Information Commissioner's Office

# Democracy disrupted?

## Personal information and political influence

11 July 2018

ico.
Information Commissioner's Office

# Contents

# Executive summary

Political parties and campaign groups in the UK and beyond are increasingly using personal information and sophisticated data analytics techniques to target voters. The behavioural models widely used in the commercial sector have in recent years been adopted in political campaigning.

But to retain the trust and confidence of electorates and the integrity of the elections themselves, all of the organisations involved in political campaigning must use personal information and these techniques in ways that are transparent, understood by people and lawful.

This report intends to 'draw back the curtain' on how personal information is used in modern political campaigns. It summarises the policy findings from our data analytics investigation, making recommendations in respect of the transparent and lawful use of data analytics in political campaigns in the future.

Digital political campaigning can involve a range of organisations in a complex ecosystem – political parties, campaign groups, social media companies data brokers and data analytics providers. A key aim of the investigation was to explain how all of these components worked together to evaluate whether data protection compliance was effective throughout the system.

One of the most concerning findings from the investigation was a significant shortfall in transparency and provision of fair processing information. In response the Information Commissioner is calling for an 'ethical pause' to allow the key players – Government, Parliament, regulators, political parties, online platforms and citizens - to reflect on their responsibilities in respect of the use of personal data in the era of big data, before there is a greater expansion in the use of new technologies.

In parallel with our investigation, the DCMS select committee has been conducting their own inquiry into Fake News which includes use of personal information in political campaigns. At the Committee's request we are providing a progress report on our investigation, separate to this policy report, which we have also published on our website.

Our investigation found a number of areas where we believe action is required to improve each of the political parties' compliance with data protection law. Some of the issues raised included a lack of fair processing:

- in relation to use of personal data from the Electoral Register;
- when micro-targeting on social media; and
- when using software to screen people's names for likely ethnicity and age

The Information Commissioner has formally written to 11 UK political parties detailing the outcome of the investigation and the steps that need to be taken. The parties are required to report to her on the actions taken within three months. The ICO will follow up with mandatory audits. A copy of the letter is attached at Annex i.

The ICO will also be monitoring political parties, online platforms and data brokers using new assessment powers so that the public can have confidence parties and campaigns are complying with the law.

A significant finding of the ICO investigation is the conclusion that Facebook has not been sufficiently transparent to enable users to understand how and why they might be targeted by a political party or campaign. Whilst these concerns about Facebook's advertising model exist generally in relation to its commercial use, they are heightened when these tools are used for political campaigning.

Facebook's use of relevant interest categories for targeted advertising and its, Partner Categories Service are also cause for concern. Although the service has ceased in the EU, the ICO will be looking into both of these areas, and in the case of partner categories, commencing a new, broader investigation.

Specific findings about the harvesting of Facebook data in relation to Cambridge Analytica are included in our separate investigation update.

## Ten policy recommendations from the report

1) The political parties must work with the ICO, the Cabinet Office and the Electoral Commission to identify and implement a cross-party solution to improve transparency around the use of commonly held data.

2) The ICO will work with the Electoral Commission, Cabinet Office and the political parties to launch a version of its successful **Your Data Matters** campaign before the next General Election. The aim will be

to increase transparency and build trust and confidence amongst the electorate on how their personal data is being used during political campaigns.

3) Political parties need to apply due diligence when sourcing personal information from third party organisations, including data brokers, to ensure the appropriate consent has been sought from the individuals concerned and that individuals are effectively informed in line with transparency requirements under the GDPR. This should form part of the data protection impact assessments conducted by political parties.

**4) The Government should legislate at the earliest opportunity to introduce a statutory code of practice under the DPA2018 for the use of personal information in political campaigns. The ICO will work closely with Government to determine the scope of the code.**

5) It should be a requirement that third party audits be carried out after referendum campaigns are concluded to ensure personal data held by the campaign is deleted, or if it has been shared, the appropriate consent has been obtained.

6) The Centre for Data Ethics and Innovation should work with the ICO and the Electoral Commission to conduct an ethical debate in the form of a citizen jury to understand further the impact of new and developing technologies and the use of data analytics in political campaigns.

7) All online platforms providing advertising services to political parties and campaigns should include expertise within the sales support team who can provide political parties and campaigns with specific advice on transparency and accountability in relation to how data is used to target users.

8) The ICO will work with the European Data Protection Board (EDPB), and the relevant lead Data Protection Authorities, to ensure online platforms' compliance with the GDPR – that users understand how personal information is processed in the targeted advertising model and that effective controls are available. This includes greater transparency in relation to the privacy settings and the design and prominence of privacy notices.

9) All of the platforms covered in this report should urgently roll out planned transparency features in relation to political advertising to the UK. This should include consultation and evaluation of these tools by the ICO and the Electoral Commission.

10) The Government should conduct a review of the regulatory gaps in relation to content and provenance and jurisdictional scope of political advertising online. This should include consideration of requirements for digital political advertising to be archived in an open data repository to enable scrutiny and analysis of the data.

# 1. Introduction

My aim as Information Commissioner is to improve public trust and confidence in how personal information is used, by ensuring that organisations work to the highest possible information rights standards. Although accountability and transparency are not new concepts in data protection law, the General Data Protection Regulation (GDPR) that took effect on 25 May 2018 puts them centre stage by providing individuals with a greater degree of control over how their data is being used and for what purpose.

The GPPR was a response to the rapidly changing environment in which personal information is used – new technologies pose greater opportunities for organisations to exploit personal information and greater risks of privacy intrusion. Organisations will have to change their entire ethos with regard to data protection if they are going to continue to be relevant, keep the trust of the public, and flourish in the modern digital age.

My office published a report on the data protection implications of big data in 2014, which was updated to cover machine learning and artificial intelligence (AI) in 2016.[1] In that report, the ICO made clear the benefits of complying with data protection law:

> *It is not a case of big data 'or' data protection, or big data 'versus' data protection. That would be the wrong conversation. Privacy is not an end in itself, it is an enabling right. Embedding privacy and data protection into big data analytics enables not only societal benefits such as dignity, personality and community, but also organisational benefits like creativity, innovation and trust. In short, it enables big data to do all the good things it can do. Yet that's not to say someone shouldn't be there to hold big data to account.*

Given the hidden and invisible nature of how new technologies are applied to the processing of personal information, it is important that the ICO identifies proactive investigations to improve standards of information rights practice in the UK. Section 51 of the Data Protection Act (DPA) 1998 gives the Information Commissioner the legal authority to conduct *own motion* investigations and to enforce compliance without receiving a complaint from an organisation or individual:

[1] https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

> *It shall be the duty of the Commissioner to promote the following of good practice by data controllers and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data controllers.*

In March 2017, the ICO conducted an initial risk review arising from the use of data analytics in the context of the European Union (EU) referendum, following an article in The Observer.[2] As part of this evidential review, we met with Leave.EU and Cambridge Analytica, and asked them preliminary questions. In May 2017, having considered the evidence arising from the initial assessment of allegations made, I announced that the ICO was opening a formal and broader investigation into the use of data analytics for political purposes, with a particular focus on the EU referendum campaign and the use of social media.[3]

A key purpose of the investigation was to 'draw back the curtain' on how personal information is used in modern political campaigns. The data protection framework in the UK (formerly the DPA 1998, now the GDPR and DPA 2018) requires organisations to process personal information fairly and transparently. The majority of the investigation was conducted under the DPA 1998, whilst also projecting forward to the GDPR where appropriate.

Rapid social and technological developments in the use of big data mean that there is limited knowledge of – or transparency around – the 'behind the scenes' data processing techniques (including algorithms, analysis, data matching and profiling) being used by organisations and businesses to micro-target individuals.

What is clear is that these tools can have a significant impact on people's privacy. It is important that there is greater and genuine transparency about the use of such techniques to ensure that people have control over their own data and that the law is upheld. When the purpose for using these techniques is related to the democratic process, the case for high standards of transparency is very strong.

Engagement with the electorate is vital to the democratic process; it is therefore understandable that political campaigns are exploring the potential of advanced data analysis tools to help win votes. The public have the right to expect that this takes place in accordance with the law as it relates to data protection and electronic marketing. Without a high level of transparency – and therefore trust amongst citizens that

[2] https://www.theguardian.com/politics/2017/feb/26/us-billionaire-mercer-helped-back-brexit

[3] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/05/blog-the-information-commissioner-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes/

their data is being used appropriately – we are at risk of developing a system of voter surveillance by default. This could have a damaging long-term effect on the fabric of our democracy and political life.

Digital political campaigning can involve a range of organisations in a complex ecosystem – political parties, campaign groups, social media companies, data brokers and data analytics providers. A key aim of the investigation was to explain how all of these components work together, ensuring that the data protection compliance is effective throughout the system.

In addition to increasing transparency about the use of data analytics and social media for political purposes, the purpose of the investigation was to use this understanding to identify whether any breaches of the DPA 1998 have occurred, and to seek to mitigate potential information rights risks arising from the practice, particularly given the implementation of the GDPR. This would include using our enforcement powers where appropriate. Where we have already taken action, this is explained in the report. In some areas, our investigations are ongoing.

This report summarises the policy findings from the investigation and makes recommendations – in particular in respect of the transparent and lawful use of data analytics in political campaigns in the future. The recommendations are included throughout the report and summarised in the Executive Summary. In parallel with our investigation, the Digital, Culture, Media and Sport Select Committee has been conducting its own inquiry into fake news, which includes the use of data in political campaigns. We believe that our report will inform its work. At the Committee's request, we are providing a progress report on our investigation; we have also published this on our website.

## 1.1 The evolution of political campaigning

Since the beginning of universal suffrage, political parties have had access to voter information, in the form of the electoral register, for political campaign purposes. Being able to communicate and engage with voters is an essential part of democratic life and effective representation. Without it, parties cannot understand citizens' priorities and develop policies accordingly; nor can citizens influence change.

Political parties and campaigns have used a variety of communication methods to engage with voters, and these have developed over time in line with advances in technology. In the early days of universal suffrage, this was in the form of doorstep canvassing and town hall hustings. Party political broadcasts have been a feature of elections since 1924 but it was not until the growth of television in the immediate post-war period that the process was formalised and the first party political broadcasts were televised in 1951 – enabling political parties to speak directly to large groups of voters.

The post-war period also saw the growth in advertising and market research techniques, which enabled political parties to better understand voters' concerns, and to shape messages accordingly through political advertising – with the use of large advertising agencies becoming widespread during the 1980s and 1990s. The advent of telephone and email canvassing by political parties and campaigns enabled direct individual contact with voters on a mass scale.

Whilst all these methods of campaigning involve traditional marketing techniques by promoting a political message in order to gain support at the ballot box, they are open and transparent; their provenance is clear; and the messages given are received against the backdrop of the wider political discourse.

The advent of social media and the growth in big data represent marked changes for political campaigning. Political parties and campaigns understandably want to take advantage of new techniques in digital campaigning. Elections are becoming increasingly 'datified', with advertising and marketing techniques being offered by a network of private contractors and data analysts, offering cutting-edge methods for audience segmentation and targeting to political parties all over the world.[4] This is attractive to political parties and campaigns as it enables them to target individual voters with messages in keeping with their particular interests and values.

In the era of closely fought elections and campaigns where the margin of votes is small, there are big gains to be made by parties and campaigns who are able to engage individual voters in the democratic debate and on major areas of public policy that are likely to influence the outcome.

