REPORT

Data and Democracy in the Digital Age

By Stephanie Hankey, Julianne Kerr Morrison and Ravi Naik

THE CONSTITUTION SOCIETY

With special thanks to colleagues at Tactical Technology, Gary Wright and Amber Macintyre.

About the Authors

Stephanie Hankey is a social entrepreneur, researcher and lecturer. She is a Visiting Industry Associate at the Oxford Internet Institute and leads a research project, using a fifteen-country case study, on the use of personal data in elections. Stephanie is the co-founder and Executive Director of Tactical Tech.

Julianne Kerr Morrison is a junior barrister whose busy practice covers many of Monckton Chambers' core areas of work. She is particularly active in Public Law and Human Rights, Competition and Regulatory, Data Protection and Freedom of Information, as well as a number of areas of European law.

Ravi Naik is a solicitor and partner at Irvine Thanvi Natas Solicitors, working at the forefront of personal rights protection in the digital age, particularly looking at the relationship between data exploitation and the democratic process. He instructed on the first case against Cambridge Analytica for the use of personal data during the Trump Presidential campaign.

Executive Summary

Data has become an increasingly valuable asset for those that control it. Our interconnected world has become ever more pervasive, ubiquitous and prominent. As personal data has taken an increasing role in all of our lives and our lives translate ever more into electronic media and data, the challenge of who controls that data and what rights we have over that data are not just questions for those in the IT world. They become problems that are as fundamental to us as any other human right.

Much has been written about the impact of the misuse of private data since the Cambridge Analytica and Facebook revelations. However, what is less explored and harder to understand is the broader use of political data – and the regulatory deficits underpinning its use.

This report seeks to explore both the manner in which data has taken an increasingly prominent role in political campaigning, as well as the regulations underpinning the underlying retention, connected processing and ultimate use of personal data in such campaigning.

Content of the Report

The body of the paper is split into the following parts:

1. **Politics vis-à-vis data:** The first part of the paper explores the increasing primacy of data to our personal lives, from the ubiquitous nature of modern digital technology to the vast 'surveillance capitalism'-based 'attention economy'. The section explores the developing power of the platforms, and the opaque algorithms underpinning them, to effect individual world views. The section also provides information and an analysis of the recent political scandals caused by the alleged use of sensitive personal data by companies such as the now notorious Cambridge Analytica. The section explores how such companies used micro-targeting to have macro effects.

2. **The problem in action:** The second part of the paper explores the origins of political advertising and campaigning, to show the historic development of digital marketing during campaigns. The section includes information on political spending on digital advertising in the UK, including the problems of analysing such spending. This section seeks to explore how the wider data brokering industry is used during the political process and, furthermore, outline how an industry is developing that increasingly impacts political processes across the globe.

3. **The existing framework:** The third part of the paper explores the current regulatory framework and the gaps in it that give rise to concern. It explores how the regulations may allow the evolving use of political data to fall within blind spots of the legislative regime.

4. **Conclusions and recommendations:** The paper concludes by providing summary outcomes and recommendations to effect positive and real change in the field. Those recommendations are produced in brief below.

5. **Annexes:** the report also annexes two tables. Annexe 1 provides a summary of publicly available campaign and party spending on digital advertising in the UK from the 2015 general election until the 2017 snap election. Annexe 2 provides an indication of the kinds of data practices used by different political parties in the UK.

Key Recommendations

The paper's recommendations are as follows:

Recommendation 1

Political parties, their campaigns and supporters should embrace the opportunities provided by the GDPR.

Recommendation 2

The Government should re-consider its position on Article 80 GDPR.

Recommendation 3

It is time to re-visit the need for a Code of Conduct for political campaigning and/or the designation of a specific regulator to review political processing.

Recommendation 4

To consider new spending limits.

Recommendation 5

To encourage spending transparency.

Recommendation 6

Engagement between data and technology companies and the government to keep up with the pace of change in technology.

Introduction

Personally I think the idea that fake news on Facebook, which is a very small amount of the content, influenced the election in any way — I think is a pretty crazy idea. Voters make decisions based on their lived experience.[3]

Mark Zuckerburg, Nov. 2016

Data is the marker of all we do; the trace of our digital existence. Personalised data also provides the fuel for the 'attention economy',[2] an economy that has allowed social media networks to evolve from a network of interconnected individuals, to 'behaviour modification empires'[3] to a 'social engineering project with incredibly deleterious effects across multiple countries and cultures'.[4]

Big data is a topic so vast and sprawling that numerous books have been written about its past problems and future concerns. From the impact of artificial intelligence on employment to the creeping ubiquity of the internet of things, technology and personal data are likely to be topics of on-going importance to the development of a new social contract. However, there is one area in which the use of data has had a marked and little understood impact: politics.

The political climate has changed rapidly in recent years. In large part, politics has evolved due to the development of technology.[5] Our interconnected world has become ever more pervasive, ubiquitous and prominent. This in turn has amended both the delivery and form of communication of political ideas, as well as shifted, and undermined, the accountability for those messages. Labels such as 'fake news' speak to the growing concern that individuals (i.e. the electorate) are constantly accessing material which is inaccurate and/or misleading without adequate, or any, *ex ante* control or *ex poste* accountability. There is also a wider lack of understanding, despite recent scandals, of how platforms, data collection and data sharing actually work, and what steps could or should be taken to make political messaging and advertising accountable, in particular by political parties and actors. This has led to understandable concerns about the shape of and any gaps in the current regulatory regime.

Those concerns could have real consequences for the democratic process. 'Fake news' not only has the capacity to create specific items of misinformation, it is also capable of undermining faith in political messaging in general. While fake news and the use of personal data for political targeting remains mired by speculation, with regulators scrambling to find answers for how data was used during past electoral processes, the electorate may lose faith in both the capacity of the regulatory regime and the integrity of the democratic process itself.

1 https://www.theverge.com/2016/11/10/13594558/mark-zuckerberg-election-fake-news-trump

2 James Williams, Stand out of our light (June 2018)

3 How we need to remake the internet, Jaron Lanier https://www.ted.com/talks/jaron_lanier_how_we_need_to_remake_the_internet/transcript?language=en

4 https://twitter.com/fchollet/status/998017580680921088

5 The types of technology and its development throughout politics is beyond the purview of this paper. We would recommend Pax Technica by Philip Howard (2018) for an overview of the development of technology and its broader use on the democratic process.

This problem is not going to go away – it can only be exacerbated by the continued pace of change. Such is the pace of change that awareness of technological developments and their consequences often occur only after the event, while the regulatory landscape is barely able to keep pace. Whilst we grapple with what technology has enabled, we also face a new wave of change, which we have only started to understand the ramifications of. For example, the concerns around evolving technology such as 'artificial intelligence' and machine learning show that any regulatory response needs to be as dynamic as the technological mischief it seeks to contain.

In this landscape, how can politics and regulations to preserve our democratic legitimacy evolve to both embrace technological developments whilst maintaining the integrity of the democratic process? This paper seeks to offer insight into what has occurred, while offering some recommendations for change.

The body of the paper is split into the following parts:

1. **Politics vis-à-vis data:** The first part of the paper explores the increasing primacy of data to our personal lives, from the ubiquitous nature of modern digital technology to the vast 'surveillance capitalism'-based 'attention economy'. The section explores the developing power of the social media platforms, and the opaque algorithms underpinning them, allowing users to effect individual world views. The section also provides information and an analysis of the recent political scandals caused by the alleged use of sensitive personal data by companies such as the now notorious Cambridge Analytica. The section explores how such companies used micro-targeting to have macro effects.
2. **The problem in action:** The second part of the paper explores the origins of political advertising and campaigning, to show the historic development of digital marketing during campaigns. This section includes information on political spending on digital advertising in the UK, including the problems faced by researchers in seeking to analyse such spending. This section seeks to explore how the wider data brokering industry is used during the political process and, furthermore, outline how an industry is developing that increasingly impacts political processes across the globe.
3. **The existing framework:** The third part of the paper explores the current regulatory framework and the gaps in it that give rise to concern. It explores how the regulations may allow the evolving use of political data to fall within blind spots of the legislative regime.
4. **Key conclusions and recommendations:** The paper concludes by providing summary outcomes and recommendations to effect positive and real change in the field.
5. **Annexes:** The report also annexes two tables. Annexe 1 provides a summary of publicly available campaign and party spending on digital advertising in the UK from the 2015 general election until the 2017 snap election. Annexe 2 provides an indication of the kinds of data practices used by different political parties in the UK.

Part I: Politics vis-à-vis Data

The history of information technology and its relationship with politics is nothing new. The often cited 1996 Declaration of the Independence of Cyberspace began:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[6]

Whilst the framers of that Declaration have moved away from its content, the implication was clear. The online space was not to be governed and was to be left to be self-regulated. Much like the 'invisible hand' of finance, the Declaration envisaged an invisible network that would ultimately self-govern. However, the internet was not a 'new home' nor a parallel space. As recent events have shown, the consequences of such an unregulated space have been seismic and resulted in political upheavals that are still playing out.

The Networked World

The majority of the developed world spend their time online. As of December 2017, it has been reported that 85% of Europe and 95% of North America is online. The global penetration of the internet is said to be 54%.[7] It is estimated that by 2020, the vast majority of the world will be online.[8]

A side effect of this long-term trend is that the platforms on which the populace spend their time are now collecting vast amounts of personal data. Most online systems and platforms are engineered to continuously monitor their users to be able to offer tailored and personal services. This type of monitoring has been termed 'surveillance capitalism'.[9]

In this race to gather and use personal data, those at the forefront of technological design have treated individual privacy concerns as an obstacle to overcome, rather than a right to respect. As Scott McNealy, then CEO of Sun Microsystems, said in 1999:

You have zero privacy anyway. Get over it.[10]

This viewpoint is by no means unique. To the contrary, this attitude to individual control and autonomy over data was supported by the early technological developers who saw the freedom of information flow as a fundamental right. This is a sentiment echoed by the modern technological architects. In 2010, Mark Zuckerberg declared:

People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people… That social norm is just something that has evolved over time.[11]

By design, therefore, privacy was seen as a postscript to the commercial gains to be made

6 https://www.eff.org/cyberspace-independence

7 https://www.internetworldstats.com/stats.htm

8 https://edition.cnn.com/2013/04/15/tech/web/eric-schmidt-internet/index.html

9 The origins of the phrase are disputed but often attributed to Shoshanna Zuboff (see: https://www.wired.com/beyond-the-beyond/2016/03/shoshanna-zuboff-condemning-google-surveillance-capitalism/)

10 https://www.wired.com/1999/01/sun-on-privacy-get-over-it/

11 https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

from monitoring users. However, the prospects of 'surveillance capitalism' being exploited for ulterior motives are only just starting to be understood, often to the surprise and concern of the platforms themselves.

Such is the commitment to this guiding thesis that it has spawned a new doctrine: 'dataism', in which information flow is the 'supreme value'.[12] Yuval Noah Harari, who detailed the dataism theory, suggests that it presents an existential challenge:

Once Big Data systems know me better than I know myself, authority will shift from humans to algorithms.[13]

Whilst we have not yet reached a level where human authority cedes to algorithmic decision making, we have entered a world where personal data allows for micro-targeting with macro effects.

Data Rules Everything Around You

The extent of the data that is gathered on individuals is overwhelming, personal and telling; who we communicate with, what we say, what content we've been consuming—images, movies, music, news. Even what mood we are in at specific times.[14] Ultimately, almost everything we perceive and do will end up recorded somewhere. For the most part, this time is spent on social media platforms.[15]

This data, in turn, allows the entities that collect it to build extremely accurate psychological profiles on both individuals and groups. Indeed, entire studies have been written about the possibility of utilising Facebook 'likes' alone to understand our psychographic details.[16] Amongst the concerns about such technologies is that the data needed to produce such profiles can be bought and collated from various entities, without involving the individuals concerned. These entities therefore have the power to develop extremely personal profiles about our most sensitive personal beliefs without individuals having ever known that they were profiled. The personal detail and accuracy of the results can be remarkable.

In particular, individual opinions and behaviour can be cross-correlated with that of thousands of similar people, achieving an uncanny understanding of individual personality sets. These profiles are probably more predictive than what the individual could achieve through introspection (for instance, it has been suggested that Facebook 'likes' enable algorithms to assess your personality better that your own friends could).[17] As recent political scandals have shown, they can predict which side you will ultimately vote for in an election.[18] And it's not just individual-level profiling power - large

12 https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c

13 Homo Deus, Yuval Noah Harari (2016)

14 http://www.bbc.com/future/story/20180201-how-your-social-media-betrays-your-mood

15 https://blog.globalwebindex.com/chart-of-the-day/social-media-captures-30-of-online-time/

16 Matz, Kosinski, Nave & Stillwell (2017) Psychological targeting as an effective approach to digital mass persuasion. Proceedings of the National Academy of Sciences. http://www.pnas.org/content/114/48/12714.full

17 Youyou, Kosinski, Stillwell, Computer-based personality judgments are more accurate than those made by humans, Proceedings of the National Academy of Sciences Jan 2015, 112 (4) 1036-1040; DOI: 10.1073/pnas.1418680112

18 See, profile of Professor David Carroll and others, as disclosed by Cambridge Analytica (see further below; profile available here: https://twitter.com/profcarroll/status/846347516341837825?lang=en; see also: https://edition.cnn.com/2018/03/17/politics/professor-lawsuit-cambridge-analytica/index.html)

groups can be even more predictable, as aggregating data points erases randomness and individual outliers.

The Curated World

Social network services now have the capacity to control what information we consume. For instance, the Facebook newsfeed is now the main source of traffic for most news websites.[19] However, those newsfeeds are not randomly generated. Rather, most social network algorithms are designed to give prominence to the content that is most likely to result in engagement, rather than providing a chronological outline of what occurs on a given platform. This is exemplified by the Facebook platform, which now uses its homepage as the key for engagement.

What we see in our social media newsfeeds has therefore become algorithmically 'curated'. As the systems behind the platforms have gathered ever more personal data, new forms of behaviour management have begun to emerge. Social networks in turn created filters – complex algorithms that looked at what individuals liked – and then fed more of the same back to them. In the process, individuals began to move, without noticing, into bubbles that isolated them from enormous amounts of other information. They only heard and saw what they liked. And the newsfeeds increasingly excluded anything that might challenge people's pre-existing beliefs.

