campaign, and that Vote Leave had then attempted to cover this up by removing evidence. He observed:

'I do not believe Brexit would have happened were it not for the data technologies and network of actors set up by Cambridge Analytica. I also do not believe that the Brexit result was won fairly or legitimately […] Facebook's system allowed this to happen, and Mark Zuckerberg's refusal to answer key questions has prevented us from finding out everything that happened during Brexit […] The EU has a right and an obligation to know whether millions of people will be losing their rights as European citizens on the basis of a flawed vote corrupted by systemic electoral fraud and data crime.'

Wylie also described how he had been banned from both Facebook and Instagram after the revelations he had made:

'Banning a whistleblower reveals the unrestrained power technology companies have over users, when a person's online presence can be so quickly and so thoroughly eliminated from existence […] What happens to our democracy when these companies can so easily delete people who dissent, scrutinise or speak out?'

At the hearing of 26 June, Angela Jelinek, Chair of the European Data Protection Board (EDPB), said that the EDPB already had 29 cross-border cases, and that the Facebook/Cambridge Analytica case was just 'the tip of the iceberg'. She said that awareness of the issues it raised

was increasing in the US and elsewhere, with signs that other countries were interested in moving towards similar levels of data protection. Asked what was being done to prevent future such abuses, she said that national data authorities had increased their staff numbers, though not all had sufficient staff, and that it was important to make sure that there was a lead authority with a responsibility to take the lead and coordinate efforts by other authorities. She stressed that the EDPB was making efforts to achieve convergence in the approaches taken by these authorities, and that the different national regulators were working closely together on this.

Paul Dehaye of data protection organisation Personaldata.io described his attempts to use SARs to get information on the data Facebook held on him, and on the way this data had been used in targeted advertising, noting that Facebook had persistently failed to provide this and brushed off his complaints, and that subsequent evidence given by Facebook executives had run directly counter to his own experience. He said Facebook had shown a 'sustained disregard for European laws regarding data protection' and described the company as 'basically Cambridge Analytica with better PR, better lawyers and even better lobbying'.

Dehaye called for enforcement of the right to portability of user data between platforms, saying that Facebook Pixel data, for instance, could be imported into systems that would offer users and researchers more insight into how this data is actually used to influence users' behaviour. He said such innovations could help 'to rebalance power within the personal data ecosystem' but that they are being 'actively stunted by Facebook', which is 'clinging to an outdated business model'. He also cautioned that data portability opens up new questions as to user privacy and fair competition, which authorities would need to consider.

Steve Satterfield, Director of Privacy and Public Policy at Facebook, told the hearing that Facebook was making efforts to give users more insight into the apps that had access to their data, through initiatives such as 'Clear History'; that it was continuing to investigate abuses by such apps; and that it had made major efforts to make the platform fully GDPR-compliant. He said that Facebook was now requesting users' explicit consent for specific types of data processing. He also claimed that 'advertising and privacy are not in conflict' and said that users could control the types of advertising they see, find out how they have been selected for specific types of advertising, and opt out of particular types of ad. According to Satterfield, the Cambridge Analytica scandal and the introduction of GDPR had prompted the company to reconsider the ways in which in which its developer platform works and given 'further impetus to consider the ways in which we're protecting data across all of our services'.

Under questioning, Satterfield gave vague answers on exactly how Cambridge Analytica had used Facebook and associated platforms to target voters with political advertising. He claimed that 'to the best information we have, Cambridge Analytica didn't receive information from European users'. He also claimed that the abuses of personal data by Aleksandr Kogan and Cambridge Analytica ran counter to Facebook policies of the time.

Asked what could be done to prevent abuse of Facebook tools during electoral campaigns, Satterfield said that efforts were focused on tamping down on fake accounts, using automated AI tools. He said the company was using third-party factcheckers to clamp down on fake news and that its new 'View Ads' feature would allow users to see all of the ads that were put out by a particular page. Asked whether the company would submit to an independent audit of its data practices, Satterfield said that the company was regularly audited by regulators such as the Irish Data Protection Commissioner and the FTC in the US. When asked to explain why Facebook had moved users out of European jurisdiction to the US, he said that the same user controls were effective worldwide. In response to questioning, Satterfield confirmed that Facebook gathers data on non-users, including unique identifiers (IP addresses), from sites that use Facebook features, but claimed that the uses to which it put these data were 'very limited'.