New techniques in digital campaigning have the potential to have a significant impact on the outcome of political elections and campaigns, particularly in targeting voters who are deemed 'persuadable' or who have not voted regularly. Taking advantage of these new techniques therefore will become only more attractive and important in the future. These digital technologies are also efficient and affordable.

[4] *The future of political campaigning*, Demos, July 2018, p.23

However, unlike more traditional forms of campaigning, these techniques are – by their nature – more opaque. Messages are often received in an 'echo chamber' online, where voters may not hear the other side of the argument. Voters may not understand why they are receiving particular messages, or the provenance of the messages.

Free and fair elections are the bedrock of a democratic society and are enshrined in human rights law. The European Data Protection Supervisor's recent report on online manipulation notes:

> *The principle of electoral transparency is not met if the voters have no freedom to seek, receive and impart information about the process and the candidates, including about the source and spending of financial support received by a candidate or a party. These rights are also therefore challenged by online manipulation.*[5]

It is therefore essential that political parties and campaigns operate from a level playing field when accessing the electorate, and that voters have access to the full spectrum of political messaging and information and understand who the authors of the messages are.

The rules that apply offline should apply online. This is not a new game played by different rules. Data protection laws continue to apply, and they require organisations to process people's data in a fair, transparent and accountable way. However, the rapid developments in these techniques have meant that – whilst data protection law continues to apply when the processing involves personal information – regulation and cultural norms around the use of social media and data analytics in political campaigns have not kept pace. These issues are explored further in the report.

## 1.2 The impact on future elections and campaigns

This investigation is timely. It is vital that policy makers, political parties, technology companies and regulators take an ethical pause to consider the wider implications of deploying these technologies, in terms of both data protection and ethics. Many of these new technologies are still developing, but the growth in big data means the potential is enormous. There is an exponential increase in volume and scale of personal information. In the coming years, the Internet of Things will significantly increase the amount of data in the world. In 2017, there were 8.4 billion connected devices in use worldwide,

[5] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

projected to increase to 30 billion by 2020.[6] The potential use of these new technologies, the data they will produce, and how they might be applied to political campaigns in future are explored further in Chapter 3.

Whilst it is not the primary responsibility of the ICO to determine all of the ethical questions raised by the use of these techniques, what is clear is that there is a trend towards data-driven campaigns and that the techniques will become increasingly sophisticated. These techniques raise fundamental questions about the relationship between privacy and democracy, as concerns about voter surveillance could lead to disengagement with the political process.

This investigation therefore is an opportunity to address the privacy issues that these new technologies create, ensuring that political parties, campaigns, data brokers and social media organisations understand the importance of transparency and accountability under the GDPR and DPA 2018 and are putting in place processes to future-proof compliance when utilising new technologies in the future.

In order to better understand the technological context and how political micro targeting could evolve in the future we commissioned a report from the Centre for the Analysis of Social Media at the independent thinktank, DEMOS. It examines current and emerging trends in how data is used in political campaigns, how use of technology is changing and how it may evolve in the next two to five years. The DEMOS report has been published alongside this report.

## 2. The legal context: Data protection law and political campaigns GNS

Until 25 May 2018, the handling of personal information by political parties and campaigns was governed by the DPA 1998. This has been replaced by the GDPR, which took direct effect in UK law on 25 May 2018, and the DPA 2018, which received Royal Assent on 23 May 2018. This investigation has been conducted under the DPA 1998 framework; the basis of this chapter therefore describes the DPA 1998 regime and how it relates to political campaigning. However, the chapter also takes a future look and describes where the GDPR updates the law in this area. The use of electronic marketing is also

[6] *The future of political Campaigning*, Demos, p2

governed by the Privacy and Electronic Communications Regulations (PECR) 2003.

## 2.1 The DPA 1998 data protection principles

Compliance with the DPA 1998 is built on eight data protection principles. The 'data controller' is responsible for compliance. This is the organisation or individual that makes decisions about the purpose and manner in which personal information is processed. In this situation, each political party and referendum campaign is a separate data controller with separate responsibilities under the DPA 1998.

The DPA 1998 governs the 'processing' of 'personal data'. Broadly, this covers all use of electronic data about individuals from which they can be identified. It also covers manual data in particular circumstances, but that is outside the concerns of this investigation.

The first data protection principle is the cornerstone in assessing whether or not a particular use of personal information is compliant, and is possibly also the most complex principle. It contains four main requirements:

(i) Personal information must be processed fairly.

As well as common-sense interpretation of what is fair, this also requires that the political party or campaign provides a privacy notice to individuals setting out the purposes for which their personal information is to be used. We would expect this to include details of use of data analytics, profiling and marketing.

This privacy notice should be provided at the time data is collected by the political party or campaign, or within a reasonable period if it is received from a third party.

The data controller must provide a privacy notice, even if it has been obtained the data from public sources.

(ii) Personal information must be processed lawfully.

This requires compliance with other laws that apply to the political parties and campaigns when using the data – for example, electoral legislation.

(iii) Each separate purpose for which personal information is processed must comply with at least one of a list of 'conditions' set out in Schedule 2 of the DPA 1998. The two Schedule 2 conditions that are most relevant here are:

a. Consent; and

b. The condition that is often referred to as 'legitimate interests', where the use of data is necessary for the pursuit of legitimate interest of the data controller – here, the political party, campaign, or a third party – and that use does not cause undue prejudice to the individual whose data it is.

   If a political party or campaign is relying on the 'legitimate interests' condition, it must first assess the necessity of the use of data, and second formally balance the legitimate interest against the harm or prejudice that might be caused to the individuals.

(iv) In addition, where personal information falls under the DPA 1998 definition of 'sensitive personal data', each separate purpose for which personal information is processed must comply with at least one of a second list of conditions set out in Schedule 3 of the DPA 1998 (and associated statutory instruments).

It is likely that many of the political parties' and campaigns' voter databases contain sensitive personal information, because they contain the political opinions of individuals (and possibly other sensitive personal data, such as ethnicity). It is not relevant whether the political opinion assigned to an individual is speculative.

The two Schedule 3 processing conditions that are most relevant here are:

a. Explicit consent; and

b. Processing of political opinion data only by a registered political party, in the course of its legitimate political activities, and which does not cause substantial damage or substantial distress to any individual (unless that individual has given written notice to the political party to stop processing).

The second data protection principle has also been considered in some detail by the investigation. This requires that personal information must be collected for particular purposes, as set out in the privacy notice, and must not then be used for an incompatible purpose.

An example would be a business collecting and using personal data in providing its goods and/or services and providing privacy information appropriate for those products or services. That business cannot re-purpose that personal data for political campaigning without first explaining this to the individual and obtaining their consent. Otherwise, such use would be in breach of both the second and first principle, as customers would not normally expect their data to be used for political campaigning, and it would be incompatible with the uses set out in any privacy information.

## 2.2 How these apply under the GDPR

There are very similar requirements under the GDPR to the DPA 1998 first data protection principle.

Article 5, Principle (a) requires that personal information is processed 'lawfully, fairly and in a transparent manner'. Article 6 sets out the list of lawful bases (broadly equivalent to the DPA 1998 Schedule 2 conditions) that contain consent and legitimate interests as lawful bases.

Political opinions and ethnicity are classified under the GDPR as 'special category data', and processing is prohibited unless a controller can comply with one of the conditions for processing set out in Article 9 (broadly equivalent to the DPA 1998 Schedule 3 conditions). This includes explicit consent.

The DPA 2018 contains additional conditions for processing special category data for reasons of substantial public interest, including an equivalent condition for registered political parties processing personal information constituting political opinions (Schedule 1, Part 2, Paragraph 22).

There is a new condition at Section 8 of the DPA 2018 where processing special category data is necessary 'for an activity that supports or promotes democratic engagement'. This is likely to cover some activities related to referendum and election campaigns. Because this is a new condition, there is no guidance or jurisprudence at this time. This is addressed later in the report.

One key change under the GDPR is the explicit wording regarding what is required for valid consent. It must be separate from other terms and conditions, specifically identify the campaigner, include an affirmative action, and be capable of being withdrawn easily.

## 2.3 Data analytics and profiling under the GDPR

The GDPR introduces a new definition of profiling (Article 4.4) alongside enhanced rights for individuals and related obligations for controllers.

Profiling is often invisible, so controllers must be clear in their privacy notice about any unexpected uses of personal information, such as combining information about individuals from a range of sources.

Controllers must comply with all the GDPR principles, identify and record the Article 6 lawful basis for the processing, and ensure that individuals have a way to exercise their data protection rights, including the right to object to profiling in certain circumstances, and an absolute right to object to profiling for marketing purposes (Article 21).

Article 22 of the GDPR introduces specific provisions for automated decision making processes, including profiling, with legal or similarly significant effects on individuals. Profiling and automated decision-making techniques are commonly used in marketing. Organisations need to consider the likely effect of the processing, bearing in mind the target market, to decide whether these provisions apply.

Micro-targeting by political parties and campaigns may be a type of automated decision making that does have sufficiently significant effects on individuals to bring this under Article 22, meaning that political parties and campaigns must obtain individuals' explicit consent. The effects can be assessed in a Data Protection Impact Assessment. Further guidance of on this issue will also be provided in the Code of Practice proposed by the ICO (see later in the report: recommendation 7).

Political parties, candidates and campaigns must also give individuals specific information and easy ways to challenge the decision, and must take steps to prevent errors, bias and discrimination. The ICO has also produced detailed guidance, available on our website.[7]

[7] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

The Privacy and Electronic Communications Regulation 2003 and the direct marketing rules are also relevant here; more detail can be found in the ICO's Guidance on Political Campaigning.[8]

# 3. Data analytics and micro-targeting by UK political parties

## 3.1 Why focus on political parties?

As data controllers, political parties are the client for the political advertising model, and sit at the hub of the ecosystem of digital political campaigning. Without them, there is no market for the third-party services that support digital political campaigning. Whilst recent debates have focused on online platforms and political consultancies, our investigation has focused on the full range of actors. The true ethical evolution of political campaigning in the long term will only be possible if political parties recognise that they are the drivers in ensuring a high standard of data protection through the whole system.

Political parties play an extremely important role in a democratic society – in a parliamentary system, they make it possible for voters to hold government to account and provide a vital link between the citizen and the state. They can fulfil this function only if they are able to communicate effectively with the electorate. This is why they enjoy a privileged position in terms of their access and ability to build databases that cover the entire adult population.

However, the proliferation of big data and the advent and growth of social media over the last decade have led to a step change in how political parties use data and communicate with the electorate. Whilst targeted advertising is not new, big data and social media have allowed political parties to use digital advertising techniques to target voters with highly personalised adverts, often free from other competing or opposing messages, based on personal information – much of it sourced from both social media and computing devices – in relation to their interests and lifestyle habits.

It is understandable that political parties and campaigns want to make use of these new techniques. In an era of closely fought elections where marginal gains count, they may be perceived as offering a way of bypassing traditional media and communicating directly with voters, using messages with which they are more likely to engage.

[8] https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf

## 3.2 Objectives of the investigation into political parties

In this strand of the investigation, the ICO identified the following objectives:

- to understand the volume, breadth and depth of the personal information processed by political parties for campaigning purposes. This includes understanding the types of data used and where they are sourced from;
- to understand how political parties analyse personal information sets and use them to create profiles of voters, and how these are subsequently used to inform voter engagement and political advertising;
- to understand how targeted online advertising, particularly social media, operates in the context of political campaigning, with a particular focus on Facebook, given that it receives the highest amount of advertising spend;
- to consider whether there is an appropriate level of transparency in relation to the political parties' collection and use of personal information, the intrusiveness of the techniques used, and how they comply with data protection law; and
- to make recommendations and, where appropriate, take regulatory action based on evidence gathered during the investigation.