Opaque social media algorithms therefore get to decide, to an ever-increasing extent, which articles we read, who we keep in touch with, whose feedback we receive on the opinions we express. Developed over many years of exposure, the algorithmic curation of the information we consume gives the entities that collect this information considerable power over our lives. If the platforms get to decide, over the span of many years, which news you will see and whose political status updates you'll digest, then those platforms have the power to affect your worldview and your political beliefs. As Timothy B. Lee said in one of the most in-depth analysis of the impact of Facebook after the 2016 election:

Facebook hasn't told the public very much about how its algorithm works. But we know that one of the company's top priorities for the newsfeed is 'engagement'. The company tries to choose posts that people are likely to read, like, and share with their friends. Which, they hope, will induce people to return to the site over and over again.

This would be a reasonable way to do things if Facebook were just a way of finding your friends' cutest baby pictures. But it's more troubling as a way of choosing the news stories people read. Essentially, Facebook is using the same criteria as a supermarket tabloid: giving people the most attention-grabbing headlines without worrying about whether articles are fair, accurate, or important.[20]

Jaron Lanier describes these platforms as 'behaviour modification empires'.[21] That's the service these platforms sell to their customers who, for the most part, are advertisers, including political advertisers. And that service is effective.

Data as a Political Tool

The use of data in political campaigns is not new. When the internet was first used as a tool for political communication, politicians treated it like other forms of broadcast media and simply built

19 https://www.vox.com/new-money/2016/11/6/13509854/facebook-politics-news-bad

20 https://www.vox.com/new-money/2016/11/6/13509854/facebook-politics-news-bad

21 https://www.ted.com/talks/jaron_lanier_how_we_need_to_remake_the_internet/transcript?language=en

websites that often contained the same pictures and text that went into their print brochures and party leaflets. For example, President Clinton's 1992 and 1996 campaigns, and Prime Minister Blair's campaign in 1997, had relatively simple online components compared to their political peers today. Yet, their campaign websites did allow supporters to register and provide information to campaign strategists. Some of that data was analysed for trends or became the first layer of the big political datasets that exist today. At that time, however, only a portion of the electorate was online and radio, television and newspapers were more important to campaign advertising strategy.

After the Presidential campaigns in 2000, political consultants began merging datasets. Sufficient numbers of voters were online which made it worth customising ads for particular districts. Operationally, webmasters usually reported to the pollster in the campaign organisation. After 2000, it became common for the pollster to report to the webmaster, or a Chief Information Officer, who oversaw all aspects of the role of data in politics, including advertising and public opinion polling.

As the datasets grew, so did the potential for their use. And as the electorate began to spend more time online, this had a dual effect, allowing for further data to be taken and to offer a platform for better and more direct targeting. The effective use of data and digital technologies in an election or referendum process can be the measure of a 'smart' campaign. This was demonstrated by the widely-praised 2008 US presidential campaign by Barack Obama. A set of practices which then became a benchmark for the effective use of social media and individual data to gain support in elections.

The Modern Campaign

In modern political campaigns, data on voters is an *essential* asset. Used effectively, data can help a party better understand the concerns of voters, more efficiently use its resources and directly speak to citizens on the issues that matter to them the most. As such, the collection, analysis and use of personal data is now an inevitable part of the democratic process.

The history of political campaigning is necessary to understand the current framework, as such a history provides a perspective of where the impetus for today's use of data and digital advertising comes from: before there were data brokers and social media platforms in the UK, direct mail and the post office were used to reach people with different political messages based on demographics. It is also relevant to understanding how the regulatory landscape has developed in order to meet the challenges posed by the increased use of individual data, and where gaps have emerged as regulation has failed to keep step with technological change.

The American approach to political campaigns is often thought of as different to that in the UK, a style that promotes the celebrity of the politician, where candidates are sold as 'washing powder'. Behavioural manipulation methods were used in political campaigns as early as the 1920s when the pioneer of public relations, Edward Bernays, used such techniques to get the mayor of New York elected.[22] Similarly, in the 1930s, advertising executives used the same techniques that they used to sell Listerine to get politicians elected, such as playing on 'fear' factors in advertising to motivate people to act. After this, techniques of the advertising sector became commonplace in US politics and gradually this inspired others.

22 Putting Politics On the Market, 1928, Edward Bernays

In the UK, the history and style of election campaigning has been somewhat different, comprising of a combination of polling, value-led marketing and developments in voter databases. Gallup polls have been undertaken since the 1940s, with a range of companies emerging in their wake, such as ICM, MORI, NOP and Harris. In 1983, the Conservative party hired Chris Lawson as a full-time director of marketing. He worked with Saatchi and Saatchi 'to design a campaign which relied to a greater extent than ever before on US-style value research and 'psychographics'.[23] Similarly, the use of individual data in political campaigns has steadily developed in step with changes in data-driven technologies: initiatives to increase voter turnout, improvements to party membership databases and experiments with a range of political marketing tools, from opinion polls to canvassing.

The history of political campaigning is necessary to understand the current framework, as such, a history provides a perspective of where the impetus for today's use of data and digital advertising comes from: before there were data brokers and social media platforms in the UK, direct mail and the post office were used to reach people with different political messages based on demographics. It is also relevant to understanding how the regulatory landscape has developed in order to meet the challenges posed by the increased use of individual data, and where gaps have emerged as regulation has failed to keep step with technological change.

So, if the use of data for individual targeting, as well as the practice of appealing to voters based on emotional values, is considered business-as-usual in politics, then what is new about the digitisation of these techniques?

23 (McNair, 2011, p.101)

What's new?

The evolution of political data is hallmarked by the subjectivity and scale of digital messaging. The scope of political campaigning, its personalisation and its dynamism are unprecedented. Voters can, through the digitisation of personal lives, be monitored and targeting continuously and in depth, utilising methods intricately linked with and drawn from the commercial sector and the vast collection of personal and individual data.

The most significant factor is the pervasive collection and analysis of individual data. Massive investments by the commercial digital marketing and advertising sector, combined with the ubiquitous everyday use of technology by citizens, has created an environment where personal data is collected and processed at scale, depth and speed. Innovations in data collection over the past decade have led to the growth of a multibillion-dollar industry, one where thousands of highly tuned methods and tools are used to collect, track, profile and target individuals with the aim of changing their behaviour. The granularity of the data collected on individuals, combined with the scope of its use is exceptional. In short, without the collection, processing and selling of vast amounts of personal data, the use of this data for political influence would not be possible.

As personal data cascades around a developing ecosystem, researchers are taking steps to understand the value of this information. It has been of particular use to psychologists, who have realised that social media platforms are a trove of information and data on individual's personalities. Those platforms have been designed to retrieve and collect personal data and store that information indefinitely. That information has led to a change

in outlook for those who want to understand personalities; previously private information is now given out voluntarily and on a vast scale.

The value of the data has also been recognised in the political arena. Ideas that have been developing for the last century about the value of personal information and its potential for influence, are finally being realised. This has been facilitated by the scale, subjectivity and low cost of that personal information, which was previously unimaginable. This raises new questions when such techniques are put to use to influence the electorate.

There are a wide-range of techniques that are currently being used in the context of individual data in elections. These techniques fit into one of three broad categories:

- **Data as a Political Asset:** data collected on potential voters, accumulated by parties, exchanged between political candidates, acquired from national repositories, sold or exposed by those who want to leverage them, such as voter data, consumer data and data processed from the open internet.
- **Data as Political Intelligence:** data on individuals collected and interpreted by political campaigns to learn about voters' political preferences, to inform campaign strategies and to test and adapt campaign messaging, such as 'digital listening'[24] tools for monitoring social media discussions and extensive 'A/B testing'[25] for honing and testing thousands of different messages.
- **Data as Political Influence:** how individual data is analysed and used to target and reach potential voters, with the aim of influencing their views or votes, such as micro-targeting (tailored advertising to the individual level), geo-fencing (dynamically targeting citizens based on their location) and 'search influence'.

These categories are a helpful guide to understand how such techniques can have a democratic impact.

We have enclosed two annexes with this paper which provide:

1. A summary of publicly available campaign and party spending on digital advertising in the UK from the 2015 general election until the 2017 snap election. It is important to note however that this information has been compiled from publicly available data and media reports. The inability to get accurate and verified data is part of the case in point within this report: there needs to be more accurately centralised, reported and documented expenditure by political parties. The figures within the first table were found by analysing the 30 highest paid suppliers shown in the Electoral Commission's (EC) database of election and referendum spending for the relevant categories set by the EC (advertising, market research/canvassing, media and unsolicited materials to electors). One further take away from preparing the table is that, due to varying degrees of details that can be found in spending invoices and self-reporting, there are limits to assessing exactly when 'digital' and 'data-driven' practices were used. This helps illustrate

24 'Digital listening' is a term used by companies selling services to political parties that enables them to get analysis of public sentiment regarding different issues through collecting and analysing information found on social media and the open internet.

25 A/B testing is the marketing term used for the practise of creating different versions of an advert or message and testing it on an audience to decide which one to use based on what best resonates with the target audience. In digital A/B testing several thousand messages can be dynamically tested and iterated on audiences.

the fundamental problems in understanding, researching and analysing political data usage.

2. An indication of the kinds of data practices used by different political parties in the UK. Again, the fact that this data is partial and mostly gleaned from media reports and a small number of academic research reports points to the fact that more comprehensive and systematic reporting is necessary.

Regardless of the fragmented nature of the content of these two tables, they give an indication of the scale and scope of data use by political parties and campaigns in the UK.

Part II: The Problem in Action

We just put information into the blood stream of the internet and then watch it grow, give it a little push every now and again… It has to happen without anyone thinking, 'That's propaganda'. Because the moment you think, 'That's propaganda', the next question is: Who put that out?[28]

Mark Turnbull, former Managing Director of SCL Elections

The effect of the combination of psychological profiling and powerful machine learning on political debate and the electoral processes are only recently being explored and considered. These problems of online political engagement have been thrown into stark relief by the now notorious Cambridge Analytica and their relationship with Facebook and their use of personal – and sensitive personal – data.

Cambridge Analytica and Facebook: A Faustian Pact

Cambridge Analytica was created as a subset of a UK-based military contractor, SCL Group. Recent revelations suggest that Cambridge Analytica was established as a front company for SCL Group to appeal to US clients.

Those revelations came as part of a much wider and significant exposé. Following detailed investigative journalism, revelations from former company employees and citizen-led inquiries and legal actions, we now have a more detailed understanding of what the company was doing. However, that picture remains far from complete. Investigations and legal action continue to seek a complete understanding of what the company was doing, how it was doing it, and for whom. In this section we outline what is known or suspected thus far, and the outstanding questions that need to be answered.

The company operated as a UK based political consultancy.[27] One of their key services was a unique 'psychographic' profile of voters. The company suggested that they had individual profiles on over 200 million American citizens. Cambridge Analytica were employed to use their 'psychographic' tools to make targeted advertisement purchases for a number of US campaigns, including *inter alia* the 2016 Republican campaign of Ted Cruz, and the 2016 Trump Presidential campaign. There remain questions over whether Cambridge Analytica was also employed by Leave.EU in respect of the British referendum on the future relationship with the European Union. The latter issue is the subject of a number of inquiries that remain ongoing at the time of writing.

The dataset that led to those profiles remains shrouded in mystery and attempts to release that dataset is currently the subject of litigation and an investigation by the Information Commissioner.[28]

26 Mark Turnbull, Former Managing Director, SCL Elections (see: https://www.channel4.com/news/factcheck/cambridge-analytica-the-allegations-so-far). Mr Turnbull also used to work with Bell Pottinger (see: https://www.newyorker.com/magazine/2018/06/25/the-reputation-laundering-firm-that-ruined-its-own-reputation)

27 The company filed for administration on 3 May 2018

28 Two of the authors of this report, Ravi Naik and Julianne Kerr Morrison, are instructed by the Claimant on that claim and complaint to the Information Commissioner

What we do know is that it has been reported that the firm bought some underlying data from a company named Global Science Research (GSR), run by a Cambridge University researcher, Dr Alexander Kogan (latterly, Dr Spector).

Dr Kogan was said to have developed such a large dataset through a number of simple applications, including 'This Is Your Digital Life'.[29] Such applications were presented on the Facebook platform, either to be used within the platform or as an external link that was accessed through the platform. The applications appear in a user's newsfeed as a personality questionnaire, producing relatively banal results which can then be shared with friends. The apps, including This Is Your Digital Life, were built to test developing theories of personality-modelling on the basis of Facebook 'likes', as initially exposed by Cambridge University researchers such as Dr Michal Korsinski and Dr David Stillwell.

The application were launched throughout 2014 and only 270,000 people were said by Facebook to have ever used the 'This Is Your Digital Life' application.[30] However, the secret to its exploits was that the applications also collected data on the user's 'friends', unbeknown to those friends. Since the average person has approximately 300 Facebook friends, this would ultimately collect data from approximately 81 million US voting-age citizens.

The evidence available suggests that Dr Kogan did gather data from a host of individuals through the applications. Following the fall out of the Facebook/ Cambridge Analytica crisis, Facebook revealed that in fact 87 million users had their data taken by Dr Kogan's application.[31] The terms of use of the application suggested that the data derived from it would be used solely for research purposes. However, contrary to those terms of use, the data derived from the application was seemingly saved for commercial use by Dr Kogan.[32]

How this data was then repurposed remains mired in controversy. Dr Kogan suggests that the data was provided to Cambridge Analytica and SCL. Commercial contracts to lease this data from Dr Kogan's company to Cambridge Analytica have also been leaked. However, Cambridge Analytica/SCL both deny having such data or using such data for their work. The Information Commissioner seized the computers from SCL's offices to find answers to these questions, following a contested warrant

29 There is a divergence of stories relating to which apps took the data. Dr Kogan, in written testimony before the DCMS Committee, suggested that no data from 'This is your Digital Life' was passed to SCL. Dr Kogan suggested that the only data passed to SCL was via a similar application, named "GSR App". For Dr Kogan's testimony, see: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/written/81613.html. However, Christopher Wylie has repeatedly stated that SCL took data from "This Is Your Digital Life." Furthermore, the Facebook "certification" orders against Cambridge Analytica, Dr Kogan and Mr Wylie only related to This Is Your Digital Life and none of the further applications such as "GSR App", while the settlement and confidentiality agreement between Facebook and Dr Kogan referred to the GSR App (https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/180514-Rebecca-Stimson-Facebook-to-Ctte-Chair-re-oral-ev-follow-up.pdf).

