ORG OPEN RIGHTS GROUP

WHO DO THEY THINK WE ARE?

POLITICAL PARTIES, POLITICAL PROFILING, AND THE LAW.

CONTENTS

ABOUT ORG

Open Rights Group (ORG) is a UK based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

Our work on data protection and privacy includes challenging the immigration exemption to UK data protection law, defending the General Data Protection Regulation (GDPR) from attempts to water down its provisions, and challenging uncontrolled and unlawful data sharing by online advertisers.

openrightsgroup.org

Written by Pascal Crowe
Data and Democracy Project Officer
Open Rights Group

Matthew Rice
Scotland Director
Open Rights Group

Mariano Delli Santi
Legal and Policy Officer
Open Rights Group

Cover photo by Rob Curran, cc-by-sa licence
Crowd image page 5 by Davide Ragusa, cc-by

Photographs inside cover and page 15 are copyright of the photographers and licensed from Unsplash.

INTRODUCTION

The political use of personal data has been hitting the headlines since the Cambridge Analytica scandal.[1] The focus so far however has been on the actions of social media companies, and activities on social media. The role of political parties, who commission this activity, and process large amounts of personal data themselves, has been ignored.

ORG's Data and Democracy Project spent the past year examining the use of personal data by political parties. We released innovative policy proposals, given evidence to Select Committees, and conducted a ground-breaking digital rights campaign during the 2019 General Election which informs the content of this report.

ORG considers the use of personal data by political parties to be especially concerning. Parties claim to have a lawful basis to conduct activities unacceptable for social media companies. Of particular concern is the "democratic engagement" lawful basis for data processing, which is used by parties to justify a wide range of profiling activities.

In order to establish what the parties are doing, ORG conducted a research campaign to encourage people to make data subject access requests (DSARs) to UK political parties. The right of subject access allows an individual to gain a copy of the data held on them by any organisation. After gaining informed consent, ORG analysed a number of these responses.

Although it is assumed that all political parties conduct some degree of profiling, ORG only received significant results from the Labour Party, the Conservative and Unionist Party, and the Liberal Democrats.

The results were startling and disturbing. In particular, we have found extensive use of personal data to try and guess characteristics such as income, number of children, and nationality. This is then used in an attempt to tailor a political relationship with that person.

We found that Labour was conducting the most sophisticated political profiling in house, followed by the Conservatives and the Liberal Democrats.[2] All political parties attempted to profile both personal information and highly protected special category data such as religion and political opinions. Generally, the accuracy of political profiling was extremely poor, although this should be explored further.

Finally, the political parties demonstrated a confused understanding of data protection law.

> **In particular, the democratic engagement lawful basis was often cited as a catch all justification for processing. In fact, it can only really be used to justify use of the electoral register - not to use or generate information about a person's income, nationality, or political opinions.**

Our results have shown that a legal grey area has opened up in data protection law in the United Kingdom. In that grey area resides a myriad of data practices from purchasing commercial data, processing special category data and the profiling and inferring of political opinions by political parties. This leaves most voters in the dark about what political parties do with their personal data. These practices have the potential to seriously undermine trust in the democratic process and damage its integrity.

[1] https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

[2] Although it is known that they both outsource a significant amount of data processing to third parties.

RECOMMENDATIONS

REGULATE THE SCOPE OF THE 'DEMOCRATIC ENGAGEMENT' LAWFUL BASIS IN THE DATA PROTECTION ACT 2018 AND MAKE ENFORCEMENT COUNT

The Information Commissioner's Office (ICO) needs to guide parties then enforce against the excessive use of this exemption, which clearly limits the use of data to that which is necessary and proportionate.

IMPLEMENT COLLECTIVE REDRESS (80.2 OF GDPR)

This would allow organisations to take forward public interest, strategic digital rights litigation without the need for individual claimants.

POLITICAL PARTIES SHOULD MOVE TO A CONSENT BASED OPT – IN MODEL OF POLITICAL PROFILING

This would allow for digital rights to be respected whilst embracing the benefits of data driven political campaigning.

OUR FINDINGS

This is a summary of the results that ORG received and the subsequent analysis.
The results in full are presented in an academic working paper that ORG can share on request.

LABOUR

None of the data subjects who sent DSARs received a meaningful response within the statutory time limit. Instead, participants received letters asking for additional ID to verify their requests, despite this having been provided in the first instance. This may be in breach of the law.