The role of the ICO is to consider whether the collection and use of personal information complies with data protection law. Ahead of the general election in 2017, the Information Commissioner wrote to all political parties with a warning that their campaigning must be within the law.[9]

The Electoral Commission is the independent body responsible for regulating political party finances and electoral registration, and providing guidance that ensures elections are well-run.[10] The ICO has therefore not investigated these matters but has considered common themes between both areas, such as transparency.

[9] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/04/information-commissioner-warns-political-groups-to-campaign-within-the-law/

[10] The Electoral Commission. Roles and responsibilities. https://www.electoralcommission.org.uk/our-work/roles-and-responsibilities/our-role-in-elections-and-referendums

There is much debate as to the effectiveness of targeted political advertising in persuading voters to vote for a particular party or campaign. The ICO's investigation has not sought to establish the extent to which these techniques work; our focus has been on whether personal information has been used within the law. The introduction to this report has set out why it is important to investigate these issues now, as the potential to target and influence voters is increasing rapidly due to technological developments. The fact that significant investment is made by the parties in targeted advertising is an indicator of its potential.

This investigation has particularly focussed on the data protection principle of transparency. Developments in the use of data analytics and social media by political parties have been so rapid that they have left many voters on the back foot – and if voters are unaware of how their data is being used to target them with political messages, then they may have limited awareness of how to exercise their rights in relation to the use of that data and the techniques being deployed.

## 3.3 Political parties and data protection law

Data protection law does not prevent political parties from using social media in campaign communications – in fact, as outlined earlier, their special status in the democratic process is recognised in law, giving them access to the electoral register and allowing them to process political opinion data when carrying out legitimate political activities.

Equally, political parties are not exempt from data protection law; they have responsibilities as data controllers to comply with all the requirements of the law, including the data protection principles. This is a different situation from that in a number of other countries outside the EU, where political parties may not be subject to data protection law at all. This is the case in Canada, for example, where – in light of the breach of personal information involving Cambridge Analytica and Facebook – the Standing Committee on Access to Information, Privacy and Ethics of the House of Commons has recently recommended that political activities should be subject to privacy laws.[11]

[11] www.ourcommons.ca/content/committee/421/ET

Previous enforcement actions taken by the ICO against political parties have centred on marketing techniques involving telephone calls, text messages and emails:

- In 2006, we served an enforcement notice on the Scottish National Party in relation to unlawful automated calls.
- In 2014, we served a civil monetary penalty on the Better Together Campaign in the Scottish referendum, as it had breached the PECR 2003 by sending text messages without valid consent.
- In 2016, Leave.EU was served a penalty for a similar contravention.

### 3.4 How did we approach the political parties?

As part of our investigation, we made enquiries with the 11 political parties that held a seat in the House of Commons at the start of the investigation in May 2017. We asked them about their processing of personal information, use of data extracted from social media, and use of data analytics and micro-targeting techniques. A list of all political parties within the scope of investigations covered in this report is provided in Annex i.

Specific areas of enquiry included:

- The source and type of data being held by political parties;
- The purpose of the processing;
- Whether the data is shared with other political parties and for what purpose;
- Whether political parties inform individuals about the data they hold about them and for what purpose; and
- Whether political parties have been using data analytics and micro-targeting techniques.

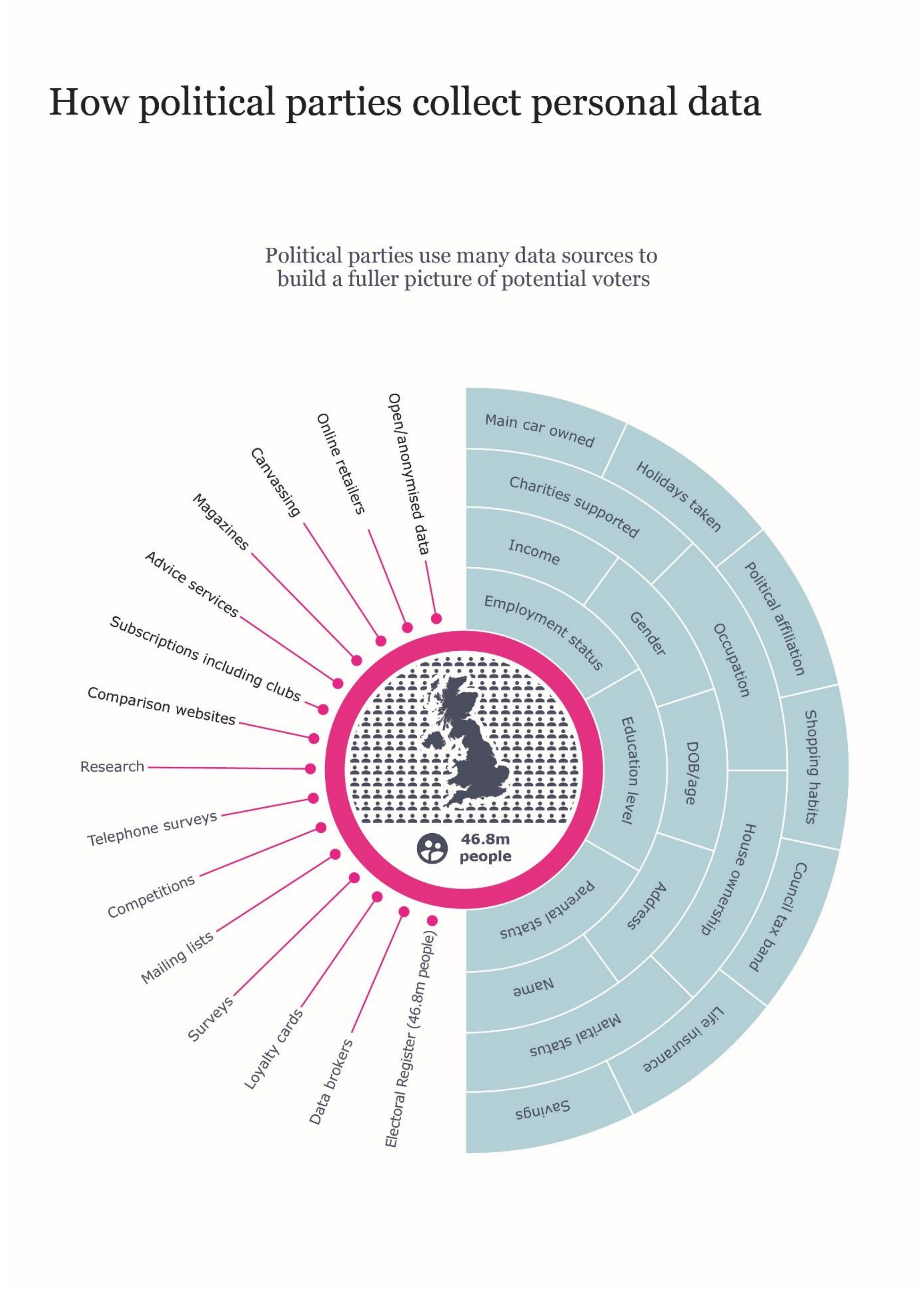
Our initial enquiries were then followed up with at least two face-to-face meetings with the three major UK wide political parties – the Conservative Party, the Labour Party and the Liberal Democrats.

Of the 11 parties contacted, only the UK Independence Party (UKIP) failed to cooperate with our investigation. It should be noted that we have not been able to progress our investigation in regards to UKIP. An Information Notice issued to UKIP in the early stages of our investigation specifying information needed to support our investigation was appealed to the Information Tribunal in November

2017. The Tribunal has dismissed the appeal, accepting that UKIP’s response to the Information Notice (which was found to accord with legislation) was brief, inadequate and in some instances possibly inaccurate and that UKIP’s apparent willingness to cooperate in the Commissioner’s enquiries rendering an Information Notice unnecessary was insufficient grounds for allowing the appeal.  The effect is that UKIP will now have to respond to the Commissioner’s request for information contained in the Commissioner’s Information Notice. We will look carefully at the evidence they send us.

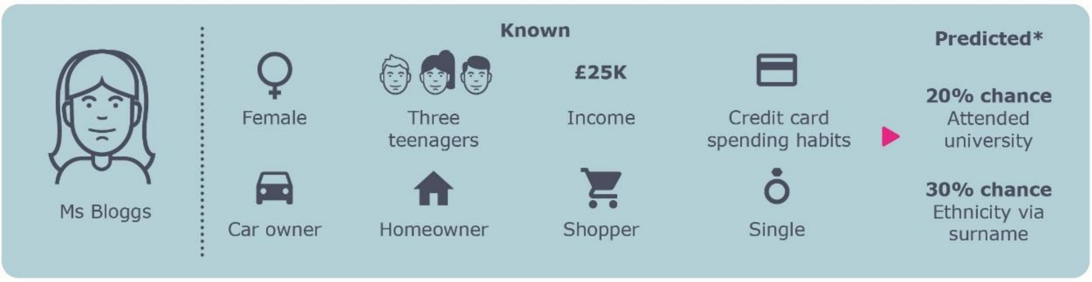
The findings and recommendations in this chapter are therefore mainly based on the activities of the Conservative, Labour and Liberal Democrat parties, but are likely to be relevant to many of the other parties too. The extent to which political parties use social media, data analytics and micro-targeting techniques is – to a large extent – dependent on their size, resources and reach into the electorate. Those who field candidates in fewer elections are less likely to deploy these methods.

## 3.5 What types of personal information do political parties use?



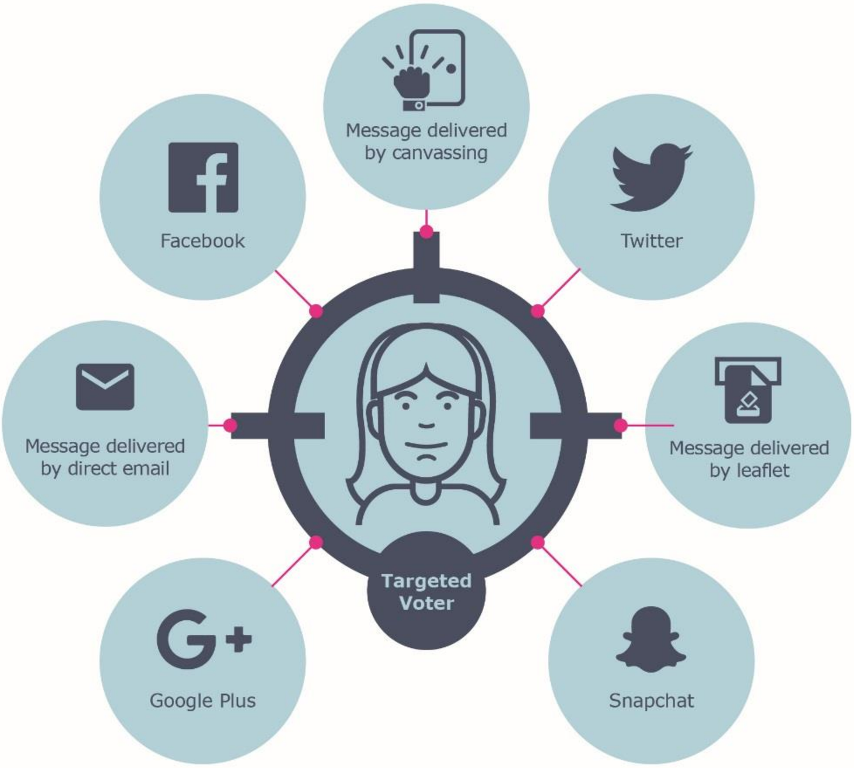
# How political parties use personal data

Information is used to create a personal profile



*Analytics is used to make predictions/assumptions about the profile

Personal profile used to target individual voters


Message delivered by canvassing
Facebook
Twitter
Message delivered by direct email
Targeted Voter
Message delivered by leaflet
Google Plus
Snapchat

All the political parties with which we made enquiries collected data about individuals in order to identify interest groups for targeted political messaging. This is done both on a geographical basis, to target marginal constituencies or wards, and on an individual basis, to attempt to identify potential swing voters and target them with personalised messages.