30 As above, it is not clear which apps were used. However, Facebook's own statements only relate to 'This Is Your Digital Life' https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/

31 That is the figure of individuals that Facebook has identified as affected (see: https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/)

32 Mark Zuckerberg claimed Dr Kogan's actions as a "breach of trust" — describing the behaviour of his This Is Your Digital Life application as 'abusive' (See: https://www.facebook.com/zuck/posts/10104712037900071). However, before the DCMS Committee, Facebook CTO Mike Schroepfer stated that 'We did not read all of the terms and conditions' of Dr Kogan's application.

application. A forensic analysis of those servers is underway and the results are unknown at the time of writing.

However, one fact has emerged through this process: Facebook knew of 'This Is Your Digital Life' and the 'GSR App' and the data they were harvesting, yet seemingly took no action to remove the application or warn those affected.[33] Furthermore, the Guardian asked Facebook how 'personal data about a large set of its users is now being exploited for experimental political campaigning purposes'. They did not answer when asked for comment.[34]

The Devil is in the Data: What Did Cambridge Analytica Do?

There are numerous questions surrounding Cambridge Analytica and its parent companies, particularly in light of their recent application for administration. Indeed, at the time of writing there are ongoing claims and applications to seek discovery of what information and data Cambridge Analytica had on individuals, how that data was used and who it was given to.[35]

According to Christopher Wylie, a former Cambridge Analytica contractor who helped build the algorithm, the initial data set of unknown quantity from Dr Kogan was married with other information from a host of different sources, to build a data rich system that could target US voters with personalised political advertisements based on their psychological profile.[36] All of this was told to the *Observer* by Mr Wylie under the headline, 'I made Steve Bannon's psychological warfare tool' by the investigative journalist, Carole Cadwalladr.[37]

That 'psychological warfare tool' was put to use by the Republican Party in the 2016 Election. Initially employed by the Ted Cruz campaign for Republican candidacy, the company was then employed by the Trump Presidential campaign.[38]

The company boasted of having 5,000 to 7,000 data points on 230 million citizens in the United States.[39] Irrespective of the veracity of these claims or whether the Facebook data was ever plugged into the Cambridge Analytica system, it is known that they did have personal profiles from a large set of American voters on their database. This is a known fact following a number of subject access requests put in by American citizens, which resulted in disclosure of an Excel sheet of a political 'model' for each individual, based on their political trigger

33 Ibid.

34 https://www.theguardian.com/commentisfree/2018/mar/26/facebook-data-misuse-cambridge-analytica

35 As above, two of the authors of the report are instructed on the lead claims/applications

36 Before the DCMS Committee on 6 June 2018, former CEO of Cambridge Analytica stated that the data included information from 'Acxiom, Experian and Infogroup' (see: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/84838.html)

37 https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

38 It is a matter of public record that the company used 'psychographics' when working for the Cruz campaign. It remains unknown if the same psychographics used by the Cruz campaign were then used by the Trump Presidential campaign. Brad Parscale (who ran Trump's digital operations) denied they used psychographics for Trump. Alexander Nix also denied it, claiming they didn't have time. However, Mr Nix did admit to BBC's *The Secrets of Silicon Valley*, that they took some 'legacy data' from the Cruz work they did and put them into the models they used for Trump.

39 https://www.youtube.com/watch?v=n8Dd5aVXLCc

points. That data was incomplete and a US citizen, Professor David Carroll, has led a claim against the company to retrieve the true picture of the data held on him (and by implication, all Americans that have been profiled).[40] At the time of writing, the Information Commissioner has served an enforcement notice on Cambridge Analytica to provide full disclosure of all information concerning Professor Carroll and, importantly, how it was used and who it was given to.[41]

Thus, despite the numerous enquiries and claims, we currently do not know the true extent of the data underlying those profiles, how it was obtained or how it was used. However, the profiles were said by Cambridge Analytica to be made up of a combination of publicly purchased information – such as voting records, car ownership etc. – whilst the remainder is unknown. That data was then paired against the OCEAN personality score, to provide a psychographic political profile for each individual on their database.[42] That was the 'psychological warfare tool' developed for use on the electorate.

Once working for the Trump Presidential campaign, they 'plugged' their data into the existing dataset held by the campaign. The journalist Jamie Bartlett, who had unique access to the campaign's data centre, explains:

Cambridge's main role … was to use this data to build what they called 'universes'. Each was a key target group for the Trump campaign … Dozens of these highly focused universes were created – and their members were modelled on how persuadable they were.[43]

Using this highly focused and personal data, the Trump campaign was able to target voters on the individual level, by creating tailored messaging and content. The data also allowed analysts to identify voter blocks in key battleground states.

The revelations about Cambridge Analytica have also exposed the extent of data-driven micro-targeting and attempts to use digital manipulation in elections worldwide. Whilst much public attention has been focused on the US Trump election and the UK Brexit Referendum, it is important to note that allegations have been made of Cambridge Analytica also selling similar techniques through partners, consultants and affiliated entities in elections in a number of other countries across the world, including Brazil, India, Kenya, Nigeria and Mexico. This has broader implications for the democratic process overall and

40 Professor Carroll has made his profile as provided by Cambridge Analytica publically available here: https://www.motherjones.com/politics/2017/12/a-groundbreaking-case-may-force-controversial-data-firm-cambridge-analytica-to-reveal-trump-secrets/

41 Two of the authors of this report are involved in litigation to understand the underlying data, what the exact profile looked like and who it was given to. On 3 May 2018, the Information Commissioner ordered SCL to provide full disclosure to the complainant within 30 days. At the time of writing, we await that data.

42 The OCEAN (or 'Big Five') personality system identifies five independent personality traits. The original research was published in 1990. Unlike many models of personality, which are driven by an expert's theory about how humans differ from one another, the Big Five model was created by data-driven statistical methods. The underlying assumption is that if a trait is important in distinguishing humans from one another, then there will be many adjectives in the dictionary that make that distinction. For example, we might call someone talkative, sociable, outgoing, excitable, friendly, gregarious, or unreserved, and all of these words have an underlying commonality which is extroversion. The Big Five traits are Openness, Conscientiousness, Extraversion, Agreeableness and Neuroticism. All humans can be compared across the five traits, and personality tests measure where an individual scores on each of the personality traits.

43 Jamie Bartlett, The People vs Tech (2018)

wider questions of social stability and security in a variety of contexts.

Fake News and Information Bubbles

The Cambridge Analytica/Facebook scandal has brought something fundamental to the political fore. The majority of Facebook's two billion individuals users had operated for years without knowing the bargain they had entered into for their otherwise 'free' service. The real cost was only starting to become clear, that they pay for the site with their information.

Indeed, it is only belatedly, after the election and before a judicial committee that the tech giants have revealed the extent of the manipulation of their use. For example, Facebook initially dismissed the idea that the platform could have hosted fake news generated from third states during the 2016 Presidential election. However, following a number of enquiries, Facebook conducted research and stated that they were able to identify 80,000 Russia-linked posts on its platform that sought to interfere in the 2016 election. Those posts were viewed by up to 126 million people.[44] In presenting this evidence, it was said that:

Many of the ads and posts we've seen so far are deeply disturbing—seemingly intended to amplify societal divisions and pit groups of people against each other… They would be controversial even if they came from authentic accounts in the United States. But coming from foreign actors using fake accounts, they are simply unacceptable.[45]

This was not from an outside actor but from Facebook's lead counsel, Colin Stretch. And the extent of such political use doesn't stop there. The former president of Facebook, Sean Parker, recently recognised that the site can 'exploit human vulnerability'.[46] This is inherent in its very design. Facebook's interface works by selecting from stories that your friends have shared to find the links you're most likely to click on. The interface is not chronological but tailored and forged to be as engaging as possible.

This is a potent mix, because what is read and posted on Facebook is not just an expression of personal interests but a reflection of what Facebook has determined you will be interested in. Users end up in an information 'bubble'. The feeds people are shown on these sites are highly personal. What you see in your feed is algorithmically tailored to your identity and your interaction history with the site. No one gets the same view.

There are no democratic checks or controls on this power. The dangers of such power become apparent when third parties are allowed to use these algorithms to target a specific audience for political ends. The architecture of the site also makes it difficult to trace its political use, as it does not treat 'political' adverts any differently than other adverts. Furthermore, the adverts disappeared so they were never examined or debated.

Facebook has recently taken steps to create an 'archive' of political adverts, as well as all election and issue-based ads on Facebook must be labelled and have a 'paid for by' disclaimer. Users can click through to an archive, which will show the

44 https://www.politico.com/story/2017/10/30/facebook-russian-planted-posts-244340

45 https://eu.usatoday.com/story/tech/2017/10/30/russian-fake-accounts-showed-posts-126-million-facebook-users/815342001/

46 https://www.theguardian.com/technology/2017/nov/09/facebook-sean-parker-vulnerability-brain-psychology

campaign budget for that specific ad, how many people saw it, and more details about viewers including age, gender and location. The archive will store this information for seven years.[47]

However, the feature itself has caused controversy. News publishers have complained that Facebook is categorising posts in which they are promoting their own journalism (paying money to target particular groups of the audience) as 'political ads', rather than journalism. The concerns are self-evident and summed up notably by Mark Thompson, the chief executive of the New York Times, who described this policy as 'a threat to democracy'. For example, New York Times articles, including recipes, had been wrongly flagged as political.[48] Mr Thompson explained the concern further:

When it comes to news, Facebook still doesn't get it. In its effort to clear up one bad mess, it seems to be joining those who want to blur the line between reality-based journalism and propaganda.[49]

A Political Tool: How Political Parties Use the Platforms

It is not just the structural design of these sites that is of democratic concern. What has been given less scrutiny is the use made by political parties of the commercial services that have been made available by platforms such as Facebook. We highlight three inter-related commercial services that are sold to political parties by Facebook (although there are others):

- **First**, the platform hosts a 'Custom Audiences' feature that allows an organisation to upload their existing customer or client database, which in turn can be used to match against the Facebook user database to see if any of those particular people are also signed-up to Facebook.[50] If they are on Facebook, then those people may be directly targeted through Facebook by the advertiser using the feature. In the case of commercial entities, this is a way of allowing companies to reach their existing customers, in the case of political parties, this is a way of reaching individual supporters who are on their database.
- **Second**, political parties can then combine 'Custom Audiences' with a feature called 'customer insights'. This is a way of increasing their knowledge of their target audience, with analysis on personal traits such as 'relationship status' and 'frequency of activities' combined with third party data showing other information, such as 'online purchases', 'household income' and 'home market value'.[51]
- **Third**, there is an expansive feature called 'look-a-like' audiences which gives the same advertiser the ability to reach other Facebook members who 'look similar' to the profile of those uploaded in the Custom Audience database. [52] Facebook are not alone in offering such services, Google for example has a competitive product called Customer

47 https://www.facebook.com/politicalcontentads

48 https://www.nytimes.com/2018/06/14/business/media/mark-thompson-facebook-algorithm.html

49 https://www.nytco.com/wp-content/uploads/sites/3/MARK-THOMPSON-OPEN-MARKETS-INSTITUTE-.pdf

50 https://www.facebook.com/business/a/custom-audiences

51 https://www.facebook.com/business/help/304781119678235

52 https://www.facebook.com/business/help/231114077092092?helpref=faq_content#

Match, which enables advertisers to reach customers across 'Search, Shopping, Gmail, and YouTube'.[53]

Political case studies of these technologies in action were previously posted on the Facebook website, under their 'Facebook; Business; Success Story' section. These were since removed yet are available in web archives.[54] These case studies document a series of campaigns directly using these features including 'Custom Audiences' technologies being used by the Scottish National Party in the 2015 UK general election and the 'look-a-like' audience feature being used in Trudeau's 2015 Canadian election campaign.

These private companies can therefore have a significant influence on the political process. They have access to vast and deeply personal data, which gives them tremendous power. Their services and access to personal data give advertisers – and political campaigns –the capacity to influence behaviour, which in turn gives the platforms a unique potential to impact the democratic process. Whether this political power was intentionally designed is irrelevant. The fact remains that the power exists and has been used in ways that the public is only now beginning to understand.

Digital Spending: the Political Zeitgeist

The data analytics methods used by Cambridge Analytica are considered relatively standard in both the commercial digital advertising sector and in the political campaigning sector. As such, it is important to understand the Cambridge Analytica story occurred within a broader context – in terms of both the methods used by data analytics companies and the broader issues of how an industry uses data in political campaigns. Some of these techniques have been driven by the broader digital advertising industry, a sector made up of thousands of companies worldwide who specialise in collecting, buying and selling data on individuals and in using that data to infer and interpret what may motivate individuals to act. It is these techniques and this logic that has been gradually adopted by political campaigns.

In 2018, a combination of media attention, the investigation of the Information Commissioner's Office, legal claims and the hearings of the DCMS Select Committee in the UK have put the spotlight on Cambridge Analytica. There are however, over 250 companies operating worldwide that specialise in the use of individual data in political campaigns.[55] This includes a range of data brokers: those who politically interpret, repackage and sell a wide-range of commercial data; companies that make tools for 'digital listening' and for tracking voters as they move across devices; and political campaign strategists who advise political parties on when and where to spend their digital money in a campaign and how to get the most out of a range of data-related techniques. Some of these companies are politically aligned and some of them are non-partisan. A significant number of them have worked in UK elections and referendums over the past ten years.

Even based on the limited information we have to date, British political parties have spent

53 https://support.google.com/adwords/answer/6379332?hl=en

54 https://ourdataourselves.tacticaltech.org/posts/methods-and-practices/

55 Tactical Tech Report forthcoming: The Influence Industry:The Global Business of Using Your Data in Elections https://ourdataourselves.tacticaltech.org/projects/data-and-politics/

increasingly vast sums on these companies. Such spending by parties on digital advertising increases each year and can vary widely. Spending on the digital platforms vastly outperforms spending on national and regional traditional media.[56] For example, for the 2017 campaign, Facebook received: £2,118,045.95 from the Conservative Party, £577,542.19 from Labour, and £412,329.31 from the Liberal Democrats. Google received £562,000 from the Conservatives, £255,000 from Labour and £204,000 from the Liberal Democrats (Martin 2018). This is a significant increase from the 2015 elections when less than half the amount was spent by the Conservative party and spending by Labour and the Liberal Democrats was less than 10% of the 2017 elections. UK political campaign spending however is relatively small compared to the context of the US elections, where over $300 million was spent on digital and advertising by the Trump campaign in the last three months of the elections.

