Response to the Consultation of the House of Lords' Democracy and Digital Technologies Committee

14th October 2019

Contents

0. SUMMARY

Online Campaigning

We are concerned that current online campaigning practices can be used to obscure both how and by whom regulated resources including money and personal data are used. As a result, electoral regulation (i.e. campaign finance regulation) is increasingly unfit for purpose. A range of policy options are available to the Electoral Commission and Information Commissioner's Office (ICO) to reform this. In particular, we suggest a 'joint data audit' taskforce that uses expertise from both the Electoral Commission and the ICO to conduct financial, ethical and legal assessments of a campaign's data assets before commencement of the regulated period.

Moderating Social Media and Misinformation

Whilst recognising that misinformation exists online, we are cautious about attempts to limit or censor content that individuals can access. For example, research suggests that much of what has been labelled "fake news" is often highly partisan rather than factually incorrect. In addition the debate around misinformation has itself become politicised. To an extent, terms such as "fake news" are increasingly used to refer to information that one does not agree with rather than information that is factually incorrect.

We also recognise that the problematic culture of abuse online can have a hugely negative impact on individuals and groups, especially those in particular positions of vulnerability. Nevertheless, regulation of online content always ultimately ends up being regulation of platform users and so should proceed cautiously in order not to undermine the protection of fundamental rights.

Regulation of content is inextricably woven with the data and advertising based business model of platforms which pushes extreme and polarising content as a fundamental part of maximising engagement, growth and revenue; this inherently makes solution-finding challenging. Difficult questions also arise over the extent to which governments or private companies can or should be defining and enforcing the limits of free speech. Over-forceful regulation could further have an unintended consequence of pushing companies towards increasing monitoring or take-down, in violation of international laws and standards. We refer particularly to our body of work on the Online Harms White Paper in this regard.

Technology and Democratic Engagement

We encourage the responsible use of technology in efforts to improve democratic engagement. However, we are sceptical about the ability of technologies such as e-voting and e-counting to assist in ballot casting and counting, and are concerned about

the impact on fairness, accuracy and accountability in awarding contracts to companies with dubious reputations and poor track records.

1. INTRODUCTION

1.1 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.

1.2 This submission draws predominantly from our "Data and Democracy" project work which is exploring the nexus of democracy, technology, digital and electronic systems and big data techniques. This work is funded by the Joseph Rowntree Reform Trust. We are aiming to establish consensus around the acceptable use of personal data by political parties and in political contexts, and are in the process of developing a series of principles which can underpin and, we hope, secure political commitment to the ethical use of personal data and associated technologies.

1.3 ORG recently gave oral evidence to the All Party Parliamentary Group on Election Campaigning Transparency and our submission below develops the information and perspectives given there.[1] In addition, our main public reports underpinning this response are: Internet Regulation, Parts I[2] and II,[3] Blocked: Collateral Damage in the War against Online Harms,[4] and Response to Consultation on the Online Harms White Paper.[5]

2. ONLINE CAMPAIGNING

<u>The effect of online targeted advertising on political processes</u>

2.1 It is important to note that the effectiveness of targeted political advertising (and targeted advertising generally) to persuade is disputed. The UK has also

[1] Evidence given by Pascal Crowe, Data and Democracy Project Officer, 23 July 2019, summary available at: <https://fairvote.uk/appg-6th-session-illuminates-anti-democratic-aspects-of-digital-campaigning/>.
[2] Open Rights Group, *UK Internet Regulation Part 1*, December 2018. <https://www.openrightsgroup.org/assets/files/pdfs/reports/Internet_Regulation_Part_I_Internet_Censorship_in_the_UK_today-web.pdf>
[3] Open Rights Group, *UK Internet Regulation Part 2*, June 2019. <https://www.openrightsgroup.org/assets/files/pdfs/reports/ORG_Regulation_Report_II.pdf>
[4] Open Rights Group, *Collateral Damage in the War against Online Harms*, April 2019. <https://www.openrightsgroup.org/assets/files/reports/report_pdfs/top10vpn-and-org-report-collateral-damage-in-the-war-against-online-harms.pdf>
[5] Open Rights Group, *Response to Consultation on the Online Harms White Paper,* July 2019. <https://www.openrightsgroup.org/about/reports/response-to-consultation-on-the-online-harms-white-paper-july-2019>

historically enjoyed a well regulated political campaigning market. Nevertheless, there now is a general sense that online political campaigning has shifted the power dynamics between citizens and political organisations in favour of the latter.

2.3 The shift has occurred largely due to two digital factors. First, the relative anonymity provided by the Internet has facilitated the proliferation of 'astroturf' campaigns: these claim grassroots status but are coordinated (and funded) by larger established commercial lobbying organisations or pre-existing political campaigns.[6] It is relatively easy under present circumstances for political campaigners to obscure the sources of their funding.[7] Secondly, political campaigners are able to exploit the data economy and use commercial data sets and scraped data to deliver highly targeted political messages to individual voters. In short, the targeting functionality provided by social media platforms such as Facebook means that "the same model that sells us shoes and cars is used to pitch political ideas and slogans."[8]

2.4 These digital campaign systems and techniques are fundamentally predicated on information asymmetry between campaigners and citizens: campaigners know everything because of the vast quantities of data which they hold; citizens know only the slice of the picture that the campaigns choose to show them, and can be kept in complete ignorance of how differently the campaign is presenting itself to others.

2.5 The effect of this is to inhibit the abilities of citizens to assess political claims and hold those making them to account. It has also previously encouraged alleged breaches of campaign finance regulation.[9] In a data protection context, it encourages unethical, and perhaps unlawful, data processing practices.[10] All of these, taken together, undermine fair and open democracy.

---

[6] For example, see the Guardian, *Facebook Brexit ads secretly run by staff of Lynton Crosby firm*, 3 April 2019. <https://www.theguardian.com/politics/2019/apr/03/grassroots-facebook-brexit-ads-secretly-run-by-staff-of-lynton-crosby-firm>

[7] See Appendix Ai.

[8] Analogy used by Information Commissioner Elizabeth Denham in evidence given to Parliament Fake News enquiry. Reported in The Telegraph, *Facebook should disclose how political parties target people online, ICO says*, 6 November 2018. <https://www.telegraph.co.uk/technology/2018/11/06/facebook-should-disclose-political-parties-target-people-online/>

[9] See BBC, *Brexit: Vote Leave broke electoral law, says Electoral Commission*, 17 July 2018. <https://www.bbc.co.uk/news/uk-politics-44856992>

[10] ORG has been investigating this through the use of Data Subject Access Requests. See Appendix B ii for initial results.