As previously described, all registered political parties named in the Representation of the People Regulations 2001 are entitled to access the full electoral register which gives them the names and addresses of approximately 40 million voters. [12]Political parties named in the Representation of the People Regulations 2001 are also entitled to access the 'marked register', which enables political parties to identify individuals who have voted in previous elections and referendums, but not how they have voted.

All three of the main political parties also have their own central databases, which are frequently updated in line with the electoral register and which are accessed according to how the political party is structured for constitutional and data protection registration purposes – either at a central level or on a constituency party basis.

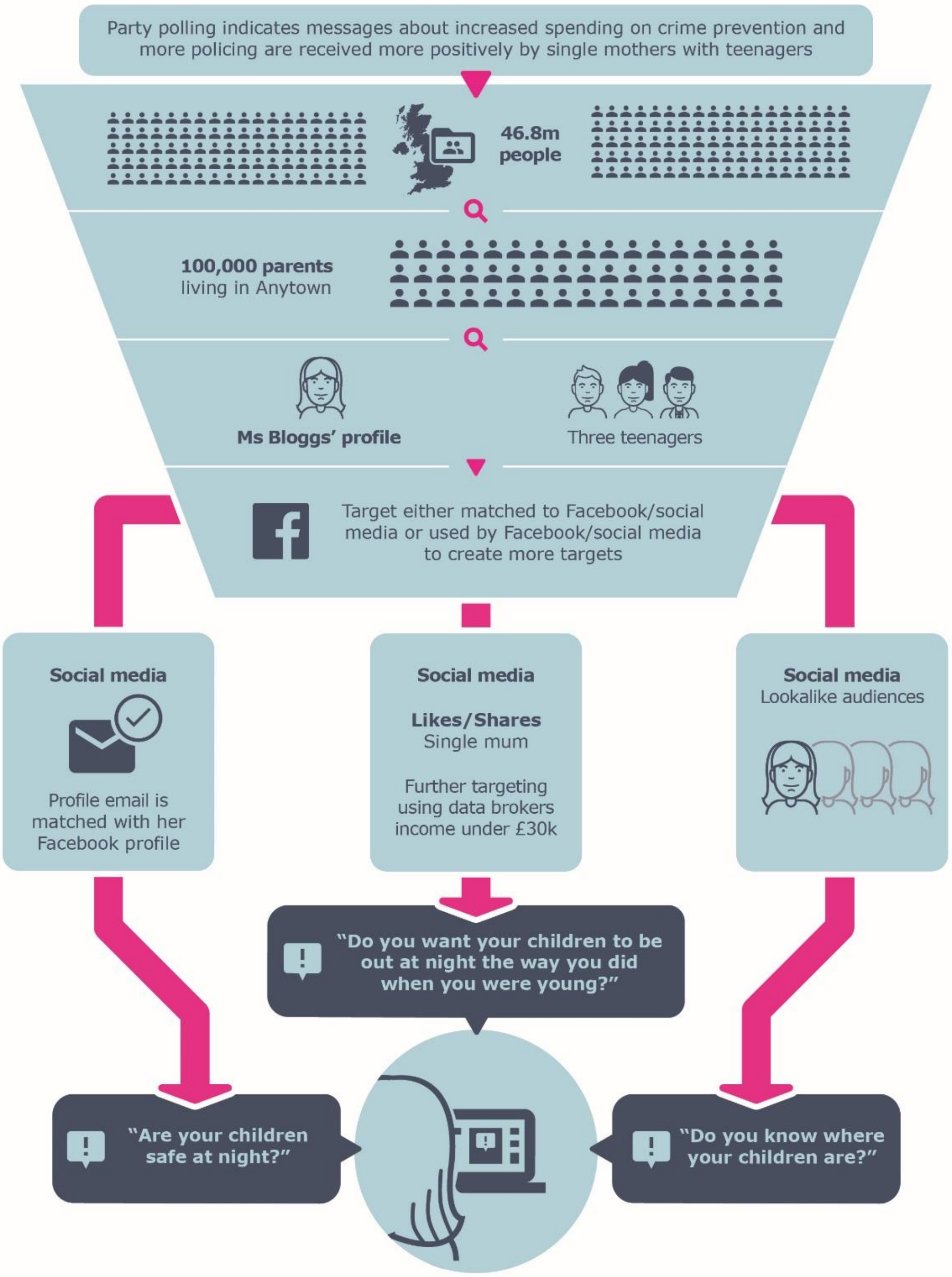
This data is then matched with other data obtained by the political parties about individuals. These include:

- Data obtained directly from the individual – for example, canvass data on the doorstep, email or telephone, and survey data. Sometimes, this will be obtained directly by the party or from third parties, for example the Labour Party told us they used 'Emma's Diary', an advice service for pregnant women.
- Third-party data, which places an individual in a particular segment/category, based on lifestyle-type information (e.g. what newspaper an individual reads, where they shop etc.) and is then used to make assumptions about their preferences and opinions. This data will be obtained from a number of sources – for example, from companies providing marketing data services (such as Experian or CACI), from data platforms (such as the widely used NationBuilder), or from people who have connected via a party's social media presence.

[12] https://www.electoralcommission.org.uk/__data/assets/pdf_file/0005/162824/List-of-people-entitled-to-be-supplied-with-the-electoral-register.pdf

## 3.6 The use of data analytics and micro-targeting by political parties

### Ways people can receive messages through micro-targeting



Party polling indicates messages about increased spending on crime prevention and more policing are received more positively by single mothers with teenagers

46.8m people

100,000 parents living in Anytown

Ms Bloggs' profile

Three teenagers

Target either matched to Facebook/social media or used by Facebook/social media to create more targets

Social media

Profile email is matched with her Facebook profile

Social media

Likes/Shares
Single mum

Further targeting using data brokers income under £30k

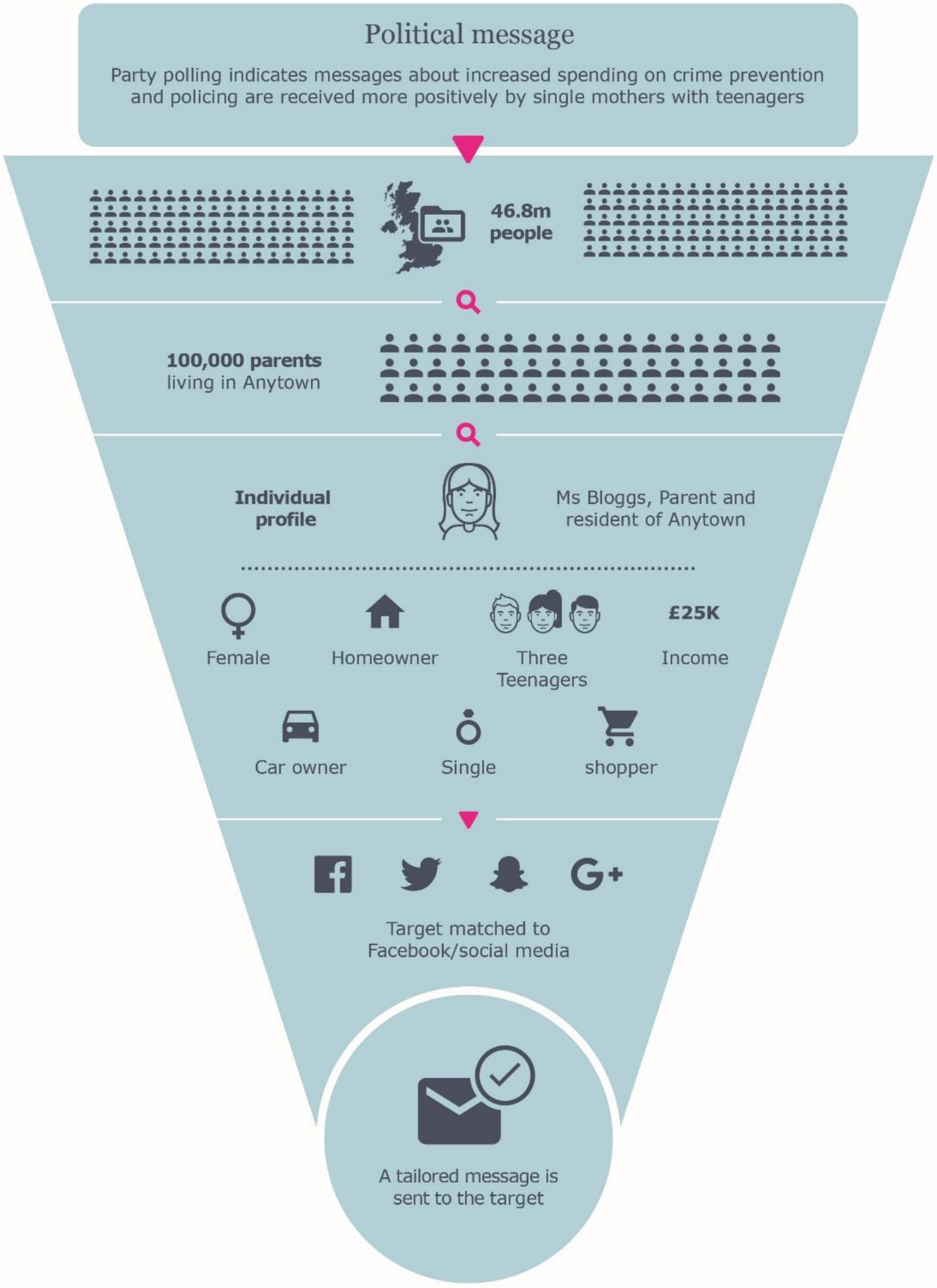
Social media
Lookalike audiences

"Do you want your children to be out at night the way you did when you were young?"

"Are your children safe at night?"

"Do you know where your children are?"

# Micro-targeting



Political message

Party polling indicates messages about increased spending on crime prevention and policing are received more positively by single mothers with teenagers

**46.8m people**

**100,000 parents** living in Anytown

**Individual profile**

Ms Bloggs, Parent and resident of Anytown

Target matched to Facebook/social media

A tailored message is sent to the target

The data held by the parties is then analysed alongside other data about previous election results and turnout. This analysis is undertaken either by the parties themselves or by a third-party data analytics company on the party's behalf, for the purposes of establishing the likelihood of an individual to vote for a particular party, and/or their likelihood of turning out to vote at all. The analysis is normally based on a model developed in advance by the party, often working with a specialised analytics company; it is usually based on actual polling data to ensure as accurate a picture as possible.