Similarly, a wide range of companies that specialise in the use of individual data in elections have worked in UK referendums and elections. These are predominantly North American companies and include, but are not limited to:

- Aristotle International, who reportedly own a '35-million-person database for the UK, which was used by at least one candidate in London's last [2004] mayoral race'[57]
- Nation Builder, a tool and set of services which has been used by most political parties in the UK in recent elections and referendums, including UKIP in the 2015 elections and SNP in the Scottish referendum
- Blue State Digital who were used by the Labour party in 2015[58]
- Jim Messina and the Messina Group, who were hired by the Conservative Party in the 2017 snap election

Brexit and Data

It has been suggested that Cambridge Analytica were also employed by Leave.EU in the Brexit referendum. However, the company deny having carried out any tangible data analysis for Leave.EU, instead suggesting that their involvement in the referendum was limited to pitching for work with Leave.EU. That position has been contested by former employees before the DCMS Committee but the Electoral Commission did not find any evidence of misused funds to Cambridge Analytica. It has been speculated that this confusion may be attributed to the fact that Cambridge Analytica did conduct some work, but they were never paid for it. This, however, has yet to be verified.

Cambridge Analytica's involvement, or lack of, in the Brexit referendum is only one aspect of the questions that have arisen with regards to the use of data-driven technologies and digital campaigning in the referendum. There are several other actors and alleged activities which are, at the time of writing, in dispute yet warrant attention. The speculations raise important questions in the context of Brexit but also serve to illustrate the breadth of the challenges at hand and the kinds of questions that will need to be navigated for increased transparency and regulation in the future.

56 The UK's seven major political parties spent £4m on advertising with US tech giants during last 2017 snap general election campaign and just £239,000 on traditional news media. (Mayhew and Kakar 2018)

57 https://www.vanityfair.com/news/2007/12/aristotle200712

58 (Blue State Digital n.d.)

For example, a hitherto little known Canadian technology company, Aggregate IQ, was involved in the Brexit referendum as a service provider. This group was not well known in the industry, nor did it have a significant web presence at the time of the referendum, yet it provided services to various Leave related groups.[59] In April 2018, Aggregate IQ told a Canadian House of Commons committee on ethics, access to information and privacy, that they are not a 'big data company' but a company who places online ads for clients and builds software that enables political campaigns to organize their contacts with voters.[60] Their current website describes them as a company providing 'digital advertising, web and software development' services.[61]

There is much speculation concerning Aggregate IQ's relationship with Cambridge Analytica and its parent companies. Former staff of Cambridge Analytica claim that Aggregate IQ were in essence a subsidiary or 'franchise'. For example, in testimony from the former Business Development Manager of Cambridge Analytica, Brittany Kaiser, before the DCMS Committee she stated, 'It was my understanding when I joined the company that AggregateIQ was our exclusive digital and data-engineering partner.'[62] Separately, evidence was submitted accompanying the testimony from Mr Wylie, which showed screenshots of corporate presentations that display the heading and logo of SCL group and the address of Aggregate IQ.[63] The Directors of Aggregate IQ, at their Commons committee hearing, acknowledged that they have been in contact with SCL in the past but denied any formal connection or more significant relationship. This is further stated on their corporate website.[64] The accuracy of their testimony, however is now under some dispute, both in Canada and in the UK.[65]

Aggregate IQ are alleged to have worked in the Brexit referendum for four Leave related parties: Vote Leave, BeLeave, Veterans for Britain and the Democratic Unionist Party. The funds Aggregate IQ allegedly received, at the time of writing are £2.7 million from Vote Leave, and an additional £625,000 from BeLeave.[66] Other money came from Veterans for Britain and the Democratic Unionist Party. It has been reported that these various payments may have broken campaign spending limits.[67]

Irrespective of the role of this particular company, the power of data was writ large over the

59 The company had a simple one page website at the relevant time, which presented much like a holding page rather than a site with any information as to their services.

60 http://www.cbc.ca/news/politics/aggregate-iq-mps-cambridge-wylie-brexit-1.4633388

61 https://aggregateiq.com/

62 https://parliamentlive.tv/Event/Index/28e9cccd-face-47c4-92b3-7f2626cd818e (Wylie) and https://www.parliamentlive.tv/Event/Index/e5ae6255-c88e-4e62-bbf4-9c0c18ba7b6b (Kaiser)

63 https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Chris%20Wylie%20Background%20papers.pdf

64 https://aggregateiq.com/

65 https://ipolitics.ca/2018/04/24/mps-roast-aggregateiq-for-murky-testimony-on-brexit-campaign-involvement/

66 It has been reported that these funds were in fact on behalf of Vote Leave

67 https://www.theguardian.com/politics/2018/apr/13/vote-leave-campaign-overspent-on-industrial-scale-says-ex-employee-mark-gettleson; and https://www.politico.eu/article/activist-suggests-vote-leave-broke-spending-rules-in-brexit-campaign-vote-leave-boris-johnson-cambridge-analytica-facebook/

referendum. In one telling example, Dominic Cummings stated that the Vote Leave campaign spent 98% of its budget on digital, which gives an indication of how important those planning the campaigns thought that digital channels were. In a blog post about his experience working on the campaign he explained that they decided to:

[P]ut almost all our money into digital (~98%) … [we held] the vast majority of our budget back and drop it all right at the end with money spent on those adverts that experiments had shown were most effective (internal code name 'Waterloo')[68]

Media reports suggest that an overall £5 million was spent in total by all 'Leave' related campaign groups on digital and data, whereas £1 million is estimated to have been spent by 'Remain' campaign groups. However, as detailed in the Annexed table, such spending is difficult to trace. Nevertheless, questions arise as to whether such spending is significant in the context of a 2% margin in the vote to leave the EU.

There is very little evidence at this point as to the efficacy of data techniques. During Mr Wylie's testimony to the DCMS Select Committee, however, he claimed that the 'conversion rates' of the digital adverts placed by the Leave campaigns were unusually high.[69] Conversion rates are the feedback mechanism for helping digital advertisers understand how many and which of their adverts lead to a significant action, such as a donation, signing up for a group or attending an event, rather than just a click. In his testimony, Wylie claimed that the 'normal' conversion rate for a digital advert would be around 1 or 2%, whereas Leave related adverts conversion rates were reportedly in the 5 to 10% range. In addition, Dominic Cummings claimed that it was one of the reasons why the Leave vote won and that in the official ten-week campaign they 'served about one billion targeted digital adverts'.[70]

A different aspect of the Brexit referendum which is currently under the spotlight is the question of where the data on citizens came from. In testimony given by Brittany Kaiser, she stated that she believed that the data was bought from companies like Experian on aspects such as citizens' credit rating.[71] How much data was bought is unknown and how it was utilised remains subject to speculation.

In her oral and written testimony, Ms Kaiser claimed that she was asked to devise a strategy for UKIP, Leave.EU and Eldon Insurance/GoSkippy data.[72] Eldon Insurance is one of Aaron Banks' insurance companies. Mr Banks is the key funder behind Leave.EU and Leave.EU's campaign activities operate from the offices of Eldon Insurance.[73]

In her testimony, Ms Kaiser raised the concern that data on customers of Eldon Insurance and data on people who had made queries to Eldon Insurance and their affiliated companies may have been used in the Brexit campaign. In her written statement to the Select Committee she stated that she had reason

68 https://blogs.spectator.co.uk/2017/01/dominic-cummings-brexit-referendum-won/

69 https://parliamentlive.tv/Event/Index/28e9cccd-face-47c4-92b3-7f2626cd818e

70 https://dominiccummings.com/2016/10/29/on-the-referendum-20-the-campaign-physics-and-data-science-vote-leaves-voter-intention-collection-system-vics-now-available-for-all/

71 https://www.parliamentlive.tv/Event/Index/e5ae6255-c88e-4e62-bbf4-9c0c18ba7b6b

72 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/written/81556.html

73 At the time of writing the contact address from the Leave.EU website and Eldon Insurance website have the same address in Bristol.

to believe that 'misuse of data was rife amongst the businesses and campaigns of Arron Bank'.[74] This remains subject to investigation. However, Eldon Insurance claims in its annual report that it holds data on 24.9 million people in Britain. The implications of such a vast data trove – and its political use – could be significant.[75]

Hiding in Plain Sight: Public Knowledge and Steps towards Accountability

There has been mass coverage and public discussion of the Cambridge Analytica/Facebook revelations. That coverage and discussion has focused on a number of issues, including the impact of the advertising techniques and the power of personal data. The very business model of companies such as Facebook has been subject to regulatory scrutiny on both sides of the Atlantic, with widespread concerns about the apparent pitfalls of a model built on data profiling and the 'attention economy'. It is these business models, and the associated potential for exploitation, that has caused political shockwaves throughout the globe.

Those involved in this drama have been called before various governmental and regional bodies to explain their actions. Notably, various personnel of Cambridge Analytica, Dr Kogan, and Mr Wylie have given evidence before the DCMS Select Committee. Whilst Facebook representatives have provided some testimony before the Committee, it has not been to the Committee's satisfaction.[76] Most of these committee hearings remain ongoing at the time of writing.

Whilst there is a grubbier angle to the alleged activities of the company[77] – and the characters involved make for convenient vaudeville villains to provide umbrage at the individuals rather than considering the industry's practices – there is a wider concern that may fall between the gaps. The actions of these companies occurred in the open, despite overtly operating to affect political change. A number of the practices also appear to have questionable legal underpinnings but the companies proceeded without sanction or accountability for a number of years. Indeed, when the companies were forced to account for their actions, they treated their own regulators with an attitude bordering on disdain.[78]

That the companies were able to operate with such indifference to any consequences shows not just a

74 Brittany Kaiser Written Testimony https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Brittany%20Kaiser%20Parliamentary%20testimony%20FINAL.pdf

75 The questions of broad data collection by Eldon Insurance and its possible misuse was further queried by journalist Carole Cadwalladr, who submitted a Subject Access Request to Eldon Insurance. The information she received showed that despite not being a customer of Eldon Insurance they did have her data on file (including her name, email address, address and family member details) due to insurance she took out through the website 'moneysupermarket'.

76 The head of the Committee, Damian Collins MP, has written to Facebook about the evidence presented. This included a potential personal summons to Mr Zuckerberg next time he is in the United Kingdom (see: https://t.co/jXZ5TjiZld).

77 An undercover "sting" operation found senior executives stating that they could perform espionage and set "honey traps" for their political clients, although the company deny being able to offer this service to their clients. See: https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation

78 In the enforcement notice from the ICO to Cambridge Analytica, the ICO revealed that Cambridge Analytica and their parent companies wrote to the ICO and said that they did ".. not expect to be further harassed with this sort of correspondence".

lack of regulation but also a lack of respect for the regulations that do exist – and an obvious gap in enforcement. The answers will not lie in wholesale legal change or reductive arguments about the loss of value in data rights. The answers rest in understanding what the role of data in politics is, the value of the regulations that exist and pairing that information to find workable and effective additional or amended solutions to make rights over data real and effective.

The issues around Cambridge Analytica also raise questions about what checks and balances need to be put in place to prevent such practices from getting out of hand in the future, both in the UK and internationally. Given the potential impact these practices have on democratic processes, this question is both urgent and in need of determined resolution.

Returning the Balance

The internet has been monetised and made commercially viable through the collection and trade of mass datasets. The inevitable conflict and necessary trade-offs that needs to be made to the value of this individual data have, until recently, been glossed over in the name of innovation. However, due to the scale and scope of the challenges that have arisen from this model in the past few years, the pendulum may be about to swing.

The first stride in the cultural shift away from voluntary data sharing and surveillance capitalism were the revelations in July 2013 by Edward Snowden, who revealed the extent of covert surveillance by a number of government agencies, including the United States National Security Agency and the British Government Communications Headquarters (GCHQ). Mr Snowden revealed that nearly every aspect of our digital lives was intercepted and retained by these agencies, which was made possible by the underlying infrastructure and mass use of large-scale commercial platforms.

One effect of the revelations was to embolden data regulators to take a stronger position in respect of personal data, in light of how easy such data was to abuse. Indeed, there was a noticeable shift in dialogue and desire for change in the drafting of the General Data Protection Regulation (GDPR) following the revelations. Whilst the GDPR was developing before the Snowden revelations, parts of the GDPR that developed in the shadow of those revelations show a marked change in approach, particularly in respect of data exports. The GDPR does make exemptions for intelligence gathering and law enforcement, yet other factors were taken into consideration in the drafting of the law. As the then Vice President of the European Commission noted,

Why would you pay someone else to hold your commercial or other secrets, if you suspect or know they are being shared against your wishes? Front or back door – it doesn't matter – any smart person doesn't want the information shared at all. Customers will act rationally, and providers will miss out on a great opportunity.[79]

Furthermore, it is notable that the European Court of Justice took an increasingly progressive and far-reaching view on data protection following the Snowden revelations. Whilst we may never know what triggered this plethora of cases, the collective effect of a number of cases should not be underestimated. For instance, within the space of 18 months, the CJEU handed down the 'right to be forgotten' case of *Google Spain*,the annulling of the US:/EU 'Safe Harbor' agreement in the *Schrems*

79 http://europa.eu/rapid/press-release_MEMO-13-654_en.htm

case and the striking down of the Data Retention Directive in *Digital Rights Ireland*.[80]

Conclusions

The recent scandals have hit public consciousness in a way that may impact personal demands for transparency and control over personal data in a greater way than even the Snowden revelations have. For, whilst the Snowden revelations revealed the extent of state surveillance carried out under the auspices of national security, recent revelations have shone a light on the potential for misuse of data on social media and collected by the private sector for political gain.[81]

In this context, the Cambridge Analytica/Facebook story coincidently arrived at the same time as the arrival into UK law as the GDPR (and the related deluge of 'consent' emails). This has had the effect of launching data regulations into mainstream consciousness, as both a force for good and a regulation with effect. Indeed, such has been the clamour for change that American legislators, lawyers and consumers have begun to ask questions as to why they are not equally protected by the GDPR.[82]

On paper, there are many companies working in the political digital space that are similar to Cambridge Analytica.[83] They are buying and processing personal data, using several different profiling and micro-targeting techniques, and working on multiple elections and referendums across borders. In practice, the difference between Cambridge Analytica and many of the other companies in the sector is how far they were willing to go and how they navigated the ethical and legal dilemmas that present themselves in using individual data for political influence. In a few important ways Cambridge Analytica is an outlier, which has garnered it a negative reputation within established political circles for some time.

However, while Cambridge Analytica is an extreme example, its story shows what can happen if the actors utilising these techniques put profit before respect for an open and fair democratic process. Moreover, it points to a need for action to ensure that all operators offering such services, and the commercial actors purchasing such services, are aware of the potential impact of different services and comply with a sufficiently robust and enforced regulatory regime.