Some ORG staff however had received a DSAR response prior to this campaign. Labour had compiled up to 100 pages of data per individual, broken down into over 80 categories. The DSAR gave the 'name' of a data point, a 'description' of what it related to, a 'dictionary' of how to interpret the value of each data point (generally given numerically), the source of data, and the legal basis for processing that data.

The following is a non-exhaustive list of what we found:

Data sources

- 'Commercial supplier'.
- 'Electoral register'.
- 'Calculated by the Labour party'.
- 'Calculated from scores using data (including profiled data) freely given by electors about their political opinion, as well as data we lawfully hold on them'.

Scores

Family life

- **'Tenure'**: an estimate of how long someone had lived at their address.
- **'Hh_with_children'**: an estimate of whether a person has children or not.
- **'P_head_of_household'**: an estimate of who the 'head of the household' is.
- **'Weekeve'**: an estimate of how likely you are to answer a knock at the door after 5PM during the week.

Social status

- **'Income_model_hh_band'**: an estimate of how much money an individual makes.

Religious and political views

- **'Remain_score'**: an estimate of how strongly an individual supports staying in the EU.
- **'SNP_ score'**: an estimate of how strongly an individual supports the SNP.
- **'LabTorySwitch'**: an estimate of how likely an individual is to switch between parties.

Ranks
Individuals were ranked within their Westminster constituency on how important they felt certain issues were.

- **'Childcare'**: how important childcare was to an individual, ranked out of other members of their Westminster constituency.
- **'powers_ScotParl'**: how important further devolved powers to the Scottish Parliament was for an individual.

LIBERAL DEMOCRATIC PARTY

ORG analysed 25 DSAR responses from the Liberal Democrats (Lib Dems). They contained mainly descriptive data, mixed with inferential data. It predominantly contained electoral roll data. Many of the DSAR responses were virtually blank. This suggests that although the Lib Dems aspire to sophisticated and comprehensive in-house profiling, they haven't yet achieved it (although this could also reflect sampling issues). The Lib Dems outsource some processing to the company CACI.

We found, for example:

Data sources

- None named in individual DSAR reponses. Individuals were instead referred back to the Liberal Democrats' Privacy Policy.

Scores

Family life

- **'SurnameCount'**: an attempt to guess the number of different families in a home.
- **'Origins Age'**: an attempt to guess an individuals age based on their name.

Religious and political views

- **'Brexit2019'**: likelihood of being a Brexit Party voter in 2019.
- **'Soft tory'**: likelihood of being a soft tory.
- **'Rem2019'**: likelihood that an individual supported staying in the EU as of 2019.

CONSERVATIVE AND UNIONIST PARTY

ORG analysed 17 DSAR responses from the Conservative and Unionist party. The Conservative responses on the whole contained more inferential data, such as demographic information and scores, than the Liberal Democrats. Most of these had been purchased from Experian. In addition, it is known that the Conservatives outsource a lot of profiling to Hanbury Strategy, a political consultancy firm, so this provides only one element of their profiling activity.

The following is a non-exhaustive list of what we found:

Data sources

- 'Modelled data from Experian'
- 'Marked register'

Scores

Family life

- **'HouseHoldWithChildrenV3HouseHold2019'**: an estimate of how many children an individual has.
- **'LengthOfResidencyPerson2019'**: an estimate of how long an individual has lived in their current home for.
- **'AgeFinePerson2019'**: an attempt to guess the ages of individuals living in a home.

Social status

- **'EmploymentStatus2011Person2019'**: an estimate of if an individual is employed or not.
- **'PersonIncomeV3BandPerson2019'**: an estimate of an individual's income.
- **FinishedEducation20OrOverPercentage2019': an estimate of if an individual was university educated or not, as of 2019.**
- **'NewspaperDailyMailPercentage2019'**: an estimate of how likely an individual was to read and enjoy the Daily Mail newspaper, as of 2019.

Religious and political views

- **'Mysticism'**: an attempt to estimate an individual's religion.
- **'Tory'**: an attempt to estimate if an individual is a likely Conservative voter or not.
- **'Mother Tongue'**: seemingly an attempt to record an individual's first language. ORG considers this to be a proxy for nationality.

DOES POLITICAL PROFILING WORK?