The parties can use their datasets and analysis in a number of ways, which include, for example:

- Informing the purchase of advertising that the parties place on social media – social media advertising can (depending on the platform being used) enable the parties to select ads on a range of geographic and demographic characteristics;
- Uploading the email addresses they possess into online platforms, including Facebook and other online micro targeting platforms, to match against addresses already held by the particular platform, for the purposes of targeting advertising;
- Sending out targeted emails or telephone canvassing voters; and
- Deciding who to canvass on the doorstep during the campaign or on the day of voting itself.

All these techniques fall under the umbrella of micro-targeting, of which a fuller explanation is given in the text box below.

*The term* ***'micro-targeting'*** *first arose in the context of United States political discourse. It describes targeting techniques that use data analytics to identify the specific interests of individuals, create more relevant or personalised messaging targeting those individuals, predict the impact of that messaging, and then deliver that messaging directly to them.*

*Personal data is analysed to create profiles in order to segment people according to their interests and attributes. Statistical techniques may then be used to generate analytical information or predict future behaviour.*

*Online micro-targeting can make use of cookies and similar technologies, including social plugins and tracking pixels. These can be used to track individuals' browsing habits and interactions across the internet.*

*The profiling used to inform micro-targeting also uses data from individuals' interactions on the specific platform, or on other websites that feature the tracking technologies made available by that platform. This is also often combined with 'offline' data provided from third parties, such as data brokers.*

*The increased and frequent use of the online platforms covered by our investigation all have large and growing datasets that can provide unique and deep insights into many characteristics of their users, which is very valuable to political parties and campaigns seeking to understand voter behaviour.*

## 3.7 How do political parties use campaigning platforms?

The ICO investigation found that many UK political parties used third-party digital campaigning platforms to host data and enable political engagement. These platforms are often part of the parties' web presence and provide tools for engagement, such as emails and fundraising.

In using these services, the political parties are likely to be acting as a data controller, with platforms acting as a data processor.

The most commonly used platform is NationBuilder. This platform also provides a function that enables political parties to match contact information with data on social media platforms such as Facebook and Twitter. The match function automatically takes some of the information that is publically available about the person from social media and pulls it into the NationBuilder database for that party or campaign.

## 3.8 The data protection issues raised by political parties' use of data analytics and micro-targeting

One of the most crucial findings from the ICO investigation was a significant shortfall in transparency and provision of fair processing information.

The investigation has considered the information provided by the political parties, related to the different types of data processing that they undertake. The privacy notices provided by political parties on their websites and apps and in emails did not explain the full extent of data gathered from voters and how it would be used. The privacy notices were often aimed at supporters rather than all voters, and were often inaccessible and hard to find on websites.

The parties must all make significant efforts to improve the prominence, precision and openness of the information they provide to the public about how their data is used. This should include a thorough review of privacy notices and how they can reach supporters and voters.

### 3.8.1 Lack of fair processing information in relation to the use of the electoral register

Political parties are entitled to receive a full copy of the register under the Representation of the People Regulations 2001.[13] However, this does not provide an exemption to fair processing requirements under data protection law. Parties are still required to tell individuals whose data has been obtained from the Electoral Register and what they are using that data for.

Some of the parties have provided some information in their privacy notice, but this is unlikely to be sufficient. When asked, the parties said that they assumed that individuals had access to this information through the electoral registration process; however, this is not currently the case. Schedule 1, Part II, Paragraph 2 of the DPA 1998 makes it clear that the data controller has a responsibility to provide individuals with information about the purpose or purposes for which the data they are holding is intended to be processed ‘so far as practicable’. As a point of principle, all the political parties said they understood the need to provide fair processing information in respect of this point, but they felt it would be too resource-intensive to contact the entire electorate.

Given the potential for political parties to hold personal information on the entire UK adult population, the ICO recognises the challenges of enabling transparency of data processing for political parties.

[13] https://www.electoralcommission.org.uk/__data/assets/pdf_file/0005/162824/List-of-people-entitled-to-be-supplied-with-the-electoral-register.pdf

Recommendation 1: The political parties must work with the ICO, the Cabinet Office and the Electoral Commission to identify and implement a cross-party solution to improve transparency around the use of commonly held data.

Polling cards or voter registration forms should carry a link to a central website so that voters can access information about what data political parties and campaigns have access to and their rights with regard to how the data is used.

Recommendation 2: The ICO will work with the Electoral Commission, the Cabinet Office and the political parties to launch a version of its successful 'Your Data Matters' campaign during the next general election. The aim will be to increase transparency, and to build trust and confidence amongst the electorate, on how personal data is being used during political campaigns.

### 3.8.2 Lack of fair processing information and due diligence in relation to personal information obtained from data brokers

The privacy notices we examined as part of the investigation were deficient in explaining the use of this personal information. In order to be compliant with data protection law, political parties should review their current practices and privacy notices to ensure that full and transparent information is provided to individuals about the use of their personal information. This should also include the use of data protection impact assessments. In particular, political parties should explain how they combine and use data obtained from data brokers with data from the electoral register and other locally held sources of information for profiling.

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

Going forward, in order to be compliant with the GDPR, if political parties obtain personal information from data brokers, they must carry out full due diligence to satisfy themselves the data has been obtained lawfully, and that individuals are aware of how their data will be used and to which organisations it will be passed. The decision and due diligence carried out must be fully audited. This must also be included in future data protection impact assessments.

Recommendation 3: Political parties need to apply due diligence when sourcing personal information from third-party organisations, including data brokers, to ensure (in the majority of cases) the appropriate consent has been obtained from the individuals concerned and that individuals are effectively informed in line with transparency requirements under the GDPR. This should form part of the data protection impact assessments conducted by political parties.

### 3.8.3 Use of software to screen individuals' names for likely ethnicity or age

All three main UK parties have used software that assigns a predicted ethnicity and age to individuals. This information is then used to target individuals for certain political messaging related to assumptions about their inferred ethnicity or age. Some parties were under the assumption that this was not personal information as the ethnicity or age of the individual was being inferred (rather than based on factual information), and therefore that no fair processing information needed to be provided to individuals.

However, once this data has been linked to an individual, it is the ICO's view that this is highly likely to be personal information as it becomes an opinion of ethnicity or age, and that fair processing information should therefore be provided to the individual. It is also the ICO's view that an opinion about an individual's ethnicity is highly likely to be classified as sensitive personal data under Schedule 3 of the DPA 1998 or 'special category data' under the GDPR. This means that the political parties should have identified a condition in both schedule 2 and schedule 3 of DPA1998 which applied to the processing of this data. And under the GDPR, political parties should be identifying an Article 6 lawful basis and a condition for processing under Article 9 of the DPA 2018

There are likely to be significant risks that assumptions or predictions about a person's ethnicity or age could be inaccurate, and – once directly attributed to an individual – would form inaccurate personal information, resulting in a potential contravention of the accuracy principle of Article 5(1)(d) of the GDPR. It should be noted that the parties using this software did question its usefulness, and one party indicated that it may not use it in future.

### 3.8.4 Lack of fair processing in relation to the use of personal information for micro-targeting on social media

In the course of our investigation, we identified a lack of understanding amongst political parties of the legal basis for uploading names, email addresses or phone numbers from their contact databases to social media platforms, such as Facebook's Custom Audience service, to enable targeted messages to be sent to those individuals.

Political parties who wish to provide personal information to third-party organisations for marketing purposes, whether this be social media organisations or other marketing companies, must make sure individuals are provided with fair processing information through, for example, a privacy notice. Political parties must also be able to satisfy a lawful basis for processing under Article 6 of the GDPR, and, where such data is special category data, a condition for processing under Article 9 or one of the additional conditions in the DPA 2018.

### 3.8.5 Use of third-party online campaigning platforms

The investigation found that most parties used these platforms, and the most heavily used was NationBuilder. The match function within NationBuilder's platform that allowed political parties to match data from their databases with social media data from public profiles and collect that information is of concern. The ICO has previously set out its position on the collection of public domain information following its investigation into wealth profiling by charities.[14] Data protection law does not stop data controllers from getting and using information from publicly available sources. However, they need to ensure that the way they do it complies with all the requirements of the law. Even where a party got the personal information from publicly available sources, they must still provide a privacy notice to individuals. The ICO is concerned about political parties using this functionality without adequate information being provided to the people affected. The parties must therefore include deployment of these platforms as part of future data protection impact assessments.

[14] https://ico.org.uk/media/about-the-ico/documents/2013426/fundraising-conference-2017-paper.pdf

The ICO has requested information from NationBuilder as part of its investigation. This confirmed that up to up to 200 political parties or campaign groups used NationBuilder during the 2017 general election.

## 3.9 Data brokers

The investigations progress report published in parallel to this report details the investigation and enforcement action we have taken in relation to data brokers in political campaigns. The ICO plans a further strand of work on the role of data brokers' compliance with data protection law generally, which we will report on separately later in 2018.

## 3.10 What do we require of the political parties in the future?

As set out earlier in the chapter, our investigation found a number of areas where we believe action is required to improve each of the political parties' compliance with data protection law. The Information Commissioner believes that the political parties need to make these improvements urgently in order to further safeguard individuals privacy and ensure that the political parties' data protection frameworks are robust, effective and in full accordance with the law. The Information Commissioner has written formally to the 11 political parties detailing the outcome of the investigation and the steps that need to be taken. The parties are required to report to her on the actions taken within three months.

Following completion of the actions in the letters, the Information Commissioner intends to serve Assessment Notices under section 146 of the DPA 2018. We will decide which parties will be served an assessment notice, having considered the evidence from the reports that they send to the ICO, and the breadth of data types they use and digital services deployed. All of the main political parties can expect to be served an assessment notice. Other parties will be offered an advisory visit that will provide them with practical advice on how to improve their data protection practice.

## 3.11 Use of online advertising and social media by political parties

As part of our investigation, we focused on four online platforms offering advertising services in the UK: Facebook, Google, Twitter and Snapchat. These platforms were selected from an initial assessment of the platforms most heavily used by political parties and campaigns. We required information from all four companies and they were required to attend meetings to follow up on the information provided.

Figures from the Electoral Commission show that the political parties spent £3.2 million on direct Facebook advertising during the 2017 general election. This was up from £1.3 million during the 2015 general election. By contrast, the political parties spent £1 million on Google advertising.

## 3.12 How the Facebook advertising model is used in political campaigns

Set out below are the main components of the Facebook advertising model and – where relevant – how they have been used for political campaign purposes. This element of the investigation took place from May 2017 to May 2018, and the ICO has focused on the compliance with the provisions of the DPA 1998 – in particular, the requirements of the first data protection principle to provide fair processing information to individuals. The ICO has made a number of findings about Facebook's compliance with the DPA 1998.

Under the GDPR, the Irish Data Protection Commission is the lead supervisory authority for Facebook Ireland Ltd which is the controller of personal data for UK users. The ICO can act as a 'concerned authority' in any future investigations that take place into these issues.

The key features of Facebook's advertising model relevant to political advertising are set out below.

## 3.13 Core audiences[15]

Facebook describes this feature as enabling an advertiser to manually select a target audience for a particular ad or ad campaign based on various characteristics, including age or gender, location, interests and behaviours.

Facebook describes these categories in the following way:

[15] https://en-gb.facebook.com/business/products/ads/ad-targeting#core_audiences

- *Demographics: Find people based on traits such as age, gender, relationship status, education, workplace, job titles and more.*
- *Location: Reach people in areas where advertisers want to do business. Advertisers can even create a radius around a shop to help create more walk-ins.*
- *Interests: Find people based on what they're into, such as hobbies, favourite entertainment and more.*
- *Behaviours: Reach people based on their purchasing behaviours, device usage and other activities.*

This highlights the depth and breadth of the dataset that Facebook has to enable micro-targeting.