80 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

81 It should be noted that, despite the recent scandal to hit Facebook, its use has actually increased since. See: https://www.techradar.com/news/what-scandal-facebook-usage-actually-increased-after-cambridge-analytica. However, it is reported that users are changing their approach to the platform, being much more cautious of what is shared.

82 See, https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge. NB, companies such as Facebook have moved operations for non-EU citizens in the wake of the GDPR, seemingly to avoid compliance.

83 At the time of writing, Cambridge Analytica and its parent companies, SCL Elections and SCL Group, have appointed administrators and commenced insolvency proceedings

Part III: The Existing Framework

The right of privacy … is a powerful deterrent to anyone who would control men's minds.[86]

Justice Douglas of the United States Supreme Court

1. Overview of the Relevant Elements of Electoral Law

Electoral law in its current form was designed and developed to create a level playing field between the various actors, whilst simultaneously allowing for accountability for campaigning practices. The key focus areas of electoral law, for these purposes, are (a) imposing spending limits (and at least some transparency and reporting obligations); and (b) controlling the use of television for political campaigning. The ability of Electoral law to combat the problems identified above is, however, limited. That is because it was designed with a different aim and was developed to combat problems in the pre-big data world. At most, tools such as spending limits (at least as currently designed), can only have an indirect impact on the challenges to democracy posed by the growth of big data.

a. Spending limits and associated controls

With respect to spending limits, the key legislation is the Political Parties, Elections and Referendums Act 2000 (PPERA). The main controls operating under PPERA are as follows:

- Political parties must register with the Electoral Commission if they are intending to contest elections within the UK (Section 22).[85]
- Political parties are under a duty to keep accounting records,[86] and prepare annual statements/audited accounts.[87] Annual statements/audited accounts must be submitted to the Electoral Commission.[88] Loan reports must also be provided.[89]
- Restrictions are imposed on the person(s) that can qualify as permissible donors,[90] and requirements for the reporting of donations received.[91] The Electoral Commission maintains a register of all reported donations.[92]

84 Public Utilities Comm'n v. Pollak, 343 U.S. 451 (1952) Page 343 U. S. 469 (https://supreme.justia.com/cases/federal/us/343/451/case.html) Dissenting opinion of Judge Douglas

85 Section 22 PPERA.

86 Section 41 PPERA.

87 Section 42 PPERA. Parties with a gross income over £250,000 must have their accounts audited (section 43 PPERA).

88 Section 45 PPERA.

89 See Part IVA, Chapter 1, PPERA.

90 Section 54 PPERA. Sections 54A and 54B PPERA, which require the source of donations over a certain limit to be declared and declarations that the donor satisfies residence conditions etc, have not yet been brought into force.

91 Chapter III, Part IV, PPERA.

92 Section 69, PPERA.

- Spending limits on what political parties can spend in relation to general elections and referendums, as well as controls on certain types of expenditure by third parties supporting political campaigns. See Sections 72 to 100 and 124A, 130-135 PPERA.[93] Spending by individual candidates on their election expenses is generally excluded from this definition of campaign expenditure and is regulated through the Representation of the People Act 1983, as amended by the PPERA.

Non-party campaigners and referendum campaigners that want to spend over a certain amount must also register with the Electoral Commission f they intend to spend more than £20,000 in England or £10,000 in Scotland, Wales or Northern Ireland at a UK parliamentary general election. Campaigners at the 2016 EU referendum had to register if they wanted to spend more than £10,000.

The legislation does not prescribe the amount or level of detail a party or candidate must provide in respect of their spending. This means that the level of information provided varies, and, as demonstrated by the analysis undertaken for this report, it is not always clear how much money has been spent on online campaigns, and what that money has been spent on. This is an issue which has been raised by the Electoral Commission itself in its recent report, 'Digital Campaigning: Increasing Transparency for Voters', published in June 2018.

b. No political broadcasts except permitted party election broadcasts

Paid broadcast political advertising is prohibited in the UK. Section 37 of PPERA also prohibits broadcasters from broadcasting any party-political broadcasts on behalf of an unregistered party, and section 127 PPERA puts in place similar restrictions in the context of referendums. Ofcom is responsible for considering whether television and radio advertisements have been directed towards a political end or placed by a body whose aims are wholly or mainly of a political nature (see Communications Act 2003 and the rules published by Ofcom[94]). Section 37 of PPERA also prohibits broadcasters from broadcasting any party-political broadcasts on behalf of an unregistered party, and section 127 PPERA puts in place similar restrictions in the context of referendums.

The only political messages or adverts that can be carried by broadcasters are relatively tightly regulated party election broadcasts. Broadcasters must comply with the harm and offence and incitement rules of the Ofcom Broadcasting Code. BBC broadcasts must also comply with relevant provisions of the BBC Editorial Guidelines.

93 See the election-specific guidance published by the Electoral Commission. For example, "Spending for EU referendum campaigners", 28 April 2016, https://www.electoralcommission.org.uk/__data/assets/pdf_file/0006/194586/Spending-for-EU-referendum-campaigners.pdf; and "UK Parliamentary General Election 2017: Political Parties (GB & NI)" https://www.electoralcommission.org.uk/__data/assets/pdf_file/0017/224810/UKPGE-2017-Political-Parties-guidance.pdf

94 https://www.ofcom.org.uk/about-ofcom/how-ofcom-is-run/committees/election-committee

2. The Absence of Specific Regulation for Online Political Campaigning: How Did We Get Here?

There is no specific regulation of other forms of political advertising, media, including posters, newspapers and online ads. Printed campaign material must indicate who is behind the campaign and who created the materials. Beyond these requirements, the contents of the material is not regulated. No such rules currently apply to online campaign material. Political campaigning is also exempt, for example, from the Advertising Code (sometimes referred to as the CAP Code) which is administered by the Advertising Standards Authority (ASA), and enforced by the Committee of Advertising Practice (CAP).

The ASA has a wide remit to deal with different types of paid and commercial advertising. It can deal with complaints relating to:

- Press ads
- Radio and TV ads (including teleshopping presentations)
- Ads on the internet, smartphones and tablets
- Ad claims on companies' own websites
- Commercial e-mail and text messages
- Posters/billboards
- Leaflets and brochures
- Ads at the cinema
- Direct mail, whether addressed to you personally or not
- Online behavioural advertising, i.e. the practice of collecting information from web browsers so that it can be used to deliver ads that are more relevant to the user of a particular computer.

This form of self-regulation is at least imposing a form of control on the types of advertising to which it applies.

Until 1999, non-broadcast political advertising was subject to some of the rules contained in the Advertising Code, for example the rules relating to denigration and offence. However, even then political ads were exempt from the rules that required all other advertisers to tell the truth.[95]

Following the 1997 General Election, however, CAP decided to exclude political advertising from the ASA's remit because of a number of factors that risked bringing regulation in general into disrepute. The factors included:

- The short, fixed timeframes over which elections run (i.e. the likelihood that complaints subject to ASA investigation would be ruled upon after an election has taken place).
- There was no consensus between the Labour, Conservative and Liberal Democrat Parties to bring political advertising wholly within the scope of the Code. This played a part in CAP taking the decision to exclude all of it as partial regulation poses its own problems.
- There were concerns about the implications of the introduction of the Human Rights Act 1998. In particular, concerns were raised that the application of the code could be contrary to the rights of freedom of speech around democratic elections and referendums.

In 1998, the ASA referred the matter to the Neill Committee on Standards in Public Life. The report

95 See https://www.theguardian.com/commentisfree/2016/jul/06/advertising-standards-authority-political-advertisements; and https://www.asa.org.uk/news/why-we-don-t-cover-political-ads-around-the-election.html

was presented to Parliament in July 1999.

In making its recommendations, the Neill Committee observed that political parties spent large sums of money on advertising and this led to the Committee's proposals to limit election expenditure by parties (recommendations 94 to 97), which is something also used by other countries as an indirect way of controlling political advertising. This point was picked up by the Government in presenting the Neill Report, and the Government's Response, to Parliament in July 1999.[96] The Government then noted at §9.3 that:

The Neill Committee further recommended that existing legislation should be reviewed to ensure that the ban on political advertising would apply equally to new communications media. The Government has recently published 'Regulating Communications : The Way Ahead'1. This sets out the results of the consultation on its Green Paper in Summer 1998 on the convergence of communications technologies2. The Government's view, endorsed by the great majority of those who responded to the consultation, is that most people will continue to rely for some time on traditional free-to-air television and radio broadcast services to meet their information and entertainment requirements.

9.4 The Government has set out in 'The Way Ahead' an evolutionary approach to the regulation of communications in the light of this assessment and will continue to keep the position under review as new services, and new delivery vehicles for those services such as the Internet, continue to emerge and gain acceptance…[97]

Clearly, times have changed.

The Neill Committee also recommended that political parties should establish a code of best practice in partnership with the advertising industry.[98] The Government responded as follows:

9.7 Paid advertising in the non-broadcast media raised a new issue for the Neill Committee that was not directly related to party funding, namely that of advertising standards. The Committee concluded that this was not an issue they could deal with in any detail in the context of their particular enquiry into the funding of political parties, but they did recommend that the political parties should seek to agree, in association with the advertising industry, a code of best practice for political advertising in the non-broadcast media (R96).

9.8 [CAP had decided to exclude political advertising from the scope of the Codes for the reasons given above.]

9.9 The Committee of Advertising Practice remains ready to assist in the development of a code of best practice which deals exclusively with political advertising, but is strongly of the view that it would not be appropriate for a body made up of representatives of the advertising industry to oversee the enforcement of such a code. The Electoral Commission has been canvassed as a possible alternative regulatory body. The Government, however, sees dangers in conferring such a role on the Electoral Commission. Adjudicating over complaints about political advertisements would inevitably draw the Electoral Commission into the party political arena in a way that could compromise its reputation for even-handedness and independence. The risk of this happening is particularly acute during the 'hothouse' atmosphere of a general election campaign. As a result, its position as

96 §9.1 of the Government's Response to the Neill Report, available at: http://webarchive.nationalarchives.gov.uk/20131205122143/http://www.archive.official-documents.co.uk/document/cm44/4413/4413-09.htm

97 Emphasis added; internal reference to 'The Way Ahead': Published by the Departments of Trade and Industry and of Culture, Media and Sport, June 1999.

98 §9.7 of the Government's Response to the Neill Report, available at: http://webarchive.nationalarchives.gov.uk/20131205122143/http://www.archive.official-documents.co.uk/document/cm44/4413/4413-09.htm

a politically impartial body could be jeopardised to the detriment of its ability to carry out its general regulatory functions.

9.10 The Government will explore with the main political parties whether there is any other existing or ad hoc body which could possibly oversee a code of practice on political advertising. If a suitable organisation can be found which commands consensus, the Government will help the political parties to reach agreement on the adoption of such a code.

However, as no consensus could be reached, this proposal was stillborn.[99]

In 2003 the Electoral Commission conducted a consultation on the regulation of electoral advertising, but concluded that the ASA should not be responsible for such advertising and did not itself establish a code. Consequently, the current CAP Code provides as follows in respect of political advertisements:

7.1 Claims in marketing communications, whenever published or distributed, whose principal function is to influence voters in a local, regional, national or international election or referendum are exempt from the Code.

7.2 Marketing communications by central or local government, as distinct from those concerning party policy, are subject to the Code.

Notwithstanding, the ASA's regular website updates explaining that it cannot consider complaints about political advertising, it received more than 350 complaints from the public about Brexit campaign advertising.[100]

The absence of control is perhaps best demonstrated by the Electoral Commission's own explanation of the legal position in respect of the content of campaign material and party election broadcasts under the hearing 'What we don't regulate – and advice on who does':

In general, political campaign material in the UK is not regulated, and it is a matter for voters to decide on the basis of such material whether they consider it accurate or not. This includes the design of the material. There is one exception to this, which is making or publishing a false statement of fact in relation to a candidate's personal character or conduct (not their political views or conduct), unless there are reasonable grounds to believe the statement is true. The Commission does not regulate this rule however, and any allegations should be made to the police.

The Advertising Standards Authority regulates advertising, but non-broadcast political material whose principal function is to influence voters is exempt from its remit. …

The Electoral Commission is also not responsible for regulating party election broadcasts (PEBs), however, these must observe the wider law - for example, on copyright, libel, contempt, obscenity, incitement to racial hatred or violence. In addition, all broadcasters' PEBs must also comply with the harm and offence and incitement rules of the Ofcom Broadcasting Code [and the BBC Editorial Guidelines when shown on that channel] …

The wider law does generally apply to political campaign material, and if you believe any material breaches have been made, for example, with regard to equalities or public order legislation, you may wish to report this to the police or seek your own legal advice.

We do not regulate the use of databases for the purpose of sending campaign material. If you are concerned as to how your name and/or address was obtained, you should contact

99 http://webarchive.nationalarchives.gov.uk/20131205122143/http://www.archive.official-documents.co.uk/document/cm44/4413/4413-09.htm; and http://www.lse.ac.uk/accounting/Assets/CARR/documents/R-R/2017-Summer/riskandregulation-33-regulating-political-advertising-in-the-uk.pdf

100 https://www.theguardian.com/commentisfree/2016/jul/06/advertising-standards-authority-political-advertisements

the organisation who sent the material in the first instance. The Information Commissioner's Office is the independent authority set up to uphold information rights in the public interest.[101]

Thus, the focus of the statutory regulation in place, and that of the Electoral Commission, is on (a) applying a restraining hand on how much parties spend and (b) regulating strictly the access of parties or political groups to broadcast media. There is no regulation designed to generally restrain the political campaigning and advertising activities of political parties or the activities of those acting on their behalf or in support of them. At best, spending limits can provide an indirect means of controlling advertising, profiling, or other data processing – and this was at least part of the purpose of introducing such controls (see above). But in the new digital age, such indirect controls are incapable of having a significant effect – not least in relation to activities of third parties on platforms such as Facebook.

As outlined above, freedom of expression concerns were relied upon, in part, in justifying a decision to preclude regulation of political advertising (beyond the restrictions on the use of broadcasting services). The question raised, however, by references to the rights of freedom of speech is whether or not any existing or proposed regulation involves a proportionate means of achieving a legitimate aim – there is no absolute right to freedom of expression.

The Electoral Commission, amongst others, points to the Information Commissioner and data protection law as a key part of the regulatory answer to the problems posed. To understand why data protection law can only be part and not the complete answer, it is necessary to understand its background and current reach.