Claire Bassett, head of the UK Electoral Commission, described how digital campaigning had some positive impact by involving more people in public debate around elections, but said that electoral rules needed to be improved to increase accountability of political advertising and transparency as to how money is spent on such advertising, and who is spending it. She said that a register of all political advertising would be very helpful in achieving this, allowing greater transparency and insight for both regulators and the public. She also said that having stronger sanctions available would help regulators enforce regulation more effectively.

Joel Kaplan, Facebook's Vice President of Global Public Policy, acknowledged that Facebook had been used by malign actors to undermine elections around the world, and claimed that it had 'learned important lessons'. He said the company has successfully deployed new tools in recent European elections and was making significant efforts to combat foreign interference, crack down on fake accounts, reduce the spread of false news, increase the transparency of ads, and support an informed electorate.

He claimed that advances in machine learning and AI were enabling the company to detect misinformation emanating from foreign sources and detect fake accounts, and that Facebook was now showing fewer stories with inauthentic content, thanks to more fact-checking, partnerships with external partners, and changes to algorithms that downgraded sensational 'clickbait' content. He also claimed that Facebook's 'View Ads' feature would make the sources and targeting of such ads more transparent to users. Kaplan stressed that Facebook was partnering with civil society organisations, regulators and academics to increase public participations in elections, and to gain a better understanding of how social media were used around electoral campaign. He said that Facebook was setting up teams ahead of each national elections to bring such tools to bear as appropriate to the particular circumstances.

Asked why Facebook had refused to hand over information to the UK Parliament to enable a judgement to be made on whether the Brexit referendum had been conducted fairly and lawfully, and whether the company was prepared to hand over such information in regard to future elections, Kaplan claimed that the company had answered 'a tremendous quantity of questions', and that when it comes to providing retrospective information, 'that's not something we can do consistent with prior commitments to people's privacy'. In effect, he was admitting that the privacy of potentially malign actors was more important to the company than the integrity of the electoral process around a crucially important referendum.

Privacy rights campaigner Max Schrems outlined his efforts over the past seven years to hold Facebook to account, and what he saw as the failure of the Irish Data Protection Commissioner to take effective action on the issues he had raised. Like other witnesses, he saw effective enforcement of GDPR as the key to forcing the company to show proper respect for user data. He noted what he described as a fundamental market failure – 'We have a lot of people who hate Facebook but they don't have any other option' – and expressed the hope that anti-monopoly action by the EU would help to change this situation.

For Facebook, Richard Allan, the company's Vice President of Public Policy, reprised his performance at the UK Parliament's DCMS committee, claiming that there are 'different opinions on concepts like consent and so on'. He claimed that the changes the company had made were more than cosmetic, and that Facebook had significantly reduced the access that app developers can have to personal data. In regard to fake news he observed that 'one person's fake news is another person's political speech' and added no significant further detail on how the company is attempting to combat the problem.

Allan once again stressed that advertising was what enabled the platform to offer its services to users for free, but echoed Kaplan's claim that Facebook is making its advertising more transparent, saying: 'It is certainly not in our interests or in the interest of consumer trust

to have poor quality or misleading ads shown on our system.' On verifying the identity of Facebook users – a key issue in controlling the spread of misinformation by malign actors –Allan remarked: 'We have not been persuaded to date that the collection of significant extra amounts of sensitive information in order to verify someone's identity would be justified.'

At the third hearing, chaired by MEP Josef Weidenhozer of the Civil Liberties, Justice and Home Affairs Committee, parliamentarians had been hoping to hear from Sheryl Sandberg, Facebook's Chief Operations Officer. In a letter to Mark Zuckerberg, Chair of the Civil Liberties, Justice and Home Affairs Committee Claude Moraes had expressed his frustration with Facebook's reluctance to allow the EU Parliament to question its most senior decision-making executives: 'I would like to stress it is essential for Facebook's credibility to show its commitment that you send staff members that are in charge of the departments concerned in your company and not public policy team members.'[84]

Instead, the company sent Richard Allan, who once again gave a series of bland apologies and assurances, without offering much in the way of new information. He described, somewhat vaguely, how 'we are working on a number of solutions to try and stem the spread of false news,' and mentioned the code of practice in relation to this on which the company had been working with the EU Commission. Again, he reiterated the company's 'strong sense of responsibility to reduce harm when we can,' while acknowledging that 'we have been slow to start' on issues such as hate speech.' Parliamentarians seeking more concrete information to add to that given at the previous two hearings were largely disappointed.