### 3.14 Custom audiences[16]

The Custom Audiences service allows those advertising to target their existing customers on Facebook. The Custom Audience is created using existing data about an individual possessed by that organisation, which is then matched with Facebook data. The Custom Audience service allows an advertiser to target adverts to individuals via multiple methods, the most common being to upload a list of email addresses, phone numbers or user IDs that they and the advertiser already possess to Facebook. If Facebook is able to match information in its database with that uploaded by the advertiser, then those individuals may see an advert from that advertiser the next time they log into their account.

The ICO’s investigation has found that political parties are using the Facebook Custom Audience function and are uploading contact details of voters, telephone numbers and emails they hold onto the Facebook platform. The ICO has highlighted its concern to the political parties about the lack of transparency about this practice in the formal letter it has sent to them[17].

Facebook explained that it never sees the underlying data uploaded by the advertiser, and that there are no flags placed on user profiles to indicate to Facebook that they are in a Custom Audience. The advertiser – in this case, political parties – never sees exactly who is in their audience, only an approximate number. The advertiser is also responsible for the transparency and keeping their audiences up-to-date. Facebook users can see the Custom Audiences they are in by accessing their ads preferences.

[16] https://en-gb.facebook.com/business/learn/facebook-ads-reach-existing-customers

[17] A copy has been published alongside this report

### 3.15 Lookalike audiences[18]

The Lookalike Audience is based on users who have similar interests to those within a Custom Audience. Lookalike Audiences are created on the basis of a pre-existing Custom Audience, where the characteristics of that Custom Audience (eg location, age, gender, interests etc) are chosen by advertisers to create a larger group of other individuals who share the same characteristics but who are not yet engaged with the advertiser through Facebook. They are then targeted with adverts that appear on their Facebook pages in the same way as the Custom Audience. The information on who falls within a Lookalike Audience is dynamic and is not stored. Most last for a maximum of seven days but might be refreshed sooner. A Lookalike Audience is quite different from a Custom Audience, which is a fixed group of Facebook users, as the Lookalike Audience will always be moving and changing according to people's behaviour and actions.

### 3.16 Facebook Partner Categories

Facebook explained that its Partner Categories service allowed advertisers to draw on information compiled by third-party partner organisations – in the UK, Acxiom, Experian and Oracle Data Cloud – to assist in targeting Facebook users with adverts, and that this is particularly useful where an advertiser does not have sufficient data of its own to create a custom audience. The feature enables an advertiser to further refine its targeting using these third party partners' offline demographic and behavioural information, such as owning a home, being in the market for a new car, or being a loyal customer of a particular brand or product. Third-party partners collect and model data from a variety of sources, such as public records, loyalty card programs and surveys. We understand that this service has been used by the major UK-wide political parties.

### 3.17 Findings and recommendations – Facebook

Our discussions with Facebook focused on understanding how their advertising model is being used by political parties and campaigns to

[18] https://en-gb.facebook.com/business/products/ads/ad-targeting#lookalike_audiences

target users with political adverts on Facebook – and, in particular, how the level of transparency around how Facebook user data and third party data is being used to target users, and the controls available to users over the adverts they see.

### 3.18 Is adequate transparency provided to the user?

Facebook has a number of measures in place that aim to comply with the first data protection principle of the DPA 1998 and to provide fair processing information to the user. Facebook provided the detail of the measures when responding to the ICO's requests for information.

These include:

- When users see an ad, the 'Why am I seeing this?' option can be selected from a drop-down box in the corner of the advert. This is different depending on whether the ad is based on core, Custom/Lookalike Audiences, location, re-marketing or Partner Categories.

- Users are given the ability to decide that they do not want to see a particular ad again or that they do not want to see ads from that particular advertiser again.

- Information is also provided to users via the Statement of Rights and Responsibilities, Data Policy, Cookies Policy and Cookies Banner.

- Users are able to see the advertising categories assigned to them and remove them.

- Privacy Basics – a 14-module tool updated in 2015 informing users about how they can control who sees what they share on Facebook – contains five further modules describing why the user is seeing certain ads and a click through to the ads setting (which contains ad preferences and controls).

The online targeted advertising model used by Facebook is very complex, and we believe a high level of transparency in relation to political advertising is vital. This is a classic big-data scenario: understanding what data is going into the system; how users' actions on Facebook are determining what interest groups they are placed in; and then the rules that are fed into any dynamic algorithms that enable organisations to target individuals with specific adverts and messaging.

Our investigation found significant fair-processing concerns both in terms of the information available to users about the sources of the data that are being used to determine what adverts they see and the nature of the profiling taking place. There were further concerns about the availability and transparency of the controls offered to users over what ads and messages they receive. The controls were difficult to find and were not intuitive to the user if they wanted to control the political advertising they received. Whilst users were informed that their data would be used for commercial advertising, it was not clear that political advertising would take place on the platform.

The ICO also found that despite a significant amount of privacy information and controls being made available, overall they did not effectively inform the users about the likely uses of their personal information. In particular, more explicit information should have been made available at the first layer of the privacy policy. The user tools available to block or remove ads were also complex and not clearly available to users from the core pages they would be accessing. The controls were also limited in relation to political advertising.

### 3.19 Intrusiveness of categories for advertising and their use in political campaigning

Facebook allows users to enter their political affiliation on their profile page, but this affiliation information is currently not available for use in the targeted advertising model. However, political parties might be able to identify likely supporters through other relevant interest categories that could have been informed by interactions with political information online. During our investigation, we were not provided with satisfactory information to understand the process for determining what interest segments individuals were placed in. Whilst Facebook confirmed that the content of users' posts were not used to derive categories or target ads, it was difficult to understand how the different 'signals', as Facebook called them, built up to place individuals into categories.

There is also a concern that by placing users into categories, Facebook have been processing sensitive personal information – and, in particular, data about political opinions. In terms of this investigation, the ICO is particularly concerned as to how this information can be used.

The DPA 1998 defines sensitive personal information as follows:

> ‘Sensitive personal data’ means personal data consisting of information as to:
>
> - the racial or ethnic origin of the data subject;
> - political opinions;
> - religious beliefs or other beliefs of a similar nature;
> - membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
> - physical or mental health or condition;
> - sexual life;
> - the commission or alleged commission by them of any offence; or
> - any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Facebook made clear to the ICO that it does ‘not target advertising to EU users on the basis of sensitive personal data’, writing as follows:

> *However users are not identified as being interested in these topics as a result of us inferring personal characteristics about them, whether sensitive or otherwise. Instead, users are identified as being interested in such topics as a result of three actions they may take on the Facebook platform, namely: 'liking' a page; clicking an ad; or using an app. At no stage do we attempt to understand the user's motivations for taking any of those actions, the context behind those actions, or infer any personal characteristics about them as a result of those actions. We simply use the actions as an indicator of interest (which could be either positive or negative) in a particular topic.*
>
> *To ensure this is the case, we also put targeting categories available through Core Audiences under human review to identify any categories which could enable (or, more accurately, could be misunderstood by advertisers as enabling) people to be reached based on sensitive personal data. Existing targeting categories have been audited in this way, and we seek to ensure that any new targeting category is reviewed and approved before it is made available to advertisers.*

Facebook did not explain further how the human review process works.

The ICO accepts that indicating a person is interested in a topic is not the same as formally placing them within a special personal information category. However, a risk clearly exists that advertisers will use core audience categories in a way that does seek to target individuals based on sensitive personal information. In the context of this investigation, the ICO is particularly concerned that such categories can be used for political advertising.

The ICO believes that this is part of a broader issue about the processing of personal information by online platforms in the use of targeted advertising; this goes beyond political advertising. It is clear from academic research conducted by the University of Madrid[19] on this topic that a significant privacy risk can arise. For example, advertisers were using these categories to target individuals with the assumption that they are, for example, homosexual. Therefore, the effect was that individuals were being singled out and targeted on the basis of their sexuality.

This is deeply concerning, and it is the ICO's intention as a concerned authority under the GDPR to work via the one-stop-shop system with the Irish Data Protection Commission to see if there is scope to undertake a wider examination of online platforms' use of special categories of data in their targeted advertising models.

### 3.20 Transparency of Facebook partner categories' service

A preliminary investigation of the service has raised significant concerns about transparency of use of the service for political advertising and wider concerns about the legal basis for the service, including Facebook's claim that it is acting only as a processor for the third-party data providers. Facebook announced in March 2018[20] that it will be winding down this service over a six-month period, and we understand that it has already ceased in the EU. The ICO has also commenced a broader investigation into the service under the DPA 1998 (which will be concluded at a later date) as we believe it is in the public interest to do so.

### 3.21 Conclusion

[19] Jose Gonzalez Cabanas, Angel Cuevas, Ruben Cuevas, *Facebook use of sensitive data for advertising*, Universidad Carlos III de Madrid, Feb 2018

[20] https://newsroom.fb.com/news/h/shutting-down-partner-categories/

The ICO has concluded that Facebook has not been sufficiently transparent to enable users to understand how and why they might be targeted by a political party or campaign.

The Facebook ads preference setting allows users to block individual ads, or block ads from a particular advertiser, so they are able to ask not to receive adverts from a particular political party, but it does not allow them to block political advertising based on issues – which is an increasing feature of political advertising, as demonstrated from recent election campaigns. Individuals can opt out of particular interests, and that is likely to reduce the number of ads they receive on political issues, but it will not completely block them.

These concerns about transparency lie at the core of our investigation. Whilst these concerns about Facebook's advertising model exist in relation in general terms and its use in the commercial sphere, the concerns are heightened when these tools are used for political campaigning.

## 3.22 Other online platforms

Facebook thus far has been the biggest recipient of spend on digital advertising by political parties and campaigns to date. We also made enquires of and interviewed Google, Twitter and Snap. We have set out explanations of how their targeted advertising model works in relation to political campaigns on these three platforms at Annex ii

What is common to all of these platforms is that – until very recently – they have not in any way distinguished political uses of their online advertising products from their commercial uses. This has included no reference to the distinction in privacy notices. There is a consequent lack of transparency and control for individuals in how their information, including sensitive categories, is used to target them with political parties.

## 3.23 Findings and recommendations for online platforms

### Support provided to political parties and campaigns accessing paid advertising

All the online platforms told us that their full range of advertising services are available to political parties and campaigns in the same way as they are to all other organisations; and that they provide advice and support to political parties and campaigns in the same manner as they do for organisations in other sectors. Facebook produces tailored guidance for elected officials, government, political parties and campaigns on how to effectively manage and use the 'Pages' service, as they do with a range of other sectors, but they do not provide specific account managers for those organisations accessing paid political advertising. Twitter also produces a 'Guide for MPs' that seems to be aimed at managing their accounts. The level of support provided to political parties and campaigns in respect of advertising, therefore, is no different to the support that Facebook offers to clients in other sectors.

Whilst we understand that the support provided to organisations accessing paid advertising is around navigating the range of available tools, and not general advice on the content or attractiveness of the adverts themselves, we think – given the sensitivity in relation to political advertising and its potential impact on democratic society – that online platforms need to put in place specific infrastructures to support these activities.

Recommendation 4: All online platforms providing advertising services to political parties and campaigns should include experts within the sales support team who can provide political parties and campaigns with specific advice on transparency and accountability in relation to how data is used to target users.