The need for more nuanced campaign spending regulations in the digital era

2.5 Excepting legislation such as the Communications Act 2003, UK political campaigning regulation has focused on regulating the spending involved in campaigning rather than its content. Online campaigning however has obfuscated many of the distinctions in spending set out in law and regulation, which make current regulation inadequate to properly address the issues at hand. ORG's research has identified three specific issues:

2.5.1 *The regulated period*

(i) The lack of shelf life on social media posts frustrates the intent of the regulated period. Political content can be generated long before the regulated period and linger online. Content created before an election can easily be "re-upped" to give it a second life during an election (unless taken down for breaching community guidelines or similar). Despite campaigning activities that are paid for outside of the regulated period but used inside the regulated period being regulated, in a networked communication environment it is incredibly difficult to determine whether "shares" are organic or part of a wider effort by actors seeking to "game" regulation.[11]

(ii) Similarly, third-party campaign groups and parties can appear and disappear outside the confines of regulated periods. The online environment empowers people to participate in political activity and there are very low barriers to entry. Whilst this can be positive in principle, a lot of conceptual effort also goes into gaming this opportunity through tactics such as encouraging organic sharing of pre-created content or artificially amplifying citizen support through systems such as botnets. What is good for individual freedom of expression is bad for the concept of a regulated period.

2.5.2 *Lines between candidate and party spending are blurred or non-existent*

(i) Social media platforms can target precisely and widely, which blurs the line between differentiated spending limits traditionally placed on actors by designations (e.g. candidate/party/national/local) to the point where these are essentially cosmetic.

[11] See Appendix Bi.

2.5.3 *Data-driven and digital campaigning is all about making spending more efficient*

(i) The 1998 recommendations of the Fifth Report of the Committee on Standards in Public Life,[12] which led to the establishment of the Electoral Commission and the spending regulations which exist today, stem from an era where mass media advertising was the dominant model for political campaigning. That era is gone, replaced by one of mass data collection and processing and precision targeting of voters through online platforms, all of which makes spending more efficient and effective by reducing costs.

(ii) It was assumed in 1998 that the amount spent on political advertising had a strong proportional relationship to the number of people that saw it. The Committee on Standards in Public Life report highlighted examples of model political advertising strategies and their costs including a national newspaper insert page costing £20k-£50k[13] and a two-week nation-wide poster campaign costing upwards of £1 million.[14] These approaches aimed to make sure that a party's message reached as many voters as possible, in the hope that by doing so the message would also reach as many persuadable voters as possible. Regulation spending limits correspondingly priced in that campaigns needed to pay for people unlikely to be persuaded or communicated with in a meaningful capacity.

(iii) By contrast, digital systems enable campaigners to drastically reduce engagement (and associated costs) with those considered unlikely to vote for them. Factors such as "shareability" and "virality" reduce the marginal cost of distribution for digital campaign materials. Technological innovations such as automated content generation, A/B testing and botnets all have the potential to drive down costs.[15]

2.6 These changes all mean that a new, more nuanced approach to spending is needed to capture the modern, digital ways in which money is used to win votes.

2.6 In ORG's assessment, transparency is key to effective regulation in a digital campaigning era. This transparency has two essential components: financial and data. The following sections set out our proposals as to what form transparency

[12] Fifth Report of the Committee on Standards in Public Life, T*he Funding of Political Parties in the United Kingdom*, October 1998, CM 4057-I .
<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/336870/5thInquiry_FullReport.pdf>
[13] Ibid, page 173.
[14] Ibid.
[15] See Appendix Bii.

of these could take (please note, these remain presently under development and are therefore shared as a working proposal):

2.6.1 *Financial transparency*

(i) The Electoral Commission should not play a part in deciding what is/is not a political advert. Online platforms should be required to open up the ways in which they define/determine these boundaries to public and regulatory scrutiny.

(ii) Any political or issue advert must be registered with the Electoral Commission, which should maintain a public record of these connected to contact details for advert sponsors. Companies House registration could be used as a model for this; however, to be effective this equivalent process needs to be cheaper and faster. The Electoral Commission database needs to be user-friendly: clear, accessible, easy to use (including search) and widely available.

(iii) Digital watermarks ("disclaimers") on adverts must include core elements of this information (advert sponsor name at the minimum) and an easily identifiable click-through to the full Electoral Commission database. Elements of this could be augmented /rescinded in the case of political dissidents.[16]

(iv) Any "Ad Library" maintained by an online platform must be reviewed by the Electoral Commission and relevant platform at regular intervals in order to ensure regulatory compliance.[17]

(v) Each political actor (including all third parties) registered with the Electoral Commission must have a designated website and/or page on each social media platform that they operate on containing their contact details and link to associated records held by the Electoral Commission. This site/page must be clear, accessible and labelled so as to be easy for citizens to locate.

(vi) Each campaign must list its campaigning partners on the above-required site/page and on all public communications, both print and digital. Non-party campaigners must list lead and/or minor campaigners. These lists must be

[16] For example, Facebook recently announced new, higher transparency standards for political adverts on its platform in the upcoming 2020 US Presidential election. Political advertisers in most cases must now provide identifying information such as tax returns. However, there is a lower standard of transparency required for 'grassroots' campaigners, that allows campaigners to claim "registered organisation" status in disclaimers. This mean astroturf groups may be able to de facto game the new terms and conditions. See <https://newsroom.fb.com/news/2019/08/updates-to-ads-about-social-issues-elections-or-politics-in-the-us/>

[17] This could be resolved without legislation, though guidance issued by the Electoral Commission.

updated regularly and reviewed against a set of criteria developed by the Election Commission.

(vii) Failure by platforms or campaigners to comply with these requirements should be sanctioned by the Electoral Commission or other appropriate regulator.[18]

2.6.2 *Data transparency*

(i) There needs to be information parity between advertiser and citizen for political purposes. For example, voters should be able to see exactly what data sources, demographics, scores and values advertisers see in terms of their targeting in an easily accessible and understandable format.

(ii) The Electoral Commission and the ICO should conduct joint data audits , prior to regulated periods, of actors captured under electoral regulations and law. Broadly, such audits should include a financial assessment of all data assets that are to be used in a campaign (so that the cost in relation to spending limits is known) and an ethical and legal assessment of the purpose, use and processing of data and associated technologies during campaigns.

2.7 Consensus on the need for change in this area exists across a wide variety of stakeholders. ORG recently convened a roundtable on the ICO's draft framework code of practice for the use of personal data in political campaigning. Following this participants published a joint signed letter highlighting, amongst other matters, the need for greater coordination between the Electoral Commission and the ICO. [19]

3. MISINFORMATION, POLARISATION AND MODERATING SOCIAL MEDIA

3.1 ORG is concerned that the rush to regulate digitised democracy may lead to overreach by both private companies and governments that could have a negative impact on fundamental human rights. Within the scope of this consultation, two concerns stand out. First, whilst factually incorrect news on the Internet clearly does exist, society should be extremely cautious about efforts to regulate political speech and determine what is appropriate speech or not. We note the high protection afforded to political speech under international free

[18] In-depth discussion of appropriate sanctions is outside the scope of the present consultation but we are able to provide more on this on request.