The realpolitik justification of the use of personal data by political parties is that it confers an electoral advantage not seen by traditional forms of advertising. Similarly, the political use of personal data has captured the public imagination in a manner unseen almost since the Watergate scandal. At its most hysterical, critics claim that the use of personal data to tailor individual political relationships can result almost in a form of 'mind control' that makes people vote in ways that they otherwise would not. For them the result is at worst, stolen elections, and at best, seriously undermining trust in election results. Without the latter, democracy cannot function.

Yet, a growing body of evidence points to the conclusion that despite the claims of the political data science industry, profiling is not as effective or sophisticated as it appears.[3] That seems to have been the experience of those who received DSAR responses from UK political parties.

ORG has conducted some preliminary research that suggests how inaccurate profiling by UK political parties may be. A number of those who received DSAR responses from political parties were then asked how accurate they felt their DSAR responses were on the whole. 57% agreed most with the statements "The results of my political Subject Access Requests were mostly inaccurate" or "The results of my political Subject Access Requests were completely inaccurate". Only 3% agreed most with the statement "The results of my political Subject Access Requests were completely accurate".

When asked "What was your overall impression of the Subject Access Request responses and how did they make you feel?" participants responded with a mixture of confusion and concern. For example, one participant who received a response from the Conservative Party felt that the "conservative party profile was based on cheap postcode data aggregation. It identified me as a tabloid reading, Labour leaver with poor education, all of which is incorrect." Others were described as "much older than I am" and felt like they were "reading about a strange hybrid caricature with very little resemblance to me" - with the overall picture being "grossly inaccurate". As a result, some commented that "they understood me so little that the likelihood of successful manipulation is slim, to say the least!". This is a revelation: despite all the hype, profiling by political parties is more Mr Bean than Machiavelli. One response seemed to sum up the responses best: "laughable".

These inaccuracies did not diminish the concerns felt by many participants, however as although "many responses were inaccurate … I still felt angry that parties were profiling me and other voters to this extent". One felt "stereo-typed … based on characteristics such as gender, race, age, circumstances and constituency". Another considered the profiling to be "the attempted invasion of my privacy" with one going as far as to say, "I feel spied upon; big brother has arrived". A separate participant stated some political parties had "claimed that information was from a survey I'd filled in; I would never knowingly fill in such a survey from a political party".

[3] See among others https://medium.com/viewpoints/cambridge-analytica-and-the-big-data-panic-5029f12e1bcb and https://www.bbc.co.uk/programmes/b0b6yz9j.

Most significantly, a particular participant was seriously concerned about the economic and material impact of this kind of profiling saying that it was "Inaccurate on some important details that might affect credit and other important things in my life. Made me feel a bit anxious and powerless". While political profiling should not relate to financial background, parties risk creating the impression it does. It seems clear that this activity, however inaccurate, has a human cost.

The root of the inaccuracy problem is one of human dignity. Information held about people needs to be accurate. GDPR and the Data Protection Act 2018 (DPA 2018) for this reason require data to be accurate as a principle of its use.[4] The manner of the profiling done clearly is not accurate and may conflict with the law.

As a potential solution, political parties could explore other less intrusive forms of profiling such as profiling by geographic area. This sort of profiling is well established in several sectors, including banking. Although the benefits are contested and it is not without controversy, this would be much less likely to engage data protection law.

In summary, political profiling may incur a significant financial, resource, and reputational cost, for very little gain. It is unclear what the business case for its continuation is. Political parties should take note and consider carefully whether the benefits outweigh the risks.

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/

CONCLUSIONS

Bigger parties = more sophisticated profiling

The degree of sophistication in profiling roughly correlated with the size of that party's membership. Of Labour, the Liberal Democrats and the Conservatives, Labour had by far the most detailed and granular profiling efforts. The Conservatives and the Liberal Democrats had a reasonably comparable number of data points, but the Conservative responses often had many more inferential data points (demographic information and propensity scores) than the Liberal Democrats.

Labour also had a significant (and seemingly the highest) number of sources of data. Labour listed the electoral register, canvassing, 'commercial' (including at least Experian), and the Labour Party itself. The number of data points that list the Labour Party as the source suggest that they are conducting a significant amount of data processing in house. This is different to other political parties – for example, the Conservatives have outsourced a significant amount of data processing to Hanbury Strategy, a political lobbying firm.

How are inferences generated, and what are they used for?