Following the hearing, Civil Liberties Committee Chair Claude Moraes said:

'In the course of our investigation, it has become clear that real transparency is needed from companies such as Facebook in terms of data processing methods, tracking, profiling and use of algorithms in order to ensure consumer trust. My impression is that much needs to be done, particularly by commercial organisations, to ensure that their business model is by design and by default compliant with fundamental rights. After hearing from the competent authorities examining the case, we expect appropriate measures to enforce the law and ensure the respect of our fundamental rights will be taken.' [85]

84 'Facebook! Stop sending us lobbyists! demands European Parliament', Jennifer Baker, The Next Web, June 2018

85 'Third Facebook-Cambridge Analytica hearing: data breach prevention and cures', press release, European Parliament, 3 July 2018.

4.0 POLICY RECOMMENDATIONS

This report and the findings of the expert bodies that it has referenced have demonstrated beyond reasonable doubt that a massively dominant social media platform such as Facebook cannot be trusted to regulate itself. Time and again, Facebook has responded to findings that it has committed serious breaches of the trust that its users place in it by saying that it will tackle these problems internally. Time and again, it has failed to do so, and the abuses have only multiplied as Facebook's global scale has grown.

These problems stem both from the company's ethos and from its basic business model, which has been to trade access to user data for opportunities to raise revenue, and to use the content it delivers as a means to stimulate user engagement, with little regard for its impact on individual users or whole societies. While tinkering around the edges of this model and introducing cosmetic changes in the hope of pacifying its critics, Facebook shows no sign of moving to a significantly different modus operandi and nor do we expect it to do so voluntarily.

As all three investigating bodies have found, Facebook has determinedly resisted attempts to gain a true picture of the scale of the problem. Such information as they have managed to obtain has had to be dragged out of the company, and its attitude to these investigations has been characterised at every stage by obfuscation or outright contempt. Meanwhile, as recent events in France have shown all too clearly, its platform continues to facilitate weaponised disinformation that is causing deepening social divisions and actual violence. This cannot be allowed to continue – least of all at a time when many countries, not least the UK, are facing crucial political decisions that will affect people's lives for generations to come.

Legal authorities in various countries finally appear to be taking a tougher approach to holding Facebook to account, using existing national and international laws.[86] Yet effective regulation poses formidable challenges, not least the need to protect the freedom of speech and of expression that are also essential to a fully engaged democracy. Facebook and other tech giants operate globally and the abuses that have taken place all have an international dimension. All three bodies whose reports we have covered recognise this, and it is encouraging to see them working together on possible solutions.

Our proposals draw on the recommendations of these three reports, and on those made recently by the EU Commission and EU parliamentarians. They are aimed not just at curbing the sort of abuses that we have described, but also at helping to foster the development of truly social (as opposed to anti-social) media.

4.1 USER CONTROL OVER DATA

The most coherent transnational approach to addressing abuses of personal data has been taken by the European Union. On 25 May 2018 the EU's General Data Protection Regulation (GDPR) came into force. It gives the data-protection authorities in EU countries far more power to penalise Facebook and other tech companies for breaches than were previously available under the Data Protection Directive that formerly applied – including the power to impose much higher fines.

The user rights that GDPR underpins all have major implications for the way in which Facebook operates. For instance, the Right to Be Informed specifies that anything that happens to such data must be disclosed to users, and the Right to Object means that users must explicitly give consent before any data is used in a particular way – and be able to withdraw this consent as easily as it is given. The Right to Data Portability states that an organisation must always give

86 In December 2018, for example, the Attorney General of Washington DC announced that the state was suing Facebook for allowing Cambridge Analytica to gain access to the personal data of nearly half the districts residents; see 'Facebook: Washington DC sues tech giant over Cambridge Analytica data use', Alex Hearn, The Guardian, 19 December 2018.

its users the ability to see all the data it holds on them. These rights mean, for instance, that companies using Facebook's Pixel system to track website users for the purpose of targeting ads now have to gain the specific consent of users before monitoring their activity on their sites.