[19] Open Rights Group, *Civil Society organisations raise concerns over rules designed to prevent a new Cambridge Analytica*, 2019. <https://www.openrightsgroup.org/press/releases/2019/civil-society-organisations-raise-concerns-over-rules-designed-to-prevent-a-new-cambridge-analytica> Full meeting notes are available.

speech laws. Second, regulating the online sphere to minimise abusive behaviour is a challenging enterprise, needing careful thought, discussion around viable technological solutions and safeguards to ensure that individual rights to freedom of expression and privacy are upheld.

3.2 In terms of misinformation, research has suggested that rather than poor quality journalism, often it is high quality partisan journalism that dominates online news diets.[20] An emphasis on fact-checking will not be effective in the face of such emotional manipulation. Similarly, there are suggestions that, even in the face of anodyne statistical information, pre-existing opinions and biases can affect interpretation and framing - particularly in the case of polarising issues such as climate change.[21] Rapid adoption of the term "fake news" has turned it almost into shorthand for 'information that one agrees with or not'.[22] ORG feels that this speaks more to a cynicism within our current politics than a radical shift in the quality of available journalism.

3.3 With this being said, ORG also recognises that attempted manipulations of national politics by rogue state actors does occur. For example, it is now taken as fact that the Russian government attempted to manipulate the 2016 US Presidential election.[23] Some of these techniques have become widely known and understood; for example the use of botnets to crowd out messaging and manufacture false support on social media; 'click-farms' which generate false engagement with content; troll factories which intimidate political rivals have all been documented and discussed in relevant academic literature.[24] In addition, the challenges of new technologies, such as deepfake videos, highlight the difficulties in discerning between creative satirical enterprise and deliberate propaganda.

3.3 Governments and regulators worldwide are wrestling with how to address issues of hate speech, abusive behaviour and other harms online. This is a particularly challenging enterprise because the advertising-based business model of

[20] Demos, *Warring Songs: Information Operations in the Digital Ages*, May 2019. <https://demos.co.uk/wp-content/uploads/2019/05/Warring-Songs-final-1.pdf>

[21] Consider e.g. the work of the Cultural Cognition Project at Yale Law School. <http://www.culturalcognition.net/>

[22] Consider e.g. Vox, *President Donald Trump finally admits that "fake news" just means news he doesn't like*, 9 May 2018. <https://www.vox.com/policy-and-politics/2018/5/9/17335306/trump-tweet-twitter-latest-fake-news-credentials>

[23] See e.g. BBC News, *US extracted high-level spy from inside Russia in 2017, reports say*, 10 September 2019. <https://www.bbc.co.uk/news/world-us-canada-49645628>

[24] See e.g. Bradshaw & Howard, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Working Paper 2019.3. Oxford, UK: Project on Computational Propaganda. Available at: <https://comprop.oii.ox.ac.uk/research/cybertroops2019/>

platforms is predicated on promoting explosive and divisive content. It is impossible to divorce consideration of negative online content and behaviour from the underlying revenue dynamics which feed on this. In short, platforms know that fear and outrage generate increased engagement and time on site; this in turn increases advertising engagement and revenue which make it profitable, if not pleasant. A tension at the heart of reform or regulation therefore, is that despite generally wanting to create environments which are positive for users in order to encourage use, platforms also have a vested interest in promoting negative content to provoke base human reactions.[25]

3.5 This said, most social media platforms already have community standards that set a lower threshold for unacceptable speech and behaviour than the law. For example, most platforms include bullying as a prohibited activity but not all types of bullying activity, content or behaviour are banned under the law. In ORG's view, regulation including mandatory transparency reporting and powers of audit could assist to improve enforcement of terms and conditions.[26]

3.6 Platforms also do already have some incentives to attempt to balance free speech rights against questions around behavioural norms; in particular, there are reputational risks to overreaction in various directions, both in over-censoring and in permitting unpleasant material and activity to persist. Lines between open discussion, community support and promotion of harmful behaviour can further be hard to define.

3.7 The many kinds of unwanted content that platforms may be pushed towards banning in a 'pro-democracy' regulation also often reflect parts of human nature that are very hard to ban or regulate. Activities such as doxing[27] and dogpiling[28] can be used as negative political tactics to silence individuals or deter public engagement but are often not caught by terms and conditions and relate more to considerations of morality or civility, better addressed by education and societal initiatives.

3.8 We note that offensive speech not reaching the bounds of illegal hate and content aggregation in a way that is not feasibly possible in the offline world can cause emotional distress and a toxic online environment for certain categories of platform user. Hower, this content may be protected by free speech rights. Hate

[25] A wide range of material is available on this subject. For an accessible overview in relation to Facebook, YouTube and Twitter, see Roger McNamee's *Zucked* (2019).
[26] See our response to the Online Harms White Paper for further detail on this.
[27] Identifying or 'outing' people's real identity on the internet, without their consent and typically with a malicious intent.
[28] Intimidation through "shouting down' a user on a comment thread with intent is to force a user to remove or rescind a comment.

speech is a controversial concept and remains without clear legal definition in international law. Thresholds of harassment may not be met if discrete postings are all legal and originate independently from multiple users. Platforms should have robust terms and conditions which make clear that hate speech and harassment violates their community standards. However, these also need to be clear on what does or does not constitute hate speech/harassment. This is necessarily a difficult balance to strike.

4. TECHNOLOGY AND DEMOCRATIC ENGAGEMENT

4.1 ORG supports efforts to enhance democratic engagement and the responsible use of technology to do so. Any attempt to do this, however, must be accompanied by appropriate tests, safeguards and contingency plans. As noted below, attempts to integrate technology into the democratic process have more often been failures than successes.

4.2 Election integrity is our primary concern here. No computer system is or can be entirely secure. Consequently, digitising elements of the electoral system opens it up to a new and specific set of threats. In addition, there are more mundane criticisms to using technology to enhance democracy, such as; errors in code, faulty hardware, cost and the privatisation of the democratic process, and a generally deterministic drift to "digital by default". Such a course of action can have a significant and detrimental effect on individual rights.[29]

4.3 In the UK, two digitisations of the voting process have been either proposed or adopted: "e-voting" and "e-counting". The former refers to broadly to ballots cast via computer (although it varies between e-voting machines, voting from a personal computer or voting via phone). E-counting refers to ballots being tallied by an electronic counting machine. ORG's investigations into these technologies have given rise to concerns about the potential negative implications for democracy in the way these are being deployed.