3. Data Protection and Regulations on Communications

Many people have now heard of the General Data Protection Regulation (GDPR) and the new related Data Protection Act 2018.[102]

This section outlines the history and rationale of data protection legislation. The data protection regime is enjoying a new level of prominence, but it has been developing for some time. We also outline a less well-known but equally important suite of provisions, forming part of the overall data protection regime, namely the Privacy and Electronic Communications Regulations 2003 (PECR). An overview of the new data protection regime introduced by the GDPR is set out first, followed by a review of the complementary provisions.

a. Background and rationale

Data has been regulated since the development of even basic computing and early automated decision making. Indeed, the development of data protection regulations often shadowed the development of technology. As early as 1968, the Council of Europe published Recommendation 509 on Human Rights and Modern and Scientific Technological Developments. In 1973 and 1974 the Council of Europe built on this initial work with Resolutions 73/22 and 74/29, which established principles for the protection of personal data in automated databanks in the private and public sectors, respectively, the

101 Emphasis added. Available at https://www.electoralcommission.org.uk/our-work/roles-and-responsibilities/our-role-as-regulator-of-political-party-finances/making-an-allegation/what-we-regulate#.

102 If not from the deluge of "consent" emails then surely as a a sign of the increased awareness of data protection.

objective being to set in motion the development of national legislation based on these resolutions.

Set against this background was the increasing economic prominence of the technology. As such, in 1980, the Organisation for Economic Co-operation and Development (OECD) developed Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (the 'Guidelines'). Those Guidelines were developed to seek to harmonise the regulation of data protection. The basis for doing so were twofold; firstly, to protect privacy in light of technological developments and secondly, the concern of a privacy hierarchy developing, which would prevent the flow of data.

The broad aim of the Guidelines was therefore said to be striking a balance between protecting the privacy and the rights of individuals without creating any barriers to trade, whilst simultaneously allowing the uninterrupted flow of personal data across national frontiers.

As the OECD is open to membership beyond Europe, the Guidelines were intended to have transnational effect. However, the Guidelines were never intended to convey more than a broad set of principles to be followed when implementing legislation. In doing so, the framers created a charter of data rights, establishing eight broad data protection principles.[103] By placing the emphasis on the individual's data, the principles seek to protect the mischief that may be caused to that individual should their information be misused as technology develops. Rather than placing controls on technology, the principles protect the individual's rights in their relationship with and within the technology itself.

In addition to the protection to individual data rights, the Guidelines include principles on trans-border data flows. The Guidelines led to the adoption of further guidelines by European institutions. Firstly, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) was adopted by the Council of Europe and opened for signature to the member states of the Council of Europe on 28 January 1981. It was also open for signature to states outside Europe.

That Convention proved unsatisfactory in establishing a uniform and consistent regional data protection regime. The Convention allowed for significant deviation and, accordingly, a diverse set of regimes to develop, even within the European Commission. The European Commission was concerned to ensure harmonisation and accordingly developed a more robust and developed framework, culminating in Directive 95/46 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data' also known as the Data Protection Directive (the Directive).

The Directive builds on the Guidelines, listing the eight data protection principles and how they should be protected. The method of implementation of the Directive was left to each member state. In the United Kingdom, the Directive was incorporated into the Data Protection Act 1998 (the DPA 1998). The DPA 1998 included the eight data protection principles in schedule 1.

The eight principles are again applied as part of the GDPR, as implemented by the current Data Protection Act.[104] The eight principles have come

103 http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

104 The principles are broadly similar within the GDPR and the previous regime. See: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

to represent the framework around which the data protection framework was developed and has since evolved. The principles seek to enshrine personal autonomy and dignity over personal data by providing a class of rights over that data. In contrast to other first-generation rights, however, the data protection principles have not given rise to the same corpus of case law and parameter setting precedents. That however could be due to change, as data becomes more influential – and powerful – in our lives.

Data protection, meanwhile, has become not just an aspect of the right to respect for private life but a distinct human right of its own, at least in the EU Charter of Fundamental Rights. The Charter became legally binding EU primary law with the coming into force of the Lisbon Treaty on 1 December 2009.

b. GDPR

The GDPR puts in place a detailed regime governing the processing of personal data, building on the existing regime under the Data Protection Directive. The Data Protection Act 2018, which came into force on 23 May 2018, includes additional provisions relating to the application of the GDPR.

In summary, the key provisions of the GDPR are as follows.

Basic Principles and Core Tenets

Article 5 GDPR sets out the data protection principles. The most relevant principles in the present context are those which require personal data to be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject (the first data protection principle);
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the second data protection principle);
- Accurate, and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (the fourth data protection principle); and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (sixth data protection principle).

Processing is only lawful if and to the extent that it complies with one of six conditions set out in Article 6(1) GDPR. These conditions include, for example, Article 6(1)(e), which renders lawful: 'processing [which] is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller…'

Consent is now defined for the purposes of GDPR as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her…', i.e. consent must be explicit – and not implicit.[105]

Article 7 imposes strict conditions for the obtaining of consent from data subjects. Data controllers

105 See, in particular, the EU Article 29 working group on data protection analysis of "consent" http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

must be able to demonstrate that explicit consent was provided. If consent is given by a written declaration, it must be given in response to a written request which is presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of the GDPR is not binding, allowing data subjects to exercise their rights in relation to any unlawful processing. The effects of the new definition of consent are already being felt. Many people will have received emails from companies requesting that they confirm they are happy to continue receiving emails and advertisements.

Article 9 outlines the rules applicable to the processing of 'special categories' of personal data. The special categories of data reveal a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. It is obviously data of the highest sensitivity. Article 9 GDPR includes 10 potential bases on which processing of special category information may be lawful. However, these include Article 9(2)(g), which states: 'processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject…' This provision grants Member States' discretion over the bases to include. One basis of lawful special category processing included in the Data Protection Act 2018 is particularly relevant here, see further below.

Based on these basic principles, the GDPR then introduces a combination of *ex ante* and *ex poste* controls on data processing. In the following sub-sections, we categories the different types of regulation imposed by the regime, as *ex ante* regulatory, *ex poste* regulatory, and rights to data subjects, in order to shape the discussion of the limits of the different aspects of the regime.

Ex ante Obligations to Get it Right

The GDPR builds on the previous data protection regime by requiring controllers to comply with a number of *ex ante* obligations, designed to reduce the risk of unlawful invasions of privacy and breaches of rights. In particular:

- As outlined above, the sixth data protection principle requires (as the previous regime required) data controllers to implement appropriate technical and organisational measures to ensure compliance.
- Article 5(2) provides that: 'the data controller shall be responsible for, and be able to demonstrate, compliance with the [data] protection principles'. Article 24 GDPR outlines again the key responsibility of the data controller to implement such measures. Organisations with more than 250 employees must keep records of their processing activities (Article 30).
- Controllers must adopt a data protection by design and by default approach (Article 25 GDPR). This means that, for example, only personal data which are necessary for the specific processing in question should be used. Article 32 then makes clear that controllers must ensure a level of security of

processing appropriate to the risk posed by any breaches. This includes consideration of protective measures such as pseudonymisation, encryption, resilient systems, and testing measures. Data protection officers must also be appointed where, for example, the organisations activities require regular and systematic monitoring of data subjects on a large scale (Articles 37-39).

- Data protection impact assessments must be carried out by controllers for high risk processing (and the supervisory authority may specify types of processing that must be subject to such an assessment) (Article 35). The supervisory authority must be consulted where the assessment concludes that in the absence of mitigation measures the processing would be high risk (Article 36). The authority may then provide written guidance and/or use its enforcement powers to prevent such processing.
- Processors, entities, persons processing personal data on behalf of a controller are also subject to specific obligations under the GDPR (Articles 28-29). Controllers must ensure that the processors used provide sufficient guarantees of compliance with the data protection regime. Processors are then required to be contracted to comply with specific obligations outlined in Article 28(3). For example, processors must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- Controllers and processors are obligated to co-operate with the Member State's supervisory authorities (Article 31).

The Role of the Regulator and Breach Notifications

Under the GDPR, the Information Commissioner – the UK's supervisory authority on data protection legislation - has a number of *ex ante* obligations and/or powers designed to ensure compliance. For example:

- As outlined above, the authority must be consulted, and then respond, if an impact assessment concludes that processing would be high risk absent mitigation (Article 36).
- Authorities are obliged to encourage the drawing up of codes of conduct and certification processes for specific needs and industry areas (Articles 40 and 42).
- Authorities have the power to approve binding corporate rules designed to ensure compliance with the GDPR during data transfers abroad, subject to the requirements laid down in Article 47.
- Article 57 outlines an array of tasks for the supervisory authority, including, inter alia, the monitoring and enforcement of the GDPR, the promotion of the awareness of controllers and processors of their obligations under the GDPR, and the duty to handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and to carry out an appropriate investigation. Article 58 outlines the correspondingly broad powers enjoyed by the supervisory authority (to make information requests to controllers and processors, to carry out investigations etc.) They also have broad corrective powers, including the power to issue warnings, reprimands and to order controllers to take steps to comply with

the GDPR.

The obligations and/or powers are reflected in the new Data Protection Act 2018 (Parts 5 and 6 in particular). In particular:

- Section 115 outlines the Information Commissioner's general functions under the GDPR and other safeguards. Section 115(2) confirms that the obligations and powers enshrined in Articles 57 and 58 GDPR are conferred on the Commissioner. Section 115(3) also provides that: 'a power to issue, on the Commissioner's own initiative or on request, opinions to Parliament, the government or other institutions and bodies as well as to the public on any issue related to the protection of personal data.'
- Section 121 obliges the Commissioner to produce guidance, other than a general data sharing code, which she considers appropriate to promote good practice in the sharing of personal data. Section 122 also makes provision for appropriate direct marketing codes of practice.
- The Information Commissioner has a broad power under section 146 to require a controller or processor to permit the Commissioner to carry out an assessment of whether the controller or processor has complied or is complying with the data protection legislation. She may also issue information and enforcement notices (see sections 142 and 149 of the new Act).
- Section 129 refers to Article 58(1) GDPR, which together with Schedule 13 of the Act, grant the Commissioner the power, with the consent of a controller or processor, to carry out an assessment of whether the controller or processor is complying with good practice in the processing of personal data.
- Under 160(2), the Commissioner may produce and publish guidance about how the she proposes to exercise her other functions under this Part.
- Section 165 outlines the Commissioner's ability to process complaints from data subjects.

When things do go wrong on a case-by-case basis, the GDPR imposes new notification requirements in the event of personal data breaches (Articles 33-34). Essentially, controllers must notify the Information Commissioner (in the UK), without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Personal data breaches must also be documented. In some circumstances, the fact of the breach must be communicated to affected data subjects (in cases where the breach poses a high level of risk to affected individuals) (Article 34).

One of the key aspects of the GDPR which has garnered publicity, and prompted action by controllers and processors, is the introduction of weighty administrative fines. Article 83 is the key provision. Infringements of certain aspects of the GDPR attract two tiers of fines of up to €10 or €20 million or 2 or4% of the undertaking's turnover, whichever is higher. The threat of such fines should have a clear deterrent effect – however, any such effect will only continue if in practice it proves likely that the supervisory authority will be willing *and able* to exercise its jurisdiction in an appropriate manner.

Giving Data Subjects Information and Rights

A combination of *ex poste* and (more limited) *ex ante* controls on data processing can be imposed by data subjects, where they have the knowledge and means to do so. The GDPR sets out a number of fundamental rights enjoyed by data subjects, including, in particular:

- The right to information (Articles 12-13) – essentially a transparency obligation requiring notices to be given of the types of processing a controller will engage in.
- The right to information where data is obtained from a third party (Article 14) – a similar right as outlined directly above, but applied in situations of data sharing.
- The right to object (Article 21) – the right to object to processing carried out in reliance on an official authority or the legitimate interests of the controller or others, in particular processing involving profiling. Data subjects also have the right to object to processing for direct marketing purposes, including profiling.
- The right of subject access (Article 15) – the most-well known data subject right. It is the key gateway to the exercise of the other data protection rights in many cases. Without knowledge of and compliance with this right, it is often nigh on impossible for data subjects to know whether and if so what data is being processed.
- The right to rectification (Article 16) – this right allows data subjects to correct inaccuracies etc.
- The right to erasure (Article 17) – this is essentially the right to be forgotten.
- The right to restriction of processing (Article 18) – which arises where (a) the accuracy of the data is contested (so that the dispute may be resolved), the processing is unlawful but the data subject does not want the data to be erased, (b) the data are required by the data subject to establish a legal claim or defence of a claim, and (c) the data subject has objected to processing under Article 21, pending verification of whether the interests of the controller can override the objections of the data subject.
- The right to data portability (Article 20).

These rights are important. Control by individuals how their data are used can assist in the effort to protect and ensure the right to privacy. Data subjects can go to Court or complain to the Information Commissioner about: (a) any failure to comply with the above rights; or (b) about any unlawful processing they discover as a result of the exercise of those rights (Articles 77-79). The GDPR also introduces joint and several liability for controllers and processors involved in the same processing, in an effort to make it easier for data subjects to bring damages claims (Article 82).

Restrictions, Exemptions and Special Conditions

Member States may introduce restrictions to the rights granted to data subjects (Article 23 GDPR). Many restrictions are included in the new Data Protection Act 2018. Member States may also impose specific conditions that controllers can rely upon to justify processing special category data. Taken together, such restrictions or special conditions can provide a defence for problematic processing.

Article 85 GDPR mandates Member States to ensure

that the rights of protection for personal data and freedom of expression are reconciled, including processing for journalistic purposes and the purposes of academic, artistic or literary expression. The Data Protection Act 2018 contains a variety of provisions protecting journalistic activity (e.g. Para 13 of Part 2 of Schedule 1 and Part 5 of Schedule 2).

It is also important to note in this context that the new Data Protection Act 2018, which became law on 23 May 2018, applies protections to political parties processing which may hinder the new regime's ability to combat misuse of data. Paragraph 22, Part 2, of Schedule 1 provides political parties with a specific substantial public interest condition for the processing of special categories of personal data. It provides that:

1. This condition is met if the processing—
    a. is of personal data revealing political opinions,
    b. is carried out by a person or organisation included in the register maintained under section 23 of the Political Parties, Elections and Referendums Act 2000, and
    c. is necessary for the purposes of the person's or organisation's political activities, subject to the exceptions in sub-paragraphs (2) and (3).

2. Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to a person.

3. Processing does not meet the condition in sub-paragraph (1) if—
    a. an individual who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject (and has not given notice in writing withdrawing that requirement),
    b. the notice gave the controller a reasonable period in which to stop processing such data, and
    c. that period has ended.