DSAR responses themselves do not provide us full information about how the scores and conclusions are generated. As a result, firm conclusions are difficult. It seems however that elements such as the person's name as stated on the electoral register, along with other householders perhaps, are important in the process of determining likely age, gender and so on. The results for each individual, while frequently inaccurate, are unique. This is important to understand, as it is clear the profiling is not merely information about an area applied to an individual for convenience.

In addition, although we have broadly assumed that this profiling is used to determine a 'political relationship' with a voter, it is unclear precisely what that means in practice. Does it relate to fundraising, canvassing, communications or policy development? Further research is needed to parse out which data is used for what purpose.

Experian dominated as a source of commercial data

The dominance of Experian as a source of commercial data was notable. It supplies data to both of the UK's biggest political parties. In this case study it had a near monopoly position. In particular, its product 'Mosaic' recurred repeatedly across both parties. Much in the way that Facebook has been described as a "one stop shop" for political propaganda and ads, it seems that Experian is a one stop shop for data used in political profiling.

Is it worth it?

Anecdotally, in this study many people did not recognise the portrait of themselves depicted by the political parties profiling efforts. People felt the information about them was false. This was the case not just for inferential information such as political opinions, but for far more fundamental information such as age, income, and gender.

Data processing by the political parties is often only the first step of a process that has a number of different branches. This includes social media adverts, but also more mundane campaign activity such as door knocking, and what policy issues canvassers should bring up in conversation to drive voters to the polls. It is questionable, however, how effective the later stages of that process can be if they are built on such inaccurate foundations. If political parties want to better understand their voters it seems like ‘low tech solutions’ - such as canvassing and focus groups - may provide more accuracy, and less legal risk, than an over reliance on commercial data brokers.

THE LAW

Summary

To process personal data, a data controller must have a lawful basis for the processing activity. Those lawful bases are set out exhaustively in Article 6 of GDPR.

One lawful basis is the processing of data in the "public interest" in Article 6(1)(e) GDPR. Section 8(e) of the DPA 2018 has augmented the concept of the "public interest" by including "democratic engagement" in its rubric. In turn, personal data can be processed as an activity in the public interest if it is processing that is "necessary for… an activity that supports or promotes democratic engagement". As a result, political parties (and others) can process personal data as a matter in the public interest, providing that it is necessary for an activity that supports or promotes democratic engagement.

In addition to the extended public interest condition, some parties also cited "legitimate interest" as their basis for processing personal data. However, "legitimate interests" under Article 6(1)(f) GDPR requires a balancing test between the rights of the data subject and the interests of the data controller.

In addition to the processing of personal data, political parties inherently process a category of data that requires a higher level of protection. In particular, "special category data", includes data revealing political opinions (among other sensitive matters, such as health and ethnicity). To process such special category data, a controller will need to demonstrate a separate legal basis to process such personal data. The standard is higher than Article 6. Indeed, Article 9 of GDPR prohibits the processing of "special categories" of personal data unless one of ten specified bases apply. This includes a "substantial public interest" provision in Article 9(2)(g).

DPA 2018 again provides an extended interpretation of this "substantial public interest" provision. In particular, paragraph 22 of Schedule 1 of the DPA states that the "substantial public interest" condition in Article 9(2)(g) allows specified individuals and organisations to process personal data revealing political opinions, where such processing is necessary for the purposes of the person's or organisations political activities. Thus, specified organisations and individuals can process such data without the need for a more cooperative legal base, such as consent – in fact they can process data without the knowledge of the individuals concerned. However, this is not unfettered. Rather, DPA 2018 states that such processing must be *necessary*.[5] The ICO has said that the necessity standard in data protection law requires the processing to be "more than just useful or standard practice".

These legal provisions are complex and open to wide margins of interpretation. This lack of certainty as to meaning is further exacerbated by divergent interpretations of the lawful basis of "democratic engagement" and a lack of guidance on what constitutes "necessary" processing for political activities. This has in turn impacted on the practical implementation of such provisions.

[5] Para 22(1)(c) DPA.

Democratic Engagement

UK political parties rely on the "democratic engagement" legal basis for processing personal data, under Section 8(e) DPA 2018 (as augmenting Article 6(1)e GDPR). However, "democratic engagement" has never been sufficiently clear as to allow a clear understanding of what it covers. Our research shows that the lack of clarity has itself led to significant processing of personal data by parties that members of the public have said left them feeling exposed, and stereotyped.