4.2.1 *E-voting*

(i) E-voting has been cited as a panacea for declining political engagement and falling voting rates.[30] However its use has also been fraught with controversy. Several countries, including the Netherlands, stopped using e-voting years ago,

[29] The Guardian, *How Britain's welfare state has been taken over by shadowy tech consultants*, 27 June 2019. <https://www.theguardian.com/commentisfree/2019/jun/27/britain-welfare-state-shadowy-tech-consultants-universal-credit>

[30] Chatham House Commission on Democracy and Technology, *Online Voting: Fantasy or Future?*, 24 October 2018. <https://demtech.chathamhouse.org/online-voting-fantasy-or-future/>

citing security concerns.[31] Others have found instances of individual votes compromised and election results called into question.[32] By contrast, countries such as Norway that have considered introducing e-voting have curtailed trials after finding that it did not increase turnout amongst under-represented or marginalised groups.[33] It has been suggested that e-voting is becoming the preferred delivery system for some authoritarian governments, as it adds a veneer of respectability and modernity to decrepit and/or corrupt electoral architecture.[34]

(ii) Fundamentally, these outcomes show that using black box technologies of increasing complexity is antithetical to ensuring public confidence in the outcome of an election.

(iii) ORG has a long history of holding e-voting trials in the UK to account.[35] Most recently, we had planned to scrutinise trials of e-voting proposed by the Scottish Government and Welsh Assembly. However, after public consultation, it was decided that there was not sufficient public appetite for such a move in addition to concern over election security. The Scottish Government consultation in particular found little appetite for a wholesale replacement of manual voting with e-voting, although there was some support for it as an assistive technology for people with disabilities.[36] As a result, further trials of e-voting have been significantly postponed and to ORG's knowledge there are no planned or upcoming trials of e-voting in statutory elections within the UK. ORG considers this to be a thoughtful, positive and proportionate policy decision.

(iv) A further issue with e-voting is the privatisation of democracy that this necessarily entails. The market for digital election services is exceptionally small.

---

[31] European Digital Rights Initiative, *Electronic Voting Machines Eliminated in the Netherlands*, 24 October 2017.
<https://edri.org/edrigramnumber5-20e-voting-machines-netherlands/>

[32] The Atlantic, *Computer Scientists Make the Case Against an Expensive New Voting System*, 13 July 2019.
<https://www.theatlantic.com/technology/archive/2019/07/computer-scientists-worry-over-election-security-georgia/593497/>

[33] Norwegian Ministry of Local Government and Regional Development, *Evaluation of the E-Voting Trial in 2011*, 2 February 2012.
<https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-vote-trial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/id684642/>

[34] Al Jazeera, *DRC's new electronic machines 'could help rig election*, 18 December 2018.
<https://www.aljazeera.com/news/2018/12/drcs-electronic-machines-could-rig-election-181218165614242.html> See also Financial Times, *Martin Fayulu has reason to thank Congo voting machines he once feared*, 15 January 2019.
<https://www.ft.com/content/78bf0af4-18e8-11e9-9e64-d150b3105d2>

[35] Open Rights Group, *Successes*, *e-Voting*, Undated.
<https://www.openrightsgroup.org/about/successes/evoting>

[36] Scottish Government, *Election Reform: Consultation Analysis*, 2018.
<https://www.gov.scot/publications/electoral-reform-consultation-analysis/pages/8/>

There are a very small number of firms that offer e-democracy services[37] and some of these straddle a number of different products. For example, Smartmatic, a company originally incorporated in Venezuela, offers "election technologies" that range from e-voting to e-counting.[38] This small market means that not only is failure often rewarded (as contracts are often extended or renewed after poor delivery), but also that firms exhibit cartel-like behaviour: those responsible for contracting companies for the GLA elections have admitted this on record.[39]

4.2.2 *E-counting*

(i) As part of our work examining how digital technologies are changing democracy, ORG has recently begun investigating the use of e-counting in the UK. E-counting is used to count ballots in several UK statutory elections, including in the Greater London Authority (GLA) Elections. However its use here has been criticised in successive reports by the Electoral Commission.[40] In particular, in the 2016 GLA elections, votes were improperly counted, leading to delays in announcing results and undermining public confidence in the outcome. The Electoral Commission has repeatedly asked the Greater London Returning Officer (GLRO) to conduct a cost-benefit analysis of e-counting, including a costing of manual counting. The GLRO failed to respond to this request until late 2019 after a change of staff and significant pressure from the GLA Oversight Committee.

(ii) The 2018 procurement cost for the 2020 GLA elections' e-counting contract, however, more than doubled since the last procurement process which took place in 2010 - rising to £8.9 million from £4.1 million.[41] ORG has scrutinised this procurement process as far as possible with publicly available documents and has lobbied for questions to be asked of the GLRO at the GLA Oversight Committee meeting. ORG is concerned that the cost of this contract is far too

---

[37] See The Guardian, *'They think they are above the law': the firms that own America's voting system*, 22 April 2019.
<https://www.theguardian.com/us-news/2019/apr/22/us-voting-machine-private-companies-voter-registration>

[38] Smartmatic company website available at <https://www.smartmatic.com/about/>

[39] GLA Oversight Committee, *Meeting record*, 16 July 2019.
.<https://www.london.gov.uk/gla-oversight-committee-2019-07-16>

[40] Electoral Commission, T*he May 2016 Mayor of London and London Assembly elections: report on the administration of the Greater London Authority elections held on 5 May 2016*, 2016.
<https://www.electoralcommission.org.uk/sites/default/files/pdf_file/2016-London-election-report.pdf>
See also the previous report, *Greater London Authority elections 2012: report on the administration of the elections held on 3 May 2012*, July 2012.
<https://www.electoralcommission.org.uk/sites/default/files/pdf_file/2012-GLA-election-report-web.pdf>

[41] Greater London Authority, *Contract for electronic counting system and related services-2020 Mayor of London & London Assembly Elections*, Signed 14 November 2018.
<https://www.london.gov.uk/sites/default/files/glro20-05_signed.pdf>

high as a result of poor products and an uncompetitive market. This is a cost we do not need for a product that does not work.