4. In this paragraph, 'activities' include campaigning, fund-raising, political surveys and case-work.

The processing of special category data, such as political beliefs, is prohibited by Article 9(1) GDPR. That provision is only-dis-applied if the controller can rely on a condition in Article 9(2). Part 2 of Schedule 1 of the new Act outlines the situations in which a controller can fall within Article 9(2) GDPR. Thus, section quoted above is designed to give effect to Article 9(2) to allow for processing of 'special category' data, namely, political beliefs. However, this basis for special category processing does not remove individual data rights and political parties should be aware of and give effect to individual data protection rights.

a. The Problems and Limitations

The GDPR marks a considerable step forward in the drive to ensure the right to privacy. But it has its limitations when considered from the point of view of whether it can provide a complete answer to the problems outlined above in relation to political processing of data and targeted marketing.

The first problem is that it only applies to data qualifying as personal data. Data is not always 'personal'. It may be shared in aggregate or anonymised form. In such circumstances, the DPA 2018 and the GDPR do not apply at all. The data protection provisions also cannot help tackle the problem of inaccurate or fake news. The means

by which it is targeted at individuals or groups of individuals may be covered by the Act. But the content itself is unlikely to be regulated by the GDPR or Data Protection Act.

Moreover, it can be very difficult to know when and if personal data is being processed. The problem is that new technologies and techniques can allow data to be re-identified. Data may be 'individual' in the hands of one controller - but become personal data once included in a database operated by another. It is very difficult for individuals, and the Information Commissioner, to keep track of data and how it is being used across many different types of companies.

The second problem is that the controls exerted by data subjects, whether *ex poste* or *ex ante*, depend on two things: (a) information; and (b) resources. Most of the time data subjects do not know whether and what data are being processed. Privacy notices, the requirement for explicit consent and other GDPR measures may help with this. But in reality, the complicated web of companies involved in compiling and processing data makes it very difficult for any individual to exert real control.

Even if the data subject knows or reasonably suspects that their data is being processed unlawfully, issuing court proceedings is an expensive and risky business. Data subjects can complain to the Information Commissioner, but she does not have the resources or the wider public mandate to act on every case of breach. Further, and in any event, individual case-by-case enforcement is only likely to have a limited impact on the practices of major platforms such as Facebook – even if such a well-resourced defendant could be realistically targeted by many data subjects.

The third problem is that much of the success of the regime depends on the Information Commissioner being in a position to be effective. That requires a significant budget and the right resources to be available.

All of these problems apply in general. With respect to political campaigning on forums such as Facebook, the problem is that individualised targeted messaging may not be recognised as such by individuals – or be transparent to a regulator. The *ex ante* obligations on data controllers, and the threat of enforcement, might be hoped to dis-incentivise bad practice, but given the scale of activities discussed above, data protection alone is insufficient to ensure lawful and appropriate behaviour which does not undermine democratic values.

b. Extraterritoriality

The data protection regime described above depends on the protection of data. In contrast to first generation rights, which necessarily tie to the individual, these rights tie to the data. Accordingly, jurisdiction follows the data and is inevitably extraterritorial, as data crosses boarders at will. As a result, individuals based in third countries such as the US can have rights over their data processed in the United Kingdom.

The power of this extraterritoriality is illustrated by the Cambridge Analytica case. In particular, a US citizen, Professor David Carroll, was able to assert his rights over his personal data processed in the United Kingdom. Cambridge Analytica were resistant to the idea that jurisdiction could flow in this way and refused to provide Professor Carroll with full and complete disclosure of his file.[106]

106 In their answer to the Information Commissioner, the company stated that Professor Carroll was "no more entitled to make a subject access request under the DPA "...than a member of the Taliban sitting in a cave in the remotest corner of Afghanistan"."

The Information Commissioner disagreed and served an Enforcement Notice on the company on 4 May 2018. At the time of writing, the Information Commissioner's action, and Professor Carroll's litigation, remain ongoing.

The battle to impose EU norms on foreign data controllers thus dominates many of the current data protection reform controversies, including the 'right to be forgotten', the requirements for the legality of data exports, and the question of how overseas cloud providers should respond to state demands for access to data in the name of national security

c. PECR

PECR implement Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the 2002 Privacy Directive) was introduced to supplement the Data Protection Directive, which preceded the GDPR.

Subject to narrow and specific exceptions, the 2002 Directive and PECR, requires specific consent[107] to be obtained before the following direct marketing communications can be executed:

- automated calls (Article 13 of the 2002 Privacy Directive, Regulation 19 PECR);
- faxes (Article 13 of the 2002 Privacy Directive, Regulation 20 PECR); and
- emails/other electronic mail systems (Article 13 of the 2002 Privacy Directive, Regulation 22 PECR).

The Information Commissioner's long-held view has been that PECR apply to direct marketing by political parties. The Information Tribunal upheld this view in *Scottish National Party v the Information Commissioner* EA/2005/0021 stating, *inter alia*, that:

There is no evidence that the SNP, or for that matter any other political party, raised the matter of their different interpretation of the 2003 Regulations with the Information Commissioner until after he started to write to the SNP about what he considered to be their breaches of Regulation 19; in other words although the Information Commissioner's guidance had been posted on his web site for some years and he took the trouble to write to each political party prior to the 2005 general election making it quite clear how he interpreted the Regulations, no political party sought to take issue with him at the time.[108]

The Information Commissioner has published excellent guidance on the promotion of political campaigns in accordance with PECR, and the GDPR, entitled 'Guidance on political campaigning', 26 March 2018 (a further version will be produced after the GDPR comes into force, but the current version already contains 'GDPR updates').[109]

The limitations of PECR are however twofold. First, it addresses direct marketing only. There are many forms of political advertisements, targeted to various degrees, over platforms such as Facebook. It is not clear the extent to which any such forms of advertising could be caught by PECR. Second, the PECR regime is reliant, primarily, on the Information Commissioner to enforce it. She has taken some action in this area. For example:

107 From 25 May 2018, the standard of consent required is that prescribed by the GDPR,

108 Paragraph 99(4). Available at http://foiwiki.com/foiwiki/info_tribunal/DBFiles/Decision/i111/SNP.pdf

109 https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf

- On 10 March 2016, the Information Commissioner fined David Lammy MP £5,000 for making nuisance calls[110]
- The Information Commissioner issued an unofficial warning to the Conservative Party, and other parties generally, on the need to ensure that campaign research calls should not stray into direct marketing[111]

However, it is essential that the Information Commissioner is well-resourced if she is to be able to enforce not only PECR, but also the data protection regime more generally, including in particular the GDPR.

110 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/03/ico-delivers-cautionary-tale-to-political-campaigners-as-it-fines-nuisance-calling-mp-5-000/

111 See https://iconewsblog.org.uk/2017/10/23/when-political-market-research-crosses-the-line/

Conclusions and Recommendations

Conclusion 1:

Data as an asset

Data is an asset for those that control it, both in terms of the commodity value and the outcomes that can be generated with that information. For this reason, data acquisition by political parties is ongoing and likely to increase. The cumulative effect may be the creation of inequities in terms of possession of data on voters and the electoral insights it provides. As data is considered to be such a key asset, it also has the potential to attract investments and donations.

For the individuals, however, the financial value of their own personal data could be negligible such to diminish its value entirely. As such, financial redress for data collection cannot balance the continuing need for data rights and protection. Indeed, such arguments based solely on data commoditisation miss the mark and such perspectives offer a convenient way for data controllers to dispose of the broader issues of data misuse without balancing the rights of the data subject.

The real asset for the individual is in the value of data rights. Irrespective of control, data rights will always subsist. That is the hallmark of a rights regime, that the value is intrinsic in our humanity. Much like first generation rights, once individuals understand the value of their rights, they will be able to assert more control over the power balance. At the same time, however, given the value of controlling huge databases of personal data, it is essential that regulators and regimes are in place to ensure that the regime is enforceable at a collective, as well as individual level. This is especially true in relation to major platforms.

Conclusion 2:

The value of the existing data rights regime

Data rights are the next generation of human rights. They are a new-world expression of the traditional right to privacy. Unlike their more established forefathers, the mischief these rights seek to grapple with is difficult to pin down. Technology is advancing and evolving at a faster pace than it is possible for legislation to keep up with. And anything without shape is difficult to contain. The existing data protection regime however offers a primary solution to the problems caused by data misuse, which is to protect individual rights over their data. The regime is currently reflected in the GDPR. The framework is detailed and evolved over many years, across many jurisdictions. It has evolved in an effort to provide a response to changed technologies and to keep up with rapid technological progress. It therefore offers an established answer to the problems caused by the ever-fluid developments of technology.

The results of that regime have been positive, through both the legal precedents set and the effect on data subjects. Whilst there can and has been criticisms that the evolution of the framework has been slow to react to new problems and challenges, this was also true of first generation rights at their embryonic stages. However, those first-generation rights are now imbedded in our law and the public consciousness. As such, the real shift required is cultural, rather than in a new and different digital charter of rights. Such a charter exists in all but name; it just needs to be respected on an *ex ante* basis, as well as enforceable on an *ex poste* basis.

Recommendation 1:

Political parties, their campaigns and supporters should embrace the opportunities provided by the GDPR

In particular:

- The Information Commissioner should be invited to carry out a consensual audit and/or provide an opinion in respect of the compliance of political parties, their campaigns and/or their supporters with the data protection legislation.
- The Information Commissioner should be invited to produce updated and/or new guidance specifically addressing any problems identified as a result of the above in respect of political campaigning.
- Campaign material should be legally required to identify its source, i.e. who has prepared, commissioned or published it. This is key for data subjects to understand who is processing their data and why. The inclusion of such 'imprints' is also a key recommendation made by the Electoral Commission in its June 2018 Report, 'Digital Campaigning: Increasing Transparency for Voters.' The clear indication of who is processing data and why will assist in ensuring accountability for the content of adverts as well as the data processing undertaken.

Recommendation 2:

The Government should re-consider its position on Article 80 GDPR

Article 80(2) GDPR allows Member States to:

... provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

The new Data Protection Act 2018 has not incorporated this section of the GDPR. But the ability for appropriate interest groups to act on behalf of groups of individuals would provide real opportunities for the enforcement of data rights.

Section 187 of the new Act allows data subjects to mandate organisations to act on their behalf. Section 188 allows the Secretary of State to issue regulations allowing for collective proceedings to be brought by representative bodies on behalf of data subjects. However, again this only allows the representative authority to act if they have the data subject's authority. Instead of including Article 80(2) now, the Data Protection Act 2018 provides at section 189 requires the Secretary of State to review the issue of representation of data subjects. Some of the matters which the Secretary of State must take into account are:

- 'The merits of exercising the power under Article 80(2) of the GDPR (power to enable a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise some or all of a data subject's rights under Articles 77, 78 and 79 of the GDPR without being authorised to do so by the data subject),'
- 'The merits of making equivalent provision in relation to data subjects' rights under Article 82 of the GDPR (right to compensation)'; and
- 'The merits of making provision for a children's rights organisation to exercise some or all of a data subject's rights under Articles 77, 78, 79 and

82 of the GDPR on behalf of a data subject who is a child, with or without being authorised to do so by the data subject.'

The review period is 30 months after section 187 comes into force. It is unfortunate that there is to be such delay in the Government's consideration of Article 80(2), which would be a key mechanism for holding controllers to account where individual data subjects may not be able or may not even know there is a reason to do so. We recommend that the Government changes its position now. In the alternative, we support the introduction of measures implementing Article 80(2) at the end of the statutory review.

Recommendation 3:

It is time to re-visit the need for a Code of Conduct for political campaigning and/or the designation of a specific regulator to review political processing

In the late 1990s and early 2000s, the ideas that political parties should have their own advertising codes of conduct and/or a regulator should have the power to review political advertising were rejected on the basis, inter alia¸ that controls on spending and political broadcasting were sufficient. The world has changed. It is time to re-visit the issues at least through a public consultation so that measures can be put in place that control adequately the conduct of political campaigns, including data processing generally (personal data and non-personal data).

Recommendation 4:

Consider new spending limits

Government should consider introducing new spending limits relating specifically to spend on digital/data campaigns to address the glaring disparity in access to such mediums.

In particular, we support the following recommendations/proposals made by the Electoral Commission in its recent report 'Digital Campaigning: Increasing Transparency for Voters', published June 2018:

- Each of the UK's governments and legislatures should amend the rules for reporting spending. They should make campaigners sub-divide their spending returns into different types of spending. These categories should give more information about the money spent on digital campaigns.
- Each of the UK's governments and legislatures should change the law so that campaign-related staff costs are included in the spending limits on political party election and referendum campaign spending.
- The Electoral Commission will make proposals to campaigners and each of the UK's governments about how to improve the rules and deadlines for reporting spending. The Commission wants information to be available to voters and us more quickly after a campaign, or during it. We recommend that information should be provided in real-time during the campaigns if it is to have any ability to meaningfully constrain campaigning behaviour.

We also strongly support the Electoral Commission's recommendation that each of the UK's governments

and legislatures should increase the maximum fine we can sanction campaigners for breaking the rules. The current maximum of £20,000 is likely to become a business cost for organisations as it does not carry any meaningful deterrent effect in comparison to the funds available to many campaigns.

Recommendation 5:

Encourage spending transparency

In addition to spending limits, meaningful transparency on spending is required to cure the issues identified within the paper relating to tracking of spending. The Report contains an annexe of spending. The figures within the first table were found by analysing the 30 highest paid suppliers shown in the Electoral Commission's (EC) database of election and referendum spending for the relevant categories set by the EC (advertising, market research/canvassing, media and unsolicited materials to electors).

One take away from preparing the table is that, due to varying degrees of accessible information that can be found in spending invoices and self-reporting, there are limits to assessing exactly when 'digital' and 'data-driven' practices are used. This helps illustrate the fundamental problems in understanding, researching and analysing political data usage. The mechanisms to track such spending is difficult, complex and research intensive. Meaningful transparency would allow for clear and accountable expenditure and would ideally include transparency on all spending, including non-cash donations.

Recommendation 6:

Data and technology companies

The government needs to continue to engage with social media and digital advertising companies. There is a need to ensure the current changes in their practices are not one-off improvements or temporary acts to alleviate current public, media and governmental pressure. The rate of change of technology has not stopped and will not do so in the future. As a result, this means it as an on-going task where responses need to be developed that are not only reactive but also proactive.