Several cases under GDPR are already being brought against Facebook in EU countries, for instance in regard to the recent incident that saw the personal data of some five million EU citizens compromised by a software vulnerability. If the company is found in breach over this incident, it could be fined up to €20 million or 4% of its annual global turnover, whichever is higher. On the basis of Facebook's reported results for the last fiscal year, this means that it could in theory face a fine of up to $1.63 billion.[87] The UK Information Commissioner has already issued its first GDPR notice against AggregateIQ, the Canadian company that featured in the Facebook/Cambridge Analytica data scandal.

Following Mark Zuckerberg's appearance before Members of the European Parliament in May 2018 – an appearance notable for the way in which Facebook's CEO evaded giving direct answers to questions – MEPs urged Facebook to allow EU bodies to carry out a full audit to assess data protection and security of users' personal data.[88] We agree, but believe that additional measures are needed.

GDPR is still in its early days, and although it greatly extends protection for individuals within EU countries, the global nature of data transfer and processing by Facebook and other tech companies means that, as expert legal commentators have noted:

'In order to effectively enforce the GDPR's extraterritorial scope, there will be a need for certain level of cooperation between EU and non-EU actors – formal, for example, through development of […] agreements on Mutual Legal Assistance by the states, and informal, based, for example, on codes of conducts or voluntary compliance by companies operating online.' [89]

We would propose that:

- Countries considering the tightening up of their data protection laws use GDPR as a model framework, and work closely with EU authorities on framing such new national legislation. This would make the task of holding tech companies such as Facebook to account across different national jurisdictions much easier. If the UK does indeed leave the EU, it too should take this approach. The UK government has indicated[90] that 'there will be no immediate change in the UK's own data protection standards,' but we would urge an ongoing commitment to fully match and comply with GDPR standards.
- Penalties specified in national legislation thus developed should be commensurate with those under GDPR, and should represent much more than the mere 'cost of business' for Facebook and other such companies;
- The EU's GDPR and comparable legislation in non-EU jurisdictions should eventually be framed/revised so that companies basing any part of their data operations in countries that are not covered by such legislation are deemed to be automatically in breach. Otherwise, it is likely that Facebook and other companies will use laxer legislation in such jurisdictions to evade transparency and other legal requirements.

4.2 DISINFORMATION AND POLITICAL ADVERTISING

In September 2018, the European Commission published its Code of Practice on Disinformation. Several online platforms, including Facebook, have signed the Code, which commits them to 'a wide range of commitments, from transparency in political advertising to the closure of fake accounts and demonetisation of purveyors of disinformation'.[91] These are, rightly, aimed at ensuring that social media users exposed to political advertising are able to see who has targeted

87 'Facebook could face $1.63bn fine under GDPR over latest data breach', Charlie Osborne, ZDNet, 2 October 2018.

88 'Facebook-Cambridge Analytica: MEPs demand action to protect citizens' privacy', press release, European Parliament, 25 October 2018.

89 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context', Paul de Hert and Michal Czerniawski, International Data Privacy Law, Volume 6, Issue 3, 1 August 2016.

90 'Brexit, GDPR and data protection: what happens if the UK becomes a third country?', Data Protection Network, September 2018.

91 Code of Practice on Disinformation, European Commission, 26 September 2016,

them and who has paid for such ads. As part of their commitment to the Code, signatories have also committed to report on the implementation, functioning and effectiveness of the Code, based on annual self-assessment reports that will be reviewed by an objective third-party organisation, and to provide information to the Commission upon request. As the Commission has noted: 'The Code and other initiatives set forth by the Commission are essential steps in ensuring transparent, fair and trustworthy online campaign activities ahead of the European elections in spring 2019.'

We welcome this development and see the international adoption of the Code as an essential part of any policy aimed at curbing the ongoing damage to democratic institutions caused by Facebook and other tech giants. However, Facebook's long history of obfuscation and deceit makes it hard to believe that the self-assessment system on which the Code relies is by any means sufficient to ensure that it (or other signatories) will in fact follow the letter and spirit of the Code, or report their activities honestly. The Code itself is also worded in a way that makes adherence to its principles merely desirable, rather than necessary. It is also worrying, in the light of the multiple recent and historical abuses detailed in this report, that a number of Facebook policies related to false news, advertising and misrepresentation are held up as examples of 'best practice'.[92] We therefore propose that:

- The EU should devise new legislation to make adherence to the Code a legal requirement for social media firms, specifying heavy penalties for any breaches of its terms – and for any attempts to conceal such breaches;
- The Code itself be tightened up to define more precisely what is required of its signatories.