(iii) The e-counting contract for the 2020 GLA elections is also split between two companies: CGI and Smartmatic. As noted above, the latter company has a poor track record of delivery and its technology and the elections it has facilitated have been criticised, notably those in the Philippines[42] and Flanders (Belgium).[43] The US government launched an investigation into Smartmatic in due to alleged links to Chavez-era officials; this ceased when Smartmatic divested itself of its American interests and ceased to operate there, leaving the UK without the benefit of transparency and accountability.[44] Robert Downes, political counsel to the US Embassy in Caracas said that "Smartmatic is a riddle...The identity of Smartmatic's true owners remains a mystery. Our best guess is that there are
probably several well-known Venezuelan businessmen backing the company who prefer anonymity either because of their political affiliation or, perhaps, because they manage the interests of senior Venezuelan government officials." [45]

(iv) The GLRO in both in the GLA oversight Committee and in its progress report to the Committee cited previous e-counting operations by Smartmatic in Scotland as evidence of its suitability for the contract.[46] Investigation by ORG showed this to be false: Smartmatic has never been awarded an e-counting contract for Scotland.[47] As a result of our drawing this to their attention, the GLRO retracted this specific endorsement.[48] Subsequently, the GLO has relied on Smartmatic having a staff member who has previously worked on delivering UK elections to assert that they are competent.[49] However, ORG does not consider this a sustainable position: from our understanding not only does Smartmatic not employ any staff member who could reasonably be said to have an in-depth technical experience of the risks involved in delivering electronically administered elections in the UK (from our understanding the staff member cited

[42] Philippines News Agency, *Smartmatic VCMs accuracy questioned*, 20 July 2019. <https://www.pna.gov.ph/articles/1075540>
[43] PC World, *Software bug disrupts e-vote count in Belgian election*, 26 May 2014. https://www.pcworld.com/article/2159260/software-bug-disrupts-evote-count-in-belgian-election.html.
[44] New York Times, *U.S. Investigates Voting Machines' Venezuela Ties*, 29 October 2006. <https://www.nytimes.com/2006/10/29/washington/29ballot.html>
[45] Robert Downes, Wikileaks, *Caracas' view of Smartmatic and its voting machines*, 2006. <https://wikileaks.org/plusd/cables/06CARACAS2063_a.html>
[46] Greater London Authority Oversight Committee, *Meeting Agenda*, 16 July 2019. <https://www.london.gov.uk/moderngov/documents/g6732/Public%20reports%20pack%20Tuesday%2016-Jul-2019%2010.00%20GLA%20Oversight%20Committee.pdf?T=10>
[47] Open Rights Group, *Out for the Count: the £9 Million White Elephant in London's Next Election*, 2 September 2019. <https://www.openrightsgroup.org/blog/2019/out-for-the-count>
[48] This retraction, as far as we are aware, has not been announced publicly.
[49] This assertion was made in a meeting with ORG.

by the GLRO currently occupies and previously occupied sales roles), the expertise of one staff member alone cannot remedy Smartmatic's many active failings. It is a company that has been defined by failure and has yet to be held to account for this. ORG utterly rejects the characterisation of it as a suitable company with which to entrust UK democratic processes.

(v) It is also concerning that Smartmatic has been awarded this contract in an uncompetitive and non transparent manner. From the information that ORG has obtained to date, it appears that GLRO has failed to carry out any or appropriate due diligence on the companies which responded to the tender. The result is spiraling costs and low confidence amongst London Assembly members and others that the same failures that happened in 2016 will not happen in 2020.[50] The fact that the GLRO will not release the assessment scores of the individual companies involved in the bidding process suggests a lack of confidence in both the process and its outcome, although it has been suggested that they may release non commercially sensitive elements in the future. [51]

(vi) ORG is following developments in this area and campaigning for a wholesale review of use of e-counting software in the GLA elections. As part of this, we are calling for the GLRO to adopt the Open Contracting Principles and Open Contracting Data Standard set out by the Open Contracting Partnership to release the scores of individual companies in the assessment of their bids, and to set an acceptable cost threshold for the next procurement process.[52]

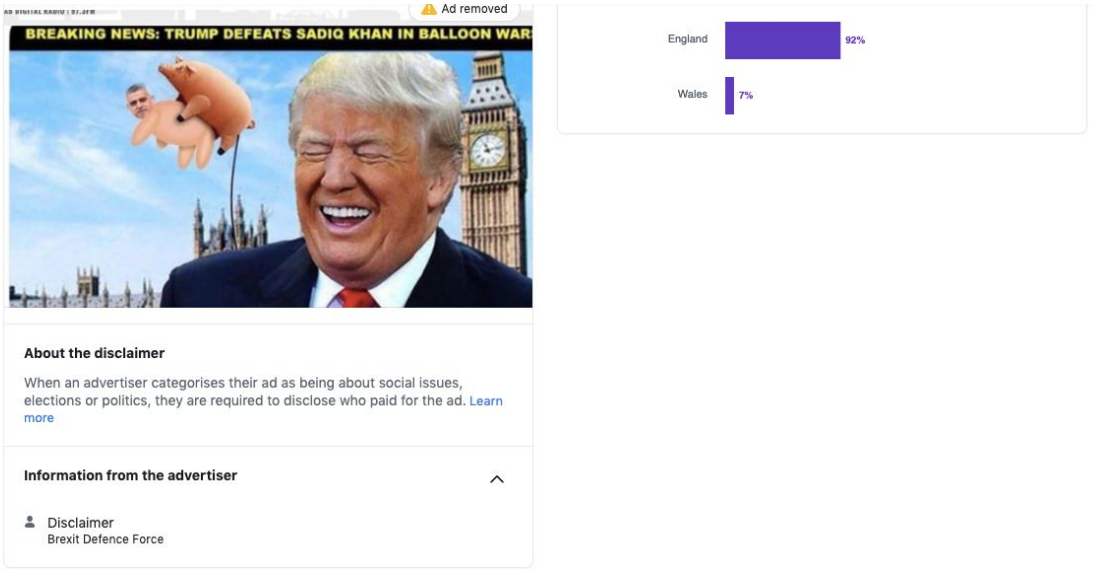
[50] n.44.
[51] Greater London Authority Oversight Committee, *Meeting Agenda 16th July 2019*, 2019. <https://www.london.gov.uk/gla-oversight-committee-2019-07-16>
We also have this confirmed in confidential emails from the Greater London Returning Officer.
[52] <https://www.open-contracting.org/implement/global-principles>

5. APPENDICES

Appendix A: Examples Demonstrating Need for Improved Financial Transparency

(i) Brexit Defence Force

'Brexit Defence Force' is the sponsor of adverts on the 'Brexit Votes Matter' Facebook community page as declared on Facebook Ad Library. The 'Brexit Defence Force' page was taken down by Facebook in January 2019 for breaching its community guidelines. The Brexit Defence Force has since resurfaced however as the sponsors of adverts on a new page 'Brexit Votes Matter'. Neither 'Brexit Defence Force' nor 'Brexit Votes Matter' are registered with Companies House.