The recent response of technology companies in the Irish referendum, for example Google banning advertising on their platform during the campaign and Facebook banning foreign advertising, shows that companies can make positive ethical choices.[112] However, some evidence exists to show that adverts were then moved elsewhere online, including into mobile phone games.[113] This emphasises that any approach to engage with digital technology companies has to be holistic and apply across the industry.

112 https://www.reuters.com/article/ireland-abortion-alphabet/google-to-ban-all-ads-related-to-irish-abortion-referendum-idUSL8N1SG6N0

113 https://www.theguardian.com/world/2018/may/24/irish-anti-abortion-campaigners-dodge-google-ad-ban

Annexe 1

Overview of UK Election and European Referendum Reported Spending 2015-2017

Introduction

The information presented in the following tables shows spending on data-driven digital campaigning for the 2015 and 2017 General Election campaigns and the EU referendum campaign. The tables show the reported digital spending as reported to the Electoral Commission (EC). Only suppliers who received more than £50,000 were analysed.

The problem of separating what is 'digital' is complex. As such, certain material was not included as 'digital' spending. Specifically, the table does not include:

- Companies that specialise in leaflets and door-to-door leafleting although they may use data available from online sources
- Companies that specialise in qualitative opinion polling or traditional surveys though this data might feed into digital strategies

However, the table does include strategists and consultants who deliver both digital and non-digital services where it is unclear which they delivered.[114]

I. General Election 2015

2015						
Platforms	Conservatives	Labour	Liberal Democrats	UKIP	Green Party	SNP
Facebook	£1,209,593.36	£16,454.67	£22,245.14	£91,322.04	£21,256.80	£5,466.64
Google	£312,033.79	£178.64	£11.96		£692.33	
Advertising and data companies	Conservatives	Labour	Liberal Democrats	UKIP	Green Party	SNP
Message Space	£102,293.14					
Return Marketing Limited	£86,458.67					
Luntz Malansky Strategic Research	£71,788.78					
VE Interactive	£53,100.00					
DS Political		£54,000.00				
Alchemy Social		£74,400.00				
Family Advertising Ltd				£175,620.13		
Total	**£313,640.59**	**£128,400.00**	**£0.00**	**£175,620.13**	**£0.00**	**£0.00**
Consultants and strategists	Conservatives	Labour	Liberal Democrats	UKIP	Green Party	SNP
Messina Group Inc	£369,098.93					
Belgrave Communications	£60,000.00					
Blue State Digital UK		£110,761.07				
Heavenly Group		£58,380.00				
TMWI		£54,437.73				
Small Axe					£52,941.41	
Total	**£429,098.93**	**£223,578.80**	**£0.00**	**£0.00**	**£52,941.41**	**£0.00**
Overall Total	Conservatives	Labour	Liberal Democrats	UKIP	Green Party	SNP
	£2,264,366.67	£368,612.11	£22,257.10	£266,942.17	£74,890.54	£5,466.64

114 For example, Clear Channel was included who specialise in digital out of home advertising, such as adverts seen in screens in public spaces. Crosby Textor (CTF) was excluded where it is assumed they provided non-digital opinion polling. Other Creative was included as an online and offline marketing company but no invoice was given. The assumption is made as the spend was registered under 'advertising'.

II. EU Referendum

EU Referendum				
Platforms	Britain Stronger In	Other Remain Groups	Vote Leave	Other Leave Groups
Facebook	£812,478.34	£561,562.27	£17,463.00	£88,369.63
Google	£276,776.93	£77,186.01	£638.58	£21,400.00
Advertising and data companies	Britain Stronger In	Other Remain Groups	Vote Leave	Other Leave Groups
AGGREGATEIQ			£2,697,020.91	£775,315.18
Advanced Skills Initiative Ltd			£72,018.50	
Clear Channel UK Limited			£114,395.38	
Global Superpower Ltd				£412,807.26
Family Advertising Ltd				£106,514.15
Creation Advertising Ltd				£65,129.50
Other Creative Ltd				£207,192.74
Alchemy Social		£999,018.79		
Creative Nerds		£118,000.00		
Goodstuff		£55,215.00		
Experian Ltd		£278,770.79		
Message Space	£60,823.44			
Data 8	£285,022.35			
Care2	£61,801.00			
NGP VAN	£56,607.06			
Total	**£464,253.85**	**£1,451,004.58**	**£2,883,434.79**	**£1,566,958.83**
Consultants and strategists	Britain Stronger In	Other Remain Groups	Vote Leave	Other Leave Groups
The Messina Group	£276,635.68			
Overall Total	Britain Stronger In £1,830,144.80	Other Remain Groups £2,089,752.86	Vote Leave £2,901,536.37	Other Leave Groups £1,676,728.46

III. General Election 2017

2017						
Platforms	Conservatives	Labour	Liberal Democrats	UKIP	Green Party	SNP
Facebook	£2,118,045.95	£577,269.80	£411,967.01		£18,753.15	£43,345.44
Google	£562,153.59	£254,515.51	£203,531.09			
Advertising and data companies	Conservatives	Labour	Liberal Democrats	UKIP	Green Party	SNP
Return Marketing Limited	£294,300.00					
Message Space	£100,000.00					
Total	**£394,300.00**	**£0.00**	**£0.00**	**£0.00**	**£0.00**	**£0.00**
Consultants and strategists	Conservatives	Labour	Liberal Democrats	UKIP	Green Party	SNP
Messina Group Inc	£500,015.00					
True Clarity Ltd.	£166,437.99					
Edmonds Elder Ltd	£156,240.00					
TMWI		£337,133.52				
Total	**£822,692.99**	**£337,133.52**	**£0.00**	**£0.00**	**£0.00**	**£0.00**
Overall Total	Conservatives £3,897,192.53	Labour £1,168,918.83	Liberal Democrats £615,498.10	UKIP £0.00	Green Party £18,753.15	SNP £43,345.44

When analysing spending in the EU referendum, we noted a series of inconsistencies between the Electoral Commission spending reports, the media accounts and the claims made by campaign officials. The following are a few select examples of the issues faced:

- The Vote Leave campaign director, Dominic Cummings, stated that around 98% of their budget was spent on digital.[115] However, the Electoral Commission reports suggest a lot more went on print. For example, £1,194,014.08 of their official £7,000,000 was spent on Graft Solutions Limited and the invoices suggest this was all for print. Another £179,055.64 was spent with Royal Mail for delivery of materials.

- There are reasons to speculate as to the veracity of the claims made by the campaigns themselves. For instance, Arron Banks said, 'We certainly weren't afraid of leading journalists up the country path, the same with politicians,' he said. 'Journalists are the cleverest, stupidest people on earth. They are clever, but they want to believe some of this stuff.'[116]

- There are inconsistencies in reported spending. For example, it was reported that Aggregate IQ received £3.9 million from the official Vote Leave campaign, rather than the £3.5 million as per the table above.[117]

- There is a lack of transparency on how money is spent by companies. For example, Aggregate IQ supposedly spent money on Facebook. As Facebook wasn't the supplier it wouldn't register as a 'Facebook' spend in the electoral commission reports. Further, the Aggregate IQ invoice doesn't detail any specific spends on other platforms or companies. As a further example of this, a spokesperson for the Labour Party said they spent £1 million on Facebook, which was actually through a company called Alchemy Social.

- Finally, there are issues with withheld information. For example, some invoices have not been submitted and it is therefore not possible to see whether the expenditure is on digital or non-digital services. Further, the Electoral Commission has fined Leave.EU for failing to include at least £77,380 in its spending return.[118]

115 https://blogs.spectator.co.uk/2017/01/dominic-cummings-brexit-referendum-won/

116 https://www.theguardian.com/politics/2018/jun/12/arron-banks-tells-mps-i-have-no-business-interests-in russia?CMP=Share_AndroidApp_Copy_to_clipboard

117 http://www.irishnews.com/news/2017/05/11/news/dup-s-brexit-campaign-spent-33-000-on-social-media-micro-targeting-firm-1023022/

118 https://www.electoralcommission.org.uk/i-am-a/journalist/electoral-commission-media-centre/news-releases-donations/leave.eu-fined-for-multiple-breaches-of-electoral-law-following-investigation

Annexe 2

How personal and individual data is used in the context of political campaigning

This table shows a breakdown of over 40 techniques and methods for using personal data in political campaigns. The table was assembled from research by Tactical Tech, a non-profit international technology and civil liberties organisation, by a combination of looking at recent elections worldwide, along with an in-depth review of the products and services of companies and consultants working for political campaigns worldwide.

The table shows methods divided into the following three categories: (1) Collection of data (data as an asset); (2) Analysis of data (data as intelligence); and (3) The use of data for targeting (data as influence).

Table courtesy of Stephanie Hankey, Gary Wright, Amber Macintyre at Tactical Tech

How Your Data is Used to Influence You in Political Campaigns

DATA AS AN ASSET

Data acquired about you as a political asset.

Valuable stores of existing data on potential voters, and how they are exchanged between political candidates, acquired from national repositories or sold or exposed to those who want to leverage them.

	Method	*Examples*
1	**Political data about you** Data accumulated directly by political parties on their constituencies, supporters and allies.	• Voter databases • Trade and accumulation of data on voters within parties and across candidates • User data from party- and politician-led voting and canvassing apps • Voter-customers matcher and custom audiences
2	**Consumer data about you** Data about you collected commercially and privately which is then analysed, packed and sold as political data.	• Lifestyle and consumer habits (including merging of offline and online data sets), e.g. periodicals, mobile phone location data • Private service data, e.g. insurance data, credit rating data
3	**Public data about you** Data about you collected on the open internet or through public data collection, which is packaged and sold for political use.	• Public data that is sold to the commercial sector, combined with other data, and then sold back to political parties e.g. transport, health, ID, census, social security, licences • Public data that is accessed by political parties • Inferred public data data from open information on the internet, for example data on Google Maps used to infer neighbourhood or household type

4	**Exposed data about you** Voter databases or party databases which are leaked, breached, hacked or exposed.	Examples of this exist worldwide, some databases are purely of voter lists, others are for specific communities such as expats or migrant workers, and can also contain detailed information, including passport scans and fingerprints.

DATA AS INTELLIGENCE

Data collected on you and used for digital listening to gain insights and make strategic decisions within a political campaign.

How data is accumulated and interpreted by political campaigns to learn about voters' political preferences and to inform campaign strategies and priorities, including creating voter profiles and testing campaign messaging.

	Method	*Examples*
5	**What kind of person you are** Data collected on you and then analysed with the purpose of ascertaining your values, what motivates you and what you may respond to.	• Psychometric tests, such as OCEAN (IBM Watson, Facebook, etc.) • Other kinds of behavioural and personality-based analytics
6	**What you are interested in** Data collected on you as you browse the web and use different devices and apps with the purpose of gaining insights into your habits, behaviours, values, interests, hobbies and affiliations.	• Cookies and third-party cookies • Cross-device targeting • ISP data • Tracking pixels
7	**What you are talking about online** Data collected, aggregated and analysed on what you are discussing and doing online, often referred to as 'digital listening' or 'social media listening', with the purpose of gleaning sentiment, political opinions and positions.	• Social media and online forum monitoring • Sentiment analysis
8	**What you respond to** Mass testing and modification of narratives, messages, advertisements or visual communications with the purpose of monitoring and analysing actions taken.	• A/B testing • Dynamically and algorithmically generated ads • Tracking performance of ads, 'engagement' and 'conversion rates'

DATA AS INFLUENCE

Data collected on you and analysed with the aim of targeting you as an individual and influencing your actions.

How data is analysed and used to target and reach potential voters, with the aim of influencing or manipulating their views or votes.

	Method	*Examples*
9	**Who you are** Using personal profiles and behavioural data to more effectively micro-target and attempt to influence you through posts, messages and adverts.	• Social network advertisements and dark posts (e.g. Facebook, Snapchat) • Direct mail and email • Mobile advertising through apps and social platforms
10	**Where you are** Using data on your whereabouts to influence and target you	• Geo-fencing based micro-targeting through platforms like Google or Facebook • Geo-fencing apps • Location based apps and services • Enhanced canvassing
11	**What you are looking for** Using data about what you're searching for online to influence and target you	• Black-hat search engine optimisation • Advertising driven search engine results • Ad exchange
12	**What you are watching and reading online** Using your viewing habits to influence and target you	Including micro-targeting through: • Online video services, e.g. YouTube • Network television • Online media
13	**Who you know** Using your networks and the groups and communities you associate with online to target and influence you	• Voter/canvassing apps that leverage your networks • Targeting political influencers • Messaging and targeting based on communities, such as WhatsApp and Tinder
14	**Experiments in using your data for political influence** New or developing experiments and attempts to use your data for any of the above reasons, or in combination with other techniques.	• Artificial intelligence (AI) applications to deliver more effective marketing, such as AI-Powered Voter Intelligence • AI-enabled 'chatbots' • Identity management and marketing automation

Other Publications from the Constitution Society:

Alastair Sutton, 'Relics of Empire or Full Partners in a New Global United Kingdom?: The Impact of Brexit on the UK Crown Dependencies and Overseas Territories', June 1 2018

Gordon Anthony, 'Devolution, Brexit, and the Sewel Convention', April 24 2018

Vernon Bogdanor, 'Brexit and Our Unprotected Constitution', February 21 2018

Lucy Atkinson, 'The Voluntary Sector and the UK Constitution', February 15 2018

Dawn Oliver, 'Constitutional Stewardship: A role for state or public sector bodies?', December 18 2017

Richard Reid, 'The House of Lords: Conventions and Brexit', December 6 2017

Alastair Sutton and Prof. Richard Gordon QC, 'Negotiating Brexit: The Legal Landscape', November 8 2017

Prof. Richard Rawlings, 'Brexit and the Territorial Constitution: Devolution, Reregulation and Inter-governmental Relations', October 20 2017

Simon Patrick, 'Scrutiny of Delegated Legislation in Relation to the UK's Withdrawal from the European Union', October 16 2017

Lucy Atkinson, 'House of Commons Select Committees & the UK Constitution', August 22 2017

Dr Andrew Blick, 'Entrenchment in the UK: A Written Constitution by Default?', May 10 2017

Prof Richard Gordon QC and Tom Pascoe, 'Preparing for Brexit & The Great Repeal Bill: The Legislative Options', April 5 2017

All of the Constitution Society's publications are available online at **www.consoc.org.uk**

Hard copies are also available on request. Please email **info@constitutionsoc.org.uk**

First published in Great Britain 2018
The Constitution Society
Top Floor, 61 Petty France
London SW1H 9EU
www.consoc.org.uk

ISBN: 978-1-9998886-7-1

THE
CONSTITUTION
SOCIETY