We note, for instance, that signatories to the Code 'commit to enable public disclosure of political advertising (defined as advertisements advocating for or against the election of a candidate or passage of referenda in national and European elections), which could include actual sponsor identity and amounts spent'. For the purposes of transparency, this is indeed absolutely necessary. However, the Code gives no detail as to how this should be done. We therefore propose that it be amended to specify that:

- All signatories should place all political advertisements that are run on their platforms in easily searchable databases to which both regulators and members of the public have access, and that the information included with these should include the sponsor of the advertising, the amount spent on the ad and the basis on which any targeting was carried out (e.g., in Facebook's case, full data relating to any 'Website Custom Audience', 'Lookalike Audience' or similar tools used).
- During political campaigns ahead of elections or referenda, all political advertising – whether from parties or non-party campaigning organisations – should be labelled as such and all such parties and campaigners should be required to register with Facebook and other social media platforms that they use. Political opinions expressed by (verified) individuals would of course be exempt, but the views of organisations or companies, if political, should have a clearly identified source.[93]
- That users of social media platforms are easily able to opt out of all political advertising and that an opt-out link enabling them to do this should be included prominently with all political ads.
- Political advertising related to elections and referenda in particular countries but that originates from and/or is paid for by sources from outside these countries should be banned under the Code.[94]:

We also note that the Code does not fully address a closely related problem: the use of false identities to disseminate misinformation, not as advertising but as 'organic' posts – which

92 'Annex II: Current Best Practices from Signatories of the Code of Practice', European Commission, September 2018.

93 Under pressure in the wake of the Cambridge Analytica scandal, Facebook has expressed its support for the 'Honest Ads Act' proposed by by a cross-party group of US senators, which would make these requirements mandatory in the US, and has introduced stricter requirements for promoters of political advertising on its platform. See 'What the government could actually do about Facebook', Emily Stewart, Vox, 10 April 2018.

94 Facebook, under pressure, banned such advertising ahead of the referendum on the reform of Ireland's abortion laws; see 'Facebook to block foreign ads in Irish abortion referendum', Graham Fahy, Reuters, 8 May 2018.

are often far more difficult for users to detect as being intended to influence their behaviour. While the Code states that 'relevant Signatories commit to put in place clear policies regarding identity and the misuse of automated bots' it does not give any detail as to what such policies should comprise. We propose that:

- The Code be amended to specify clear requirements on identity verification and the prohibition of automated posts by non-human agents. Social media companies should be required to verify the identities of all their users before accepting them onto their platforms,. These should be made available to relevant authorities following up on allegations of dissemination of misinformation or other damaging materials, making those using social media channels accountable for their communications.
- Personal social media accounts should always be clearly linked to accountable people, who should be limited in the number of such accounts they can hold. Pages should be linked to legally founded organisations or associations with responsible (named) people behind them.

We see such measures as the only way to ensure transparency and legal accountability for messages promoted on social media platforms. Social media companies should have the same level of responsibility as publishers, and only by measures such as these will they be made to do so.

4.3 CURBING MONOPOLY POWER AND FOSTERING A HEALTHIER SOCIAL MEDIA ECOSYSTEM

This is probably the most challenging area for policymakers. Facebook's global dominance and vast user base give it an enormous advantage over any – perhaps more socially responsible – competitors in the social media arena, and the company has used its massive resources from advertising revenues to bolster this position, often by buying up any promising looking newcomers to what it sees as its territory. For users of any social media network, the size of the network itself is naturally seen as one of its main strengths: the more users it has with whom to make potential connections, the more potentially valuable it is to any individual user. And however sceptical we may be of the hollow rhetoric of inclusivity that Zuckerberg has used to disguise the true nature of his company's operations, we should not lose sight of the fact that Facebook does indeed offer real benefits to its users and could potentially help us to build the global village that many have long dreamed of.