Taken from Facebook's 'Ad Library'

The real-world identity of the individual/s behind 'Brexit Defence Force' to date remains unknown. This renders the Facebook Ad Library disclaimer impotent in terms of transparency to citizens and the ability to hold 'Brexit Defence Force' to account. It is also notable that a banned group has seemingly been able to easily bypass Facebook moderators to continue broadcasting political messages.

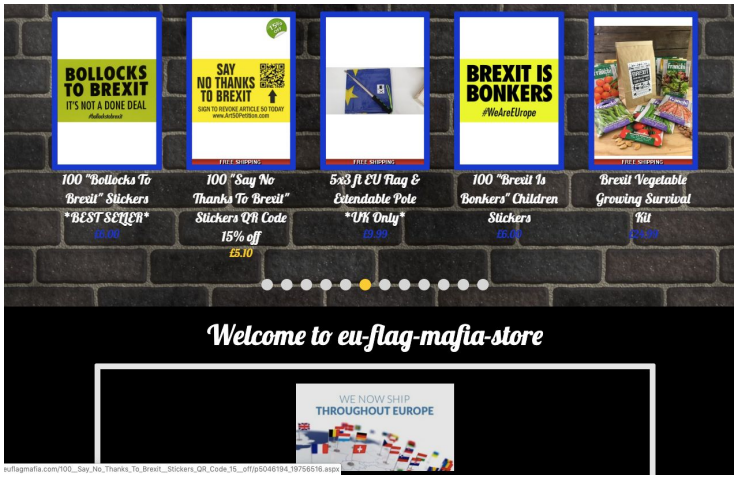
(ii) EU Flag Mafia

'EU Flag Mafia' is both a Facebook community page and the given identity of the individuals or organisation that pay for EU Flag Mafia adverts. Their online presence is

relatively limited, mainly encouraging the attendance of an event for which individuals have to buy tickets.

The EU Flag Mafia also runs a commercial website that seems to be capitalising on the 'Remainer' market to sell a variety of products, including the 'Brexit Vegetable Growing Survival Kit' for £24.99.

EU Flag Mafia is not listed at Companies House. The name listed under the 'contact' section of their website is 'P Casso'.



Taken from the 'EU Flag Mafia' website

Appendix B: Examples of the complex relationship between political campaigns, data protection and campaign finance regulation

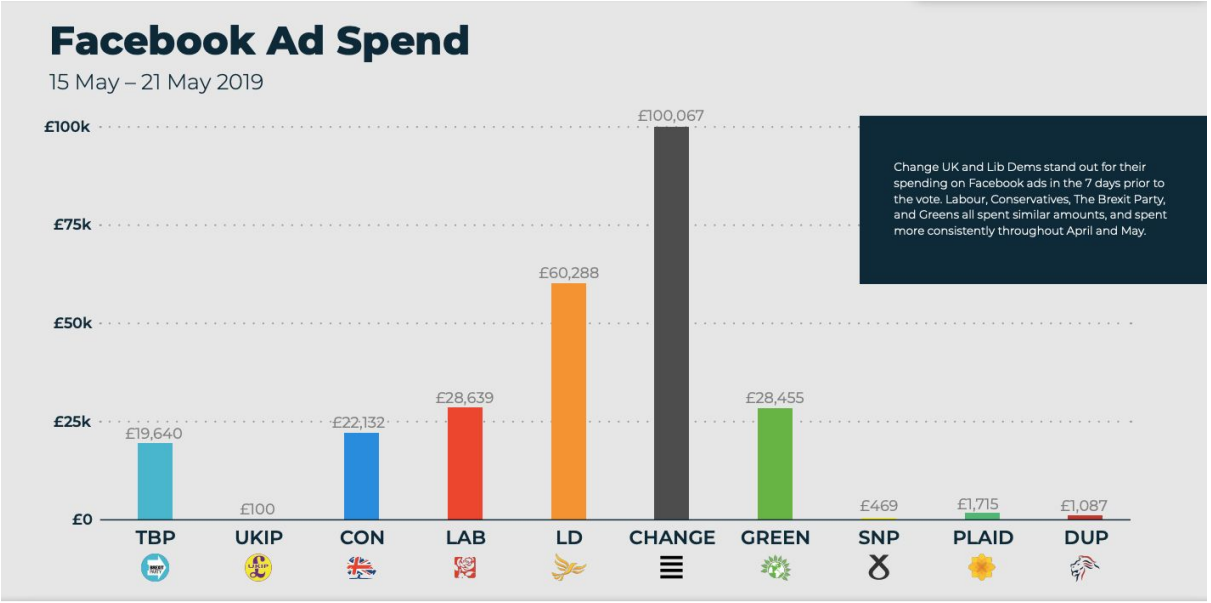
(i) Change UK vs Brexit Party Facebook Data Use and Voter Targeting

A report by the organisation 89UP on the 2019 European Parliament elections' digital campaigns identifies that the Brexit Party ran a far more successful Facebook campaign than Change UK, despite only spending one-fifth of the same budget.[53] Two key factors appear to have made the difference:

1. **The Brexit party understood their audience better, possibly as a result of better data analysis and expertise**. This made it easier for them to hone their messaging. Presumably this was work done outside of the regulated period. ChangeUK didn't have the same level of data infrastructure to model and target their persuadable segment of the electorate.

2. **The Brexit party were far more active with many more posts and shares**. During the period 5 April - 23 May 2019, the Brexit Party made 212 posts, compared with Change UK's 62. The Brexit Party received 325,900 shares compared to ChangeUK's 7,200. This activity translated into increased followership which could in turn be leveraged: the Brexit Party gained 30,200 Facebook followers vs ChangeUK's 3,600.

[53] 89UP, *The European Elections: How the Brexit Party won the online battle in the UK*, Undated <https://www.89up.org/sites/default/files/reports/The%20European%20Elections%20How%20The%20Brexit%20Party%20won%20the%20online%20battle%20in%20the%20UK%20f1.pdf>