This report has highlighted a number of findings in relation to the compliance of the online advertising model of the various platforms. However, the GDPR introduces a consistent approach to regulation under the one-stop-shop system. This means that the platforms are primarily subject to regulation by a lead data protection authority – determined by their main establishment in the EU – in the first instance. For example, Facebook's main EU establishment is in Ireland, and so the Irish Data Protection Commission is the lead authority. Therefore, a number of the broader issues identified in this report will need to be addressed through this system.

The European Data Protection Board, made up of the EU data protection authorities under the GDPR, have established a new sub-group to collaborate on a strategic approach to regulation of online platforms. The

ICO will be active in communicating the findings of this report to the relevant data protection authorities and the EDPB.

Recommendation 5: The ICO will work with the European Data Protection Board, and the relevant lead data protection authorities, to ensure that online platforms comply with the GDPR, that users understand how personal information is processed in the targeted advertising model, and that effective controls are available. This includes greater transparency in relation to the privacy settings, and the design and prominence of privacy notices.

We have noted that some of the online platforms have taken specific steps in relation to transparency of political advertising. For example, Twitter and Facebook both recently announced enhanced features.[21] Whilst these are welcome, they seem to be limited to specific jurisdictions and we are unclear whether their effectiveness have been assessed by third parties, including regulators.

Recommendation 6: All of the platforms covered in this report should urgently roll out planned transparency features in relation to political advertising to the UK. This should include consultation and evaluation of these tools by the ICO and the Electoral Commission.

# 4. Where next for data analytics in political campaigns?

This report has made a number of recommendations in respect of specific issues. This chapter considers the implications for our findings in the round and makes strategic system-wide recommendations.

## 4.1 Improving transparency and accountability: political campaigns and online platforms

This report has found that the use of social media and data analytics by political parties and campaigns has developed rapidly over the last five years. We can expect that technologies and the use of big data will develop at an even quicker pace in the future, and that political parties and campaigns will want to take advantage of these possibilities to better target potential voters.

[21] https://blog.twitter.com/official/en_us/topics/product/2017/New-Transparency-For-Ads-on-Twitter.html
http://facebookcanadianelectionintegrityinitiative.com/

However, the GDPR recognises that having strong data protection rights for individuals and control over how their data is used builds trust between organisations and individuals; this is as true for the relationship between political parties and the electorate as it is between commercial organisations and their customers.

All actors in this space, in particular the political parties and campaigns, now need to get the foundations right. The messaging and technologies used by political parties will vary, but they all have to be working to the same rules when it comes to data protection. We therefore recommend that the Government legislates to introduce a statutory Code of Practice for the use of personal information in political campaigns with the same effect as section 127 of DPA2018[22] and that this applies to political parties and campaigns, online platforms, analytics organisations and others engaged with the democratic process. We also propose that the code should provide guidance on how to apply the democratic engagement processing provision under section 8(e) of the DPA 2018. As with all our guidance and Codes of Practice, we would fully consult with all relevant stakeholders; this would take the form of written submissions and roundtables.

This work needs to move forward quickly to ensure that the Code of Practice is fully operational by the next general election. We also recognise that legislative time is limited; therefore, we plan to produce guidance that would then be put on a statutory footing once the government makes the legislative vehicle becomes available.

Recommendation 7: The Government should legislate at the earliest opportunity to introduce a statutory Code of Practice under the DPA 2018 for the use of personal information in political campaigns. The ICO will work closely with the Government to determine the scope of the Code.

With regard to safeguarding data in referendum campaigns, whilst this report has largely focused on the transparent use of personal information by political parties, the unique and short-term nature of referendum campaigns raises issues about how personal information used by the campaigns is protected after the referendum has taken place.

[22] http://www.legislation.gov.uk/ukpga/2018/12/section/127/enacted

Recommendation 8: It should be a requirement that third-party audits be carried out after referendum campaigns are concluded to ensure personal data held by the campaign is deleted, or if it has been shared, that the appropriate consent has been obtained.

## 4.2 Addressing future ethical questions

The findings from the investigation call for an 'ethical pause' to allow the key players – government, Parliament, regulators, political parties, online platforms and citizens – to reflect on their responsibilities in respect of the use of personal information in the era of big data before there is a greater expansion in the use of new technologies. This report focuses on the ethical questions raised about truthfulness, fairness, respect, bias and maintenance of public trust in political campaigns, but such a debate is relevant in the commercial and public sector too:

- Government and Parliament have a responsibility to ensure that transparency in the use of personal information is at the heart of policy making and legislation in relation to big data, AI and the digital economy.
- Regulators have a responsibility to support organisations to exercise their responsibilities in relation to personal information and to investigate and take action when breaches occur.
- Political parties have a responsibility to be clear about what data they are holding about voters and how they intend to use it.
- Social media companies have a responsibility to act as information fiduciaries, as citizens increasingly live their lives online.
- Citizens have a responsibility to ensure they understand their data protection rights and to ensure that they exercise them.

Demos has identified seven key trends in how political campaigns are being used in political campaigns already, and how it might develop in the future.

- Detailed audience segmentation;
- Cross-device targeting;
- Growth in the use of 'psychographic' or similar techniques;
- Use of AI to target, measure and improve campaigns;
- Use of artificial intelligence to automatically generate content;
- Election prediction using personal data to predict election results; and
- Delivery via new platforms.[23]

[23] *The future of political campaigning*, Demos, June 2018, pp.24–32

We believe that the new Centre for Data Ethics and Innovation, once up and running, could have an important role to play in leading such a debate in relation to political campaigns, bringing the key players together, and making any recommendations for future action.

Recommendation 9: The Centre for Data Ethics and Innovation should work with the ICO, the Electoral Commission and the Advertising Standards Agency to conduct an ethical debate in the form of a citizens' jury to understand further the impact of new and developing technologies and the use of data analytics in political campaigns.

## 4.3 Review of the regulation of online political advertising

This report focuses on the use of personal information in political campaigns and the roles that data protection law and the ICO play in regulating this. However, direct marketing and electoral law also play a role in this area and regulatory oversight of political campaigning is therefore shared with the Electoral Commission.

This has been the case since data protection legislation was first introduced more than two decades ago, and is now part of the cultural zeitgeist. The rules in combination are there to ensure free and fair elections, and to enhance – rather than undermine – democracy. However, the central role now played by data analytics in modern digital political campaigns means that there is an ever greater interplay between the regulatory strands, with their reach extending to the activities of social media platforms and their role in targeted political advertising.

These rules have generally worked well up to now. However, our investigation has found that whilst data protection law has been brought into the digital era, the broader law in this area has not kept pace with developments in technology. Micro-targeting techniques used by political parties and campaigns have exposed some gaps in the regulatory landscape that have occurred due to the move from offline to online campaigning.

The Electoral Commission has noted that electoral law in the UK is fragmented and – although it is generally respected and complied with – would benefit from a wholesale review to meet the challenges of modern elections. Its recent report, 'Digital campaigning: Increasing transparency for voters'[24] makes a number of recommendations to increase the transparency of digital campaigns and to ensure they are complying with UK electoral rules. These include recommendations to make it a requirement for digital material to carry an imprint saying who is behind the campaign and who created it, and for increased regulatory powers, including the ability to impose higher fines.

We support the Electoral Commission's report and welcome the UK Government's commitment to consult on whether to change the law so that digital material has to have an imprint, and we support the Electoral Commission's call for greater regulatory powers.

Recommendation 10: The Government should conduct a review of the regulatory gaps in relation to the content, provenance and jurisdictional scope of political advertising online. This should include consideration of requirements for digital political advertising to be archived in an open data repository to enable scrutiny and analysis of the data.

## 4.4 So has democracy been disrupted?

This is a complex and rapidly evolving area of activity, and the level of awareness amongst the public about how data analytics works and how their personal information is collected, shared and used through such tools is low. What is clear is that these tools have a significant impact on individuals' privacy. It is important that there is a greater and genuine transparency about the use of such techniques to ensure that people have control over their own data and the law is upheld.

We opened this report by asking whether democracy has been disrupted by the use of data analytics and new technologies. Throughout this investigation, we have seen evidence that it is beginning to have a profound effect whereby information asymmetry between different groups of voters is beginning to emerge. We are a now at a crucial juncture where trust and confidence in the integrity of our democratic process risks being undermined if an ethical pause is not taken. The recommendations made in this report – if effectively implemented – will change the behaviour and compliance of all the actors in the political campaigning space.

[24] https://www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf

We are committed to advocating and pressing for the implementation of all these recommendations, and will be updating on progress in our annual report and other public forums.

# Annex i: Political Parties in scope of investigation

- Conservative and Unionist Party
- Democratic Unionist Party
- Green Party
- Labour (and Co-operative) Party
- Liberal Democrats
- Plaid Cymru
- Scottish National Party
- Sinn Fein
- Social Democratic and Labour Party
- UK Independence Party
- Ulster Unionist Party

## Warning letter

**RE: The Information Commissioner’s investigation into data analytics for political purposes.**

The Information Commissioner has observed with concern the application of commercial behavioral advertising techniques and the lack of transparency of profiling in political campaigning, during recent elections and the EU referendum campaign in 2016.

After initial preparatory evidence gathering, in May 2017 the Commissioner announced a formal investigation into the use of data analytics in political campaigning. As part of our investigation, we contacted each of the main political parties in the UK, regarding their use of personal data.

We have had ongoing communications and discussions with the political parties over the last few months in relation to this investigation. We appreciate your co-operation in this regard.

Through that proactive engagement we have identified a number of areas where we believe action is required to improve each of the political parties’ compliance with data protection law.

The Commissioner believes that these improvements need to be made by you, and others, in order to further safeguard individuals' privacy, and make sure your data protection frameworks are robust, effective and in full accordance with the law.

In view of the significant risks we have identified, we require you to take immediate action and report on your actions to the information Commissioner by 02 October 2018.

The actions are set out below.

### 1. Obtaining lifestyle information from third party organisations ('data brokers')

Some political parties are obtaining lifestyle-type information on individuals from data broking organisations. The information is used to categorise individuals in a number of areas according to various social and lifestyle factors. This information is then directly linked to individuals forming an attribute on which processing decisions are made.

In our view, once an attribute is linked to an individual it forms personal data. As such, individuals should be provided with fair processing information to demonstrate how their personal data will be processed.

Some political parties do not appear to be providing individuals with adequate fair processing information to make individuals aware of how their personal data is being processed.

Action Required

You must review your current practices and privacy notices to ensure full and transparent information is provided to individuals about your use of their personal data. This should also include the use of data protection impact assessments in accordance with General Data Protection Regulations (GDPR). In particular, you should explain:

- how individuals' information gained from sources (such as the electoral register) is supplemented by other information,
- the source of that information,
- and how it is processed by you.

### 2. Obtaining marketing lists from third party organisations ('data brokers')

Some political parties have purchased marketing lists of personal data from data brokers and used this for election or campaigning messaging.

We have evidence that some data brokers have failed to obtain lawful consent for those political parties to use the personal data they have supplied for election or campaigning messaging. We intend to consider our formal enforcement options in respect of other organisations.

This is because no fair processing information was provided to the individuals whose personal data was obtained by the data broker, which would inform them it would be passed to a political party for a particular purpose. Therefore, individuals were not aware of how their information would be processed.

Action Required

If you obtain personal data from a third party data broker and use it for election or campaigning messaging, you must carry out full due diligence to satisfy yourself the data has been obtained lawfully, and that individuals are aware of how their data will be used and to which organisation(s) it will be passed.