Moreover, it is principally the users of Facebook who create its value as a social network – value in the shape of the human connections and interactions that it enables, but also its market value as a mechanism for delivering advertising. Yet the interests of these users – who should be seen as the organisation's most important stakeholder group by far – have been routinely ignored and indeed actively damaged by the company's activities. Rather than being respected as stakeholders, they have been treated as 'inventory' to be exploited purely for the financial gain of Facebook's owners. Moreover, as Germany's Bundeskartellamt (Federal Cartel Office) has found, Facebook has abused its dominant market position 'by making the use of its social network conditional on its being allowed to limitlessly amass every kind of data generated by using third-party websites and merge it with the user's Facebook account.' [95]

Various suggestions have been made as to how users' interests could be better protected and represented in the way the company operates and is structured. By analogy with the treatment of industrial monopolies and especially natural monopolies, we might consider nationalisation, along the lines of historical nationalisations of transport, water and energy utilities But this seems at present a remote prospect, given the global nature of Facebook's operations and the fact that it is based in a country that is likely to look askance at any such proposals. And while power of the sort that Facebook exercises over people's personal data is clearly not safe in

95 'Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive', press release, Bundeskartellamt, 19 December 2017.

the hands of its current ownership, there could also be real risks in placing such power at the disposal of national governments.

Some commentators have suggested that the solution lies in giving users fuller control of their data, for example by establishing a publicly controlled central infrastructure for the storage and exchange of personal data, with individual users deciding what elements of their data are stored in this way and to what uses these can be put by specified third parties such as social media companies.[96] However, in addition to the technical challenges that this presents, it could be seen as simply deferring the problem, if such third parties cannot be trusted to use data licensed to them in this way responsibly.

Another, more market-based, solution to giving users more control has been suggested: for personal data to be treated – as The Economist has put it – as 'the currency in which customers actually buy services' and for laws to be drawn up, analogous to intellectual property laws, 'to govern the ownership and exchange of data, with the aim of giving solid rights to individuals'.[97] The idea is that regulators would oblige tech companies to share with rival firms – and with the permission of the users themselves – the data they hold, in exchange for a fee, thus encouraging more competition between such firms and loosening the monopoly grip of companies such as Facebook. By enabling portability of data between platforms, such proposals might, in combination with stricter application of existing anti-monopoly laws, succeed in levelling the corporate playing field to some extent, but they too fail to address the central problem, which is one of trust and accountability.

Other commentators have suggested that Facebook turn itself into a mutually owned company controlled by a trust that is operated in the interests of the organisation's users and employees.[98] We see this as a solution that would indeed address the core problem, but given the track record of its owners it does not appear to be one that will materialise without a clear direction being set by lawmakers.

In view of this, we propose that national governments and regulators, working with transnational authorities, consider legislation that requires:

- Users of social media networks to be treated as core stakeholders who should be represented both in the ownership of the company and at board level. This could also potentially be a requirement of an internationally applied code of practice.

Since user data is the most valuable asset of a social network such as Facebook, and the ultimate driver of its revenue, we would propose that:

- Every verified user of a social network owned either by a publicly traded company or a private limited company be granted a share that carries voting rights in the company.

In Facebook's case, this would entail the transfer of a substantial part of the company's value to its users – something which we believe to be entirely justified by the fact that Facebook's value as a social network derives precisely from these users. It would also mean that Zuckerberg would lose his controlling interest in the company – and that too would be seen by many as a major step in the right direction.[99]

Having voting rights would enable users, as a block, to gain a powerful say over the direction of the organisation, and having a board-level representative, chosen by users themselves, would help ensure that their interests were treated with the respect they deserve.

We believe that a strictly enforced international code of practice for social media companies as outlined above could do much to prevent abuses such as this report has described. However, we also believe, in view of the company's track record, that Facebook is likely to resist such proposals and/or attempt to circumvent any regulation that it sees as threatening to its current

96 For a well-developed proposal along these lines, see The Digital Commonwealth: From private enclosure to collective benefit, Mathew Lawrence and Laurie Laybourn-Langtone, IPPR Commission on Economic Justice, 2018.

97 'How to tame the tech titans', The Economist, 18 January 2018.

98 'An open letter to Mark Zuckerberg: It's time to give Facebook to its users', Molly Scott Cato, Left Foot Forward, 21 March 2018.