Our concerns are that the lack of clarity or specificity has led to parties over interpreting what the provision allows them to do. The limits to the scope of activities this lawful basis allows is not immediately clear. The Explanatory Notes which accompany DPA 2018 state that the term democratic engagement is intended to cover a wide range of political activities inside and outside election periods, including but not limited to: democratic representation; communicating with electors and interested parties; surveying and opinion gathering; fundraising; among other things.[6]

By contrast the ICO considers democratic engagement to be much narrower. In their submission to the Public Bill Committee when the Data Protection Bill was making its legislative progress, they said that democratic engagement "is likely to be restricted to activities such as those covered by electoral law, for example sending mail outs allowed to each voter".[7] This interpretation from the ICO was also demonstrated in their "draft framework code of practice on the use of personal data in political campaigning", where they acknowledge the scope of the Explanatory Notes but state that this processing should be supported by additional law, such as electoral law.[8]

The difference between these two interpretations is a chasm. The practices we have seen, as set out in the Explanatory Notes, of purchasing commercial data, matching it to voter profiles and using it to communicate with electors and interested parties, are not clearly within the confines of DPA 2018. Such processing could be considered within the outer boundaries of the "public interest" provision, providing such processing is necessary. However, the ICO's interpretation is much narrower and only allows for a very limited set of activities including, mostly revolving around sending mail-outs to individuals as parties are entitled to under electoral law. In between these two interpretations many different practices could - and do - persist. This is a problem, both for the integrity of DPA 2018 and for trust in how political parties handle data.

A key part to this puzzle is the principle of necessity. What activities can political parties undertake in order to meet their aims that are necessary? The ICO has said that the necessity principle requires the activity to be more than just useful or standard practice.[9] Courts have articulated that the test of necessity is a strict one and that the requirement that data processing is necessary requires the data controller to consider whether, inter alia, a less intrusive measure is available.[10]

[6] Data Protection Act 2018, Explanatory Notes, section 8: Lawfulness of processing: public interest etc., para 86, http://www.legislation.gov.uk/ukpga/2018/12/notes/division/6/index.htm.

[7] Information Commissioner's Office, Data Protection Bill, House of Commons Public Bill Committee - Information Commissioner's further written evidence, https://ico.org.uk/media/about-the-ico/documents/2258462/data-protection-bill-public-bill-committee-ico-further-evidence.pdf

[8] Information Commissioner's Office, *Guidance on political campaigning*, Draft framework code for consultation, p37, https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf .

[9] *Ibid* p38.

[10] See *Guriev v. Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB).

Recently, the Conservatives elaborated on their interpretation of necessary democratic engagement, where an MP sends a birthday card to a constituent at the point at which they reach 18 and are entered onto the electoral register.[11]

There is a dire need to bring the principle of necessity into a practical understanding and provide a suitable ring-fence around which political parties can process personal data. At this stage, we do not see in practice suitable limits to the scope of democratic engagement. We would encourage greater transparency and scrutiny over what the parties consider to be permissible and impermissible under these provisions.

Consent and Legitimate Interest

Other legal bases have been relied upon the parties in their responses to the requests: notably "legitimate interest" and "consent".

Political parties may rely on consent to process certain types of data, particularly in relation to communicating with their membership. Consent would require the parties to be clear and open, in order to provide individuals with the opportunity to provide "freely given, specific, informed and unambiguous indication of [their] wishes".[12]

Legitimate interest seems to be relied upon more often to process a broad range of personal data, including political opinions and personal information purchased from commercial data brokers.[13] However, Article 6(1)(f) GDPR requires a balancing assessment between the interest of political parties conducting profiling and the rights and freedoms of the individuals being profiled, yet most political parties have not provided an explanation as to how they have conducted that balancing test.[14] That balancing test once again engages the principle of necessity and whether the profiling activities undertaken individuals are unlikely to be aware or to expect these kinds of profiling activities to take place, as we lack evidence that political parties are informing individuals at the time of collection of their personal data or in the course of electoral activities (such as during canvassing or in marketing communications), in line with Article 13 and Article 14 of GDPR. In this, profiling does not seem to be proportionate, accurate, nor transparent, all fundamental elements in determining whether legitimate interest overrides one's own rights and freedoms.