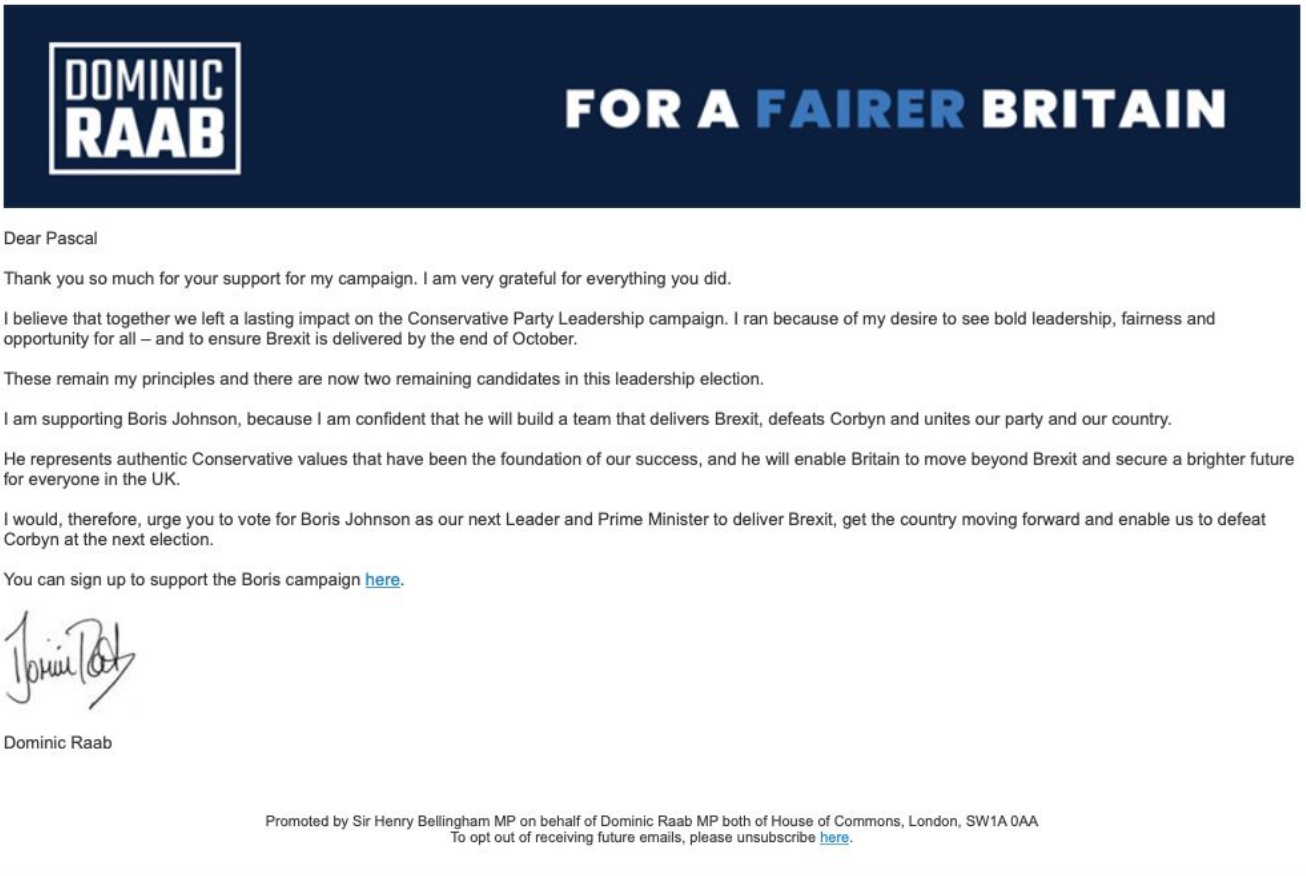
Taken from 89Up's report 'The European Elections: How The Brexit Party won the online political battle in the UK'

(ii) The digital activity of Conservative party leadership campaigns

As part of its investigation into the activities of political parties, ORG signed up to the mailing lists of Conservative party leadership candidates' campaigns during the 2019 leadership contest eventually won by Boris Johnson.

a) Dominic Raab's campaign

Dominic Raab's campaign emailed supporters, encouraging them to support Boris Johnson. Additionally, the email included a link to sign up to Boris Johnson's campaign.



DOMINIC RAAB

FOR A FAIRER BRITAIN

Dear Pascal

Thank you so much for your support for my campaign. I am very grateful for everything you did.

I believe that together we left a lasting impact on the Conservative Party Leadership campaign. I ran because of my desire to see bold leadership, fairness and opportunity for all – and to ensure Brexit is delivered by the end of October.

These remain my principles and there are now two remaining candidates in this leadership election.

I am supporting Boris Johnson, because I am confident that he will build a team that delivers Brexit, defeats Corbyn and unites our party and our country.

He represents authentic Conservative values that have been the foundation of our success, and he will enable Britain to move beyond Brexit and secure a brighter future for everyone in the UK.

I would, therefore, urge you to vote for Boris Johnson as our next Leader and Prime Minister to deliver Brexit, get the country moving forward and enable us to defeat Corbyn at the next election.

You can sign up to support the Boris campaign here.

Dominic Raab

Promoted by Sir Henry Bellingham MP on behalf of Dominic Raab MP both of House of Commons, London, SW1A 0AA
To opt out of receiving future emails, please unsubscribe here.

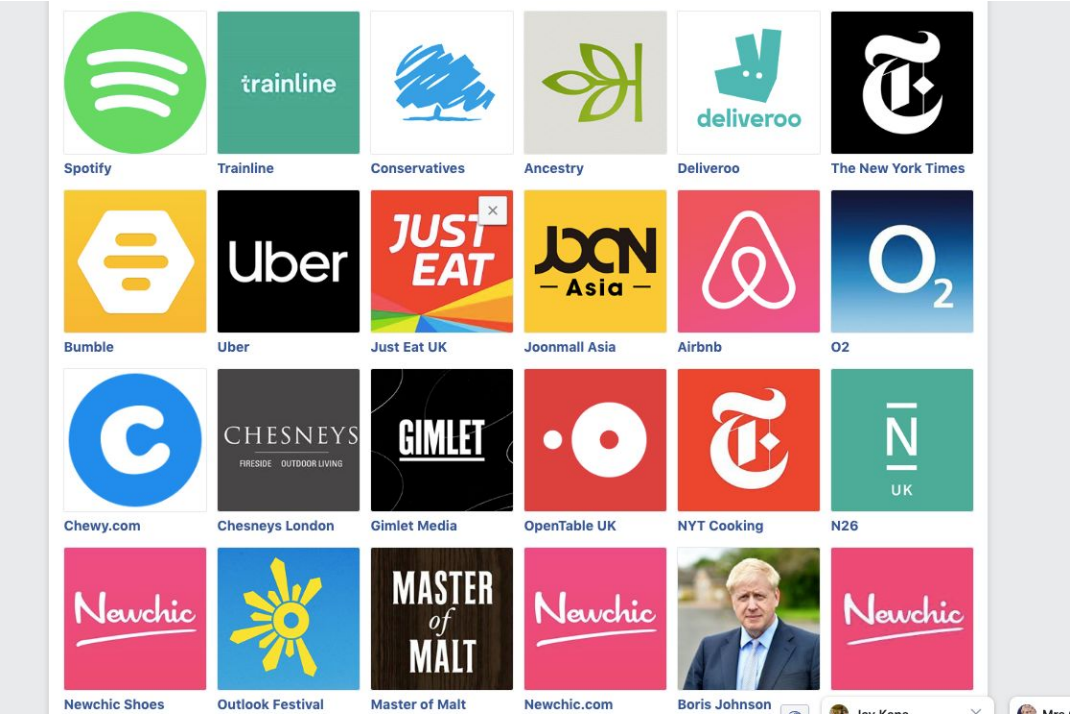
Email from Dominic Raab's campaign to Open Rights Group staff

We can see from this that the Boris Johnson leadership campaign was able to capitalise on the mailing list of the Dominic Raab campaign. It effectively targeted Conservative supporters who might have been otherwise unknown to them, and exhorted them to vote for Boris Johnson, for little or no additional cost.