You must provide a fully auditable record of your decisions and the due diligence you have carried out. We do not believe that insertion of simple contractual terms between you and a data broker is sufficient to mitigate the risk.

### 3. Use of Data Analytics Modelling

Some political parties are using third party organisations to carry out data analytics modelling, in order to create predictive scores on the party's behalf. For example, the likelihood to vote in a certain way.

We have concerns that some third party companies carrying out data analytics for modelling purposes, have not obtained the personal information they process in compliance with current data protection law. As such, the personal data should not be used by political parties for modelling purposes.

Action Required

Should you intend on using third party organisations to carry out data analytics for modelling purposes on your behalf, a full review of how the personal data has been obtained, and the lawful basis for obtaining and processing that personal data must be carried out.

You must be able to demonstrate your compliance, and the compliance of any third party organisation you use to process personal data, with the law. You must be able to provide a fully auditable record of how the personal data has been obtained and is being processed.

If you are unable to meet a lawful condition of processing, you should not use personal data for this purpose.

### 4. Estimated ethnicity and age data linked to individuals

Some political parties are using software which assigns a predicted ethnicity and age to individuals. This programming assumption is recorded against the individual on the databases used by the political party.

The information is then used to target individuals for certain political messaging related to assumptions about their assumed ethnicity or age.

Some political parties are of the view that this assumed data – for example, based on assumptions about the heritage of a name and not necessarily factual information about a data subject - is not personal data and, as such, no fair processing information is required to be provided to individuals.

Once assumed data has been linked to an individual, it is likely to amount to personal data, as it is an opinion of ethnicity and age. Therefore, fair processing information should be provided to the individual.

An opinion of an individual's ethnicity is highly likely to be classed as 'special category data' in law and, as such, a lawful basis under Article 6 and a condition for processing under Article 9 of the General Data Protection Regulation must be identified (this was previously classed as 'sensitive personal data' under the Data Protection Act 1998 in which a condition of schedule 2 *and* schedule 3 would have been required). There are additional conditions set out in the Data Protection Act 2018 for this category of personal data, with which you must comply.

In our view, it is a significant risk that assumptions or predictions of a person's ethnicity could be inaccurate and, once directly attributed to an individual, could form inaccurate personal information, which could be a potential breach under Article 5(1)(d) of the General Data Protection Regulation.

Action Required

If you use this method of assigning this type of data to an individual, then you must identify the lawful basis under Article 6 and Article 9 of the General Data Protection Regulation. You must document the lawful basis for processing this type of special category data.

You must demonstrate your compliance in relation to the processing and fully audit your decisions.

If you decide to continue to process data in this manner, you must take action to ensure the accuracy of the data you are attributing to an individual.

### 5. Social Media used for marketing purposes

In order to target particular individuals with advertising on social media websites, some political parties are providing telephone numbers and email addresses of contacts on their databases to social media companies. This enables targeted messages to be sent to those individuals on social media.

We have identified deficiencies in the privacy notices or fair processing information used to inform individuals of this type of processing.

Action Required

If you intend to provide personal data to third party organisations for marketing purposes, you must make sure individuals are provided with adequate fair processing information to inform them their personal data will be processed in this manner. You must also satisfy a legal condition in Article 6 GDPR (or one of the additional conditions in the DPA 2018).

As with our other recommendations, you must fully record any decisions made about the processing, in order to provide an auditable record and demonstrate your compliance with the law.

### 6. Use of third party online campaigning platforms

The investigation found that most parties used these platforms, including Nationbuilder. We are concerned about the functions which allow political parties to match data from their databases with social media data from public profiles. The use of these platforms, including the collection and use of publicly available sources must comply with the requirements of the law. Any use of these platforms should be assessed in a Data Protection Impact Assessment.

### 7. Data Protection Impact Assessment (DPIA)

A DPIA allows organisations to systematically and comprehensively analyse their processing in order to identify and minimise data protection risks.

We believe you should undertake a DPIA in order to consider the broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. This will allow your party to identify and mitigate any risks to your processing activities.

A DPIA does not have to eradicate the risks altogether, but should help to minimise them and assess whether or not any remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk; the advantage is that a comprehensive and effective DPIA will demonstrate your accountability and build trust in your party’s processing of personal data.

Action Required

You will undertake a DPIA on the processing of personal data by your party within three months of the date of this letter, and report the findings to the ICO.

### Guidance from the ICO

We provide detailed, comprehensive guidance aimed at political parties and political campaigns on compliance with data protection and related law.

All of our guidance is published on our website at www.ico.org.uk.

We have established stakeholder engagement contacts, who will continue to provide you with advice and guidance in relation to specific or general issues of compliance.

**Intention to serve Assessment Notice under section 146 of the Data Protection Act**

In view of the concerns we have identified through our investigation, and to provide reassurance to the public about the processing of personal data by political parties, we intend to exercise our powers and issue Assessment Notices over the coming year to each of the main political parties.

The Assessment Notice will provide for a compulsory audit of the processing of personal data. We will decide which parties will be served an assessment notice having considered the evidence from the reports sent to my office, the breadth of data types they use and digital services deployed. All of the main political parties can expect to be served an assessment notice. We intend to take this step following completion of the actions identified above.

We will contact you in due course when we are ready to serve an Assessment Notice on your party.

Yours sincerely

Elizabeth Denham
Information Commissioner

# Annex ii: Other platforms

### Google

Google told us that it does not offer separate services to political parties or campaigns in the UK. Political parties and campaigns have access to all Google products, services and application programming interfaces in the same way as other customers. However, Google told us that the three main UK-wide political parties predominantly used AdWords (used to advertise on Google services and the third-party properties that are part of the Google Display Network) and DoubleClick (Google's fully featured advertising platform that allows customers to create, transact and manage digital advertising) at the 2017 general election.

Google told us that whilst political advertising in itself is permitted, Google has a clear position in the UK that political affiliation (which includes political ideologies and engagement in political discourse) cannot be used by advertisers to target ads or promote products or services. This position is reflected across a number of Google policies.

Google told us that customers can set up advertising campaigns without any input from the Google team, but Google does provide direct support to some customers (proportionate to the level of spend) and this would be available to political parties. This includes support with onboarding, product training and technical support.

Google has two types of user: authenticated users (those signed in with a Google account) and unauthenticated users (those who are not signed in or use Google Services without an account). Ads personalisation is based on user interest categories. These are created by inferring users' interests through visits to websites or viewings on YouTube. The more similar they are in nature, the more reliable the signals that are created. Google then applies these signals to its own interest categories, which might include 'People & Society – Social Sciences – Political Science' but Google says that no category would indicate the political affiliation of the user in the UK. Demographic data is also inferred from sites visited by an unauthenticated user.

Google's general targeting methods are available to all customers, including political parties. These include interest targeting, geographic and language-based targeting, and demographic targeting. The methods can be used simultaneously. An example given by Google was that a political party could decide that its key audience for its ad campaign is females in North London aged 30–35 with an interest in finance.

Google does not offer an opt-out from all advertising and it is therefore not possible to block all political advertising. Users can click on an icon or drop-down menu on ads displayed on Google websites, and block or mute adverts from that particular advertiser or campaign. On third-party websites, users can click on the AdChoices logo and icon. Google also offers an Ads Settings function with an option to disable 'Ads Personalisation' on Google properties and for ads shown by Google on websites and apps of publisher clients. Authenticated users can disable the option, or manage the personalised ads they see by adding and removing topics. A similar option exits for unauthenticated users. Users will still see ads, including, potentially, political advertising, but those ads will be selected based on the content of the specific website, time and location and will not be targeted based on the user's interests. Authenticated users can directly control the data that Google collects and uses through the Ads Settings tool, by either adding demographic and interest information or deleting inferred interests.

### Twitter

Twitter told us that – like individuals or businesses – political parties and campaigns can engage with the Twitter services in a variety of ways, including as a user, developer or advertiser. Many of the features of Twitter, such as viewing individual tweets or Twitter profiles, are available without having to create an account – but other features, including being able to send a tweet, require a user to create an account.

Twitter confirmed that it allows political campaigning but that it requires all political advertisers to comply with any applicable laws regarding disclosure and content requirements, eligibility restrictions and blackout dates for the countries where they advertise. The Twitter Ads Policy also prohibits advertisers from targeting based on sensitive categories of data, including political opinions.

Twitter has developed a handbook for political parties and campaigns for use during elections, which has advice on best practice for using the platform. Beyond this, it provides advice and support to political parties and campaigns on the use of their advertising products in the same way as it would other clients.

Twitter uses information provided to it by users (including when interacting with services) to infer topics and issues an individual might be interested in. Twitter also uses cookies and similar technologies to collect additional website usage data to further personalise the service delivered. Users can view the interests that Twitter has inferred about them in the 'Your Twitter Data' setting. Users can also control how Twitter personalises the ads they receive by using the 'Personalisation and Data' settings. The 'Your Twitter Data' setting provides information to users about the data that Twitter holds, including demographic and interest data, and whether a user has been used in a tailored audience by an advertiser. Viewers can view and modify the data directly.

Twitter has confirmed that users cannot completely disable advertising, but can use the 'Personalisation and Data' setting to adjust the personalised ads setting. Additionally, when a user sees a promoted Tweet in their timeline, they can click on the 'Why am I seeing this ad?' link, which will provide an explanatory message based on information (demographics/interests) about the user. There is also a link to the data dashboard that allows users to edit the types of information that inform what ads and recommended content they see on Twitter.

Twitter said that promoted assets or adverts are clearly labelled as promoted to the user. The user will be able to identify who is promoting the tweet either because the promoter is the author account of the Tweet or because the ad will say (in the case where one account is promoting another's content) 'Promoted by X'.

**Snap**

Snap views itself as being different from other social media platforms as information is shared on a one-to-one basis or in small groups through pictures rather than text.

Snap told us that it had three core ad products: Snap Ads, Filters and Lenses. Snap Ads are full-screen video ads, Filters are location-based filters allowing an advertiser to target audiences in a particular geographic area and Lenses place a themed graphic over the user's picture.

These products are available through Snap's self-service platform introduced in 2017. Any advertiser, including political parties, can create an advertiser account with Snap, and buy and run advertising on Snapchat. We understand that the Conservative Party, the Liberal Democrats and the Labour Party each purchased Snap Ads in the run up to the 2017 General Election. The Labour Party purchased one national Filter.

Snapchat user data is used to identify users who will receive the ads and to place people into particular demographic or interest groups. Snap's Audience Match enables advertisers to reach their own audiences on Snapchat by uploading a list of their own users' identifiers (hashed email addresses or device advertising IDs), which is then matched with Snapchat users' data. If a successful match is made, that user will be shown the advertiser's ad.

If an advertiser wants to target users who are not its usual customers, then Snap will create a Lookalike audience. Data points are used to create a target audience based on demographic data.

Snap told us that they do not analyse private communications within the app to create advertising categories, but a more granular analysis might be done on location data from city to shop or restaurant. If a user has opted into using Snap Map, that is, in turn, used to identify location. The more location points taken, the better the app gets at confirming the right location. Snap confirmed that in relation to advertising by political parties, the most granular it would get was city level.

It is not possible to opt out of advertising on Snapchat entirely, but users can opt out of Audience Match advertising through the 'Advertising Preference Center'. They can further opt out of having their mobile device identifier processed for advertising purposes through their settings on their device. Snap also told us that users can avoid advertisements by swiping past filters, and can tap to bypass individual Snap Ads.

# Annex iii: The Future of Political Campaigning – DEMOS report

You can find the DEMOS report on the ICO's website