99 In 2009, after Facebook users objected to changes in the company's terms and conditions, Zuckerberg suggested that Facebook would move to give users a say over the direction of the company by establishing a 'user council' and enabling users to vote on major changes. Like so many of his statements, this was not translated into meaningful action. See 'Facebook lets users set its terms and conditions', Mark Harris, TechRadar, 26 February 2009.

business model. Proposals to make its governance more inclusive and accountable are also likely to meet stiff resistance from Facebook, and in this it may find support from the system of corporate law under which it currently operates in the US. In view of this, and taking account of the utility nature of a company such as Facebook, we propose that:

- National governments, including that of the UK, set up dedicated regulatory bodies equivalent to existing regulators that oversee the behaviour of the print and broadcast media and the energy utility industries. A national social media regulator would be responsible for ensuring that platforms adhere to regulations and codes of practice as described above, with powers to impose heavy fines for breaches and, ultimately, the power to withdraw an offending company's licence to operate.[100]

Finally, we believe it is vital to support the development of more socially responsible social media organisations and enable these to develop into viable alternatives to Facebook and similar commercially oriented companies. This needs to be a central focus of government policy, and it requires substantial public investment.[101] Enabling such investment is the aim of our final proposal.

As we have noted, to be effective the financial penalties for any regulatory breaches should represent a substantial proportion of the offending company's revenues. Our final proposal is that:

- The money raised from penalties imposed by regulators on companies such as Facebook should be earmarked for funding of:

  a) Grants to not-for-profit organisations developing social media networks that offer genuine benefits for their users and take a transparent and responsible attitude to user data, and that are under the control of fully accountable trusts;

  b) Funding for projects aimed at counteracting the spread of disinformation online.

100 Ofcom, the UK media and telecoms regulator, outlined a blueprint for social media regulation in September 2018 – see 'Ofcom outlines case for regulating social media networks'.Aliya Ram and Nic Fildes, The Financial Times, 18 September 2018. One possibility in the UK would certainly be for Ofcom to assume responsibility for such oversight, but we would suggest a dedicated social media regulator would be more suited to this large and technically specialised role.

101 For a detailed proposal as to how this might work in practice, see The Digital Commonwealth: From private enclosure to collective benefit, Mathew Lawrence and Laurie Laybourn-Langtone, IPPR Commission on Economic Justice, 2018.

5.0 CONCLUSION

If one were starting from scratch in devising a social media network that offered the greatest possible benefits to its users and the fullest respect for their interests, one would certainly not be starting from a model that looked anything like Facebook today. But that is not to say that we should simply accept that Facebook is the only possible model for the future of such networks.

An interesting comparison is with Wikimedia, a not-for-profit organisation that is run by and for its users and is funded by public contributions and grants. Its main project, Wikipedia, has been hugely successful in making reliable information easily available to billions of users around the world, using free, open-source software. It is, in fact, a shining example of 'commons-based peer production' of the sort that Yochai Benkler and Helen Nissenbaum foresaw in 2006, and there is no reason why social media networks run in the same spirit should not also be successfully developed.

We hope that this report has left its readers under no illusions as to the scale of the threat that Facebook currently represents to democracy and civil society worldwide. As EU countries face an upsurge in far-right populist movements, with imminent elections to the European Parliament and a very real possibility of a second referendum on Brexit in the UK, this is a threat that calls for immediate action.

Facebook has consistently lied and dissembled to both its users and to regulators, and there is little reason to suppose that it will change its ways voluntarily. Much damage has already been done, and unless urgent action is taken by governments and regulators, this is likely to get very much worse

The proposals we have outlined above may help to steer Facebook in a more positive direction and limit the harm it is currently causing to users, democratic institutions and whole societies. But we should not assume that the future of social media networking will or should be dominated by Facebook or other profit-oriented corporations.

This moment of crisis is also one of opportunity. Working together, national governments, transnational authorities and regulators have it within their power to curb the abuses we have described and to create the conditions for a healthier social media ecosystem to develop.

It is critical that they do not fail in these tasks.

ABOUT THE AUTHOR

Tom Scott is a freelance writer and editor who also teaches on undergraduate and postgraduate writing courses at Falmouth University in Cornwall. A self-confessed Twitter addict, Tom first became interested in the way social media are being used to spread disinformation after watching this happen in real time during the Trump and Brexit campaigns in 2016.

MOLLY SCOTT CATO
GREEN MEP FOR THE SOUTH WEST

www.mollymep.org.uk
@MollyMEP
office@mollymep.org.uk
facebook.com/MollyMEP/

Designed by www.lifework.biz Printed on 100% recycled paper