This has significant implications for the regulation of coordination between campaigns. Rules around coordination are currently well defined in terms of limits in sharing financial resources and costs. Whilst spending limits on data assets such as email lists (whose financial value may be low, poorly defined, or contextual) do exist, they are not applied *effectively*. This is partly due to the limited number of declared spending categories, the timeline for reporting spending, and the limited capacity of an already overstretched regulator. As a result, existing cost based regulation would have been totally ineffective for significant campaigning efforts in the Conservative leadership election.

b) Boris Johnson's campaign

ORG staff signed up to Boris Johnson's campaign as part of its investigation. Later one member of staff noticed that the 'Boris Johnson' page was listed on Facebook as a page that had uploaded a list with their personal information onto Facebook.



Taken from ORG staff member's advertisement page on Facebook settings

This suggests that the Boris Johnson campaign had uploaded the staff member's personal information to Facebook without obtaining consent for this.

Privacy International had conducted an analysis of the various privacy policies of the leadership campaign websites;[54] however, it is now impossible to check whether this activity followed the Boris Johnson campaign privacy policy since the website containing this (and those of other candidates) were taken down after the campaign and not archived. This makes it difficult to scrutinise the candidates' campaign activities and hold them to account under the law.

c) Data controllership and response to Subject Access Requests

[54] Privacy International, *How the UK Conservative Leadership Race is Latest Example of Political Data Exploitation*, 2019. <https://privacyinternational.org/long-read/3019/how-uk-conservative-leadership-race-latest-example-political-data-exploitation>

In the case of several Conservative leadership campaigns, the MP in question was listed as the data controller for the campaign. For example, Jeremy Hunt was listed as the data controller for the 'Team Hunt' campaign, meaning that Jeremy Hunt is legally responsible for their campaign's use of data.

ORG sent Subject Access Requests (SARs) to the individual leadership campaigns. Whilst some were responsive and timely, others were not. For example, the 'Team Hunt' campaign has, at the time of writing, still not responded to ORG's SAR. As the time limit has now expired, ORG plans to highlight this via a complaint to the ICO to draw attention to Jeremy Hunt's controllership role.

The listing of individual MP's as controllers suggests a severe lack of engagement with, or misunderstanding of data protection law by some Conservative leadership candidates.

(iii) Open Rights Group Subject Access Requests to UK Political Parties

During the leadership campaign, two ORG staff members sent Subject Access Requests (SARs) to the largest UK political parties. This process acted the pilot for a wider campaign of SARs that ORG intends to run later in the year. From the data obtained in these SARS, we have drawn several preliminary conclusions:[55]

1. **Bigger, more established parties have more data capabilities**. The Conservatives use the Experian product 'Mosaic', which generates demographic data based on 300 data points. In contrast, the Liberal Democrats in this election assigned a possible 37 scores - it's not known whether this statistical calculation used a paid-for external product. This difference provisionally indicates that smaller parties are less likely to have profiling capabilities - which may affect their ability to target voters.

2. **Conclusions drawn by profiling often seemed very general, or incorrect**. For example, "Uptown Elite" (one of the Mosaic audience categories which individuals are ascribed based on their data points) is described as "High status households owning elegant homes in accessible inner suburbs where they enjoy city life in comfort".[56] Without more granular data about individuals available, this seems a comparable level of insight to identifying 'Mondeo man' in the 1990's. Staff members who sent SARs also noted that profiling and scores appointed by the Liberal Democrats were inaccurate and at odds with their

[55] These are extremely limited by the sample on which they are based but will be able to be strengthened and developed with extension and replication.
[56] The Audience Agency, *Explanation: Mosaic.*
<https://www.theaudienceagency.org/insight/mosaic>

political beliefs, suggesting potential for a high error rate in the conclusions drawn by these systems.[57]

3. **A bigger study, with better sampling, could provide greater evidence of targeting.** SARs only reveal what data is held about the sender. It was always unlikely that the SARs of two individuals who work in data protection, enjoy a high level of data protection and live in safe seats, would be priority targets for profiling for political parties. It is more likely that individuals who live in marginal seats, have low levels of data protection and are members of minority demographics would be more interesting political targets - and thus yield more interesting research results. ORG intends to run a wider study focused on individuals resident in swing seats in order to obtain even more valuable insights.

4. **Labour did not respond adequately to any SARs - perhaps because they are processing large amounts of personal data.** Labour informed us that they would not comply with their requirements under UK data protection law. We hypothesise this is because they are processing large amounts of personal data - however we stress that this is a conclusion based on speculation alone. It will be impossible to confirm or refute this speculation until we receive a completed SAR response. ORG has raised a complaint with the ICO about Labour's non-responsiveness to the SAR requests. We do not expect a response to this complaint for three or more months due to the backlog of complaints at the ICO.

Full results obtained are displayed below. 'Data', 'profiling', 'scores' and 'sources' refer to non-electoral register (ER) data.

Political Party	Replied in Time	Data held	Profiling	Scores	Sources other than ER	Other
Labour	No- complaint sent to ICO	NA	NA	NA	NA	NA
Conservatives	Yes	Yes	Yes	"Uptown Elite A02_2"	Experian Mosaic	NA
Lib Dems	Yes	Yes	Yes- various	Yes-various	Yes, not specified	NA
Greens	Yes	No	NA	NA	NA	NA

[57] Sky News, *The Lib Dems are using data to profile every voter in the UK - and give you a score*, 2019. <https://news.sky.com/story/the-lib-dems-are-using-data-to-profile-every-voter-in-uk-and-give-you-a-score-11828202>

UKIP	Yes	No	NA	NA	NA	NA
SNP	Yes	No	NA	NA	NA	Only held data for Scotland ER
Brexit Party	No-complaint sent to ICO	No	NA	NA	NA	Did not provide contact for DPO
Change UK	Yes	No	NA	NA	NA	NA
DUP	Yes	No	NA	NA	NA	NA