Special Category Data

Our research has shown that profiling has taken place that reveals special category data not related to political opinions, such as estimates of one's religious beliefs by the Conservatives. In order to profile information other than political opinions another legal basis is required. It is not clear from this research on which basis the Conservatives relied.

It is also important to recognise that fundamental rights of the data subject persist under this basis. In particular, paragraph 22 of Schedule 1 is not absolute but rather provides an opt out. Individuals can give "notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject". This is an important statement of personal data rights. We would encourage UK political parties to provide clear and easy access to such opt-outs, such as a clear tool on party websites.

[11] Democracy and Digital Technologies Committee, submission by Conservative and Unionist Party, https://committees.parliament.uk/writtenevidence/6338/html/.

[12] Per Article 4(11) GDPR.

[13] https://www.conservatives.com/privacy, https://www.libdems.org.uk/table-of-legal-basis.

[14] Notably, the Labour Party states in its privacy policy that "the Labour Party will maintain a Legitimate Interests Assessment Register, in which the Labour Party will formally record the results of the balancing assessments for each processing activity or data set where legitimate interest is the processing condition."

POLICY RECOMMENDATIONS IN FULL

Regulate the scope of the 'democratic engagement' lawful basis in DPA 2018 and make enforcement count

Regulators should continue to investigate whether the data processing activities of political parties are strictly necessary for activities that support or promote democratic engagement, or merely a no holds barred attempt to grab any data that might confer some sort of electoral advantage. A clearer outline of what this constitutes would make the use of this lawful basis more accountable. The ICO has helped clarify this somewhat in its recent guidance, and ORG supports the incorporation of this guidance into law. The ICO must enforce against parties where their guidance is clearly contravened.

If the use of the democratic engagement lawful basis was appropriately tightened, it is likely that parties would have to rely on the legitimate interest lawful basis, which requires at its heart an assessment of whether an organisation's legitimate interests outweigh an individual's rights. ORG is of the opinion that many profiling activities of the political parties would not pass such a test as they fundamentally conflict with principles of data protection law.

Implement collective redress (Article 80.2 of GDPR)

ORG supports measures incorporating GDPR Article 80(2) into domestic law.

Article 80(2) of GDPR enfranchised member states to authorise a body, organisation or association to lodge a complaint with the relevant supervisory authority (in this case the ICO) 'if it considers that the rights of a data subject under this regulation have been infringed as a result of the processing'. However, the UK did not take up the option to provide for this power in DPA 2018. Instead the Secretary of State must review the issue 30 months after Section 187 comes into effect. This review is due by the end of 2020.

Although civil society organisations can currently take instruction from claimants to coordinate a collective complaint, they cannot take the initiative on a data protection case themselves, even when there is a clear public interest basis. It is unrealistic to expect members of the public to be fully aware of when their data rights are being infringed, and it is often in commercial and political interests to prevent them from being thus aware. Not enacting GDPR Article 80(2) will prevent many key rights issues from being scrutinised.

Introducing this part of the law would make political parties such as Labour, who have not complied with their legal obligations, easier to hold to account.

Political parties should move to a consent based opt - in model of political profiling

There are additional legal bases that political parties can rely upon to process personal data. For example, they can rely upon legitimate interest broadly, and DPA 2018 Schedule 1 paragraph 22 to process political opinion data. However, these legal bases are likely to be tightened over time and incur a high compliance burden. For example, the ICO has said in recent guidance on the lawful basis for processing political opinion data that "if you can achieve the same political campaigning purpose without processing data relating (to) people's political opinion data, then you cannot rely on this condition".[15] This must also be weighed against the likelihood of causing substantial damage or distress, which would be open to possible legal challenge.

In addition, our research has highlighted an unspoken truth of political profiling in its current form - **it does not work**. Most participants in our survey did not recognise the profile constructed of them.

To ORG, the best value for money, most effective, and digital rights friendly form of profiling would be an opt in system of profiling based around consent. This could revolve largely around keeping up with existing members, interested individuals, and fundraising. This would be more accurate and useful for parties and their supporters, and more in line with people's expectations. A recent survey by ORG has suggested that this could be a popular option.[16]

[15] https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf p45.

[16] https://www.openrightsgroup.org/blog/political-parties-listen-to-your-membership-on-data-rights/.

ORG OPEN RIGHTS GROUP