CENTRE FOR IT & IP LAW

Kenniscentrum
Data & Maatschappij

AGAINST OPACITY in Digital Political Campaigns

Vian Bakir[1]
Professor of Journalism & Political Communication
Bangor University, UK

How has digital technology changed the way that democracy works? Has this been a net positive or negative effect? In 2019, these were among the questions asked by the UK Parliament's House of Lords Select Committee on Democracy and Digital Technologies. Along with Andrew McStay (Professor in Digital Life), we responded with a written submission that argues that we need an ethical code of conduct for transparent, explainable, civil and informative digital political campaigns. We discussed these in December 2019 as part of our Fellowships at the Interdisciplinary Study of Law at KU Leuven, under the theme of "Tackling Grand Challenges in Society".

The need for such an ethical code of conduct arises because Artificial Intelligence (AI) is an increasing feature of political campaigning. AI is used in order to "profile" audiences - to generate automated insights into datasets using data-mining techniques. AI is used for iterative, large-scale, rapid testing of ads online ("A/B" tests) in order to identify and deploy the most persuasive ad. Finally, AI is used to gather data on, and target, the most important voters with tailored messages. This brings both democratic benefits and harms.

1. Benefits and Harms from Digital Political Campaigning

On democratic benefits, digital political campaigning has the potential to better engage hard-to-reach parts of the electorate. Furthermore, by tapping into voters' sentiments, it can help politicians identify issues and policies that voters care about, thereby making politicians more responsive to electorates. However, to realise these benefits requires that campaigns are conducted honestly and *openly*, otherwise we descend into covert, attempted manipulation of electorates.

Unfortunately, digital political campaigning is currently *opaque*, presenting many harms exploitable by bad actors. These include negatively impacting on citizens' ability to make informed choices; fragmenting national conversations thereby weakening our ability to hold political campaigners to account; increasing the potential for targeted voter suppression; and enabling exploitation of people's psychological vulnerabilities.

[1] The views expressed in this paper are those of the author and do not necessarily reflect the views or policies of the Knowledge Center Data & Society or CiTiP. The paper aims to contribute to the existing debate on AI.

2. Opaque Digital Political Campaigning: the "Leave" campaigns in the "Brexit" referendum

In the UK, the height of this opacity was the 2016 "Brexit" referendum on whether the UK should leave, or remain in, the European Union (EU). In particular, the various "Leave" campaigns operated with a degree of opacity that concerned multiple regulators.

"Vote Leave" (the designated official campaign to leave the EU) spent £2,901,566 on data-driven platforms, advertising/data companies, and consultants/strategists in the EU Referendum – over £1 million more than the official Remain group, "Britain Stronger In". The largest element of Vote Leave's outlay was on Canadian digital advertising web and software development company, AggregateIQ. This company was employed to build a "core audience" for Vote Leave's adverts, by identifying the social media profiles of those who had already "liked" Eurosceptic pages on Facebook, and advertising to this audience to bring them onto its website where they were invited to add their details to its database. AggregateIQ also used Facebook's "Lookalike Audience Builder", which applied demographic features identified by Facebook in the core audience group to the wider UK population. This second group (the "persuadables") consisted of 9 million people on Facebook whom Facebook identified as having the same demographic features as the core audience, but had not previously expressed interest in Eurosceptic Facebook content by "liking" Eurosceptic pages. Vote Leave's campaign director, Dominic Cummings, estimates that Vote Leave ran around one billion targeted digital ads in the run up to the vote, mostly via Facebook, testing multiple different versions in interactive feedback loops.

Aggregate IQ worked not just for Vote Leave, but also for several other unofficial "Leave" campaigns: "Be Leave", "Veterans for Britain" and "DUP Vote to Leave". According to UK electoral law, this is legal as long as each of the campaigns is separate, and *not coordinated* with each other However, for several years following the referendum, there was opacity about whether spending limits had been breached, campaigns coordinated with other groups, and data shared among the Leave campaigns. It was not until June 2018 that The Electoral Commission (the independent body which oversees UK elections and regulates political finance) found that Vote Leave and BeLeave acted under an undeclared common plan, for which they both relied on the services of Aggregate IQ. The UK Information Commissioner's Office further clarified in November 2018 that Vote Leave and BeLeave used the same data set to identify audiences and select targeting criteria for ads.

There is also opacity about what data-mining services the political campaigns actually used. For instance, a long-running question is whether the now defunct political analytics company, Cambridge Analytica, worked for Leave.EU. Arron Banks (Leave.EU's founder) claims that Cambridge Analytica/SCL Group merely prepared a detailed *pitch* to Leave.EU to help make the case to the Electoral Commission that Leave.EU should be the official campaign group for Leave, but that Leave.EU did not take it forward. Nonetheless, and worryingly, part of this pitch offered voter suppression. The pitch claims that its "powerful predictive analytics and campaign messaging capacity can help you to segment and message the population according to a range of criteria". One of these criteria is "Partisanship". As well as describing the "General Voter" and "Ideological Voter", it describes the "Opposition Voter – groups to dissuade from political engagement". This would be achieved by Target Audience Analysis – a once exclusively military psy-ops tool that claims to be able to identify and influence influential target audiences in order to change their behaviour, and to model different interventions in this desired behaviour change. In July 2019, Cambridge Analytica whistleblower, Britanny Kaiser, supplied ten documents to the UK Parliament's Digital, Culture, Media and Sport Committee on Fake News. They show that Cambridge Analytica analysed membership data and survey results from UKIP (UK Independence Party - a hard Eurosceptic, right-wing UK political party) to model four key groups of persuadable UK voters to be targeted with Leave.EU messaging. Later in 2019, whistleblower Dan Dennemarck, UKIP's former data controller, claimed that he had been ordered to hand over UKIP's database of over 100,000 current and ex-members to staff of Leave.EU during the EU referendum.

Use of such tools, and such data sharing, to optimise messages for profiled audiences is especially problematic when the messages are emotive, deceptive and targeted at audiences predisposed to be receptive to such messages. Indeed, while Vote Leave campaigned strongly to control immigration, Leave.EU pumped out much harsher anti-immigration messages on social media during the campaign. Indeed, Leave.EU's founder, Arron Banks, described the issue of immigration as one that set "the wild fires burning" on social media. A typical Leave.EU Facebook post warned voters that "immigration without assimilation equals invasion". An investigation by UK national broadcaster, Channel 4 News, in 2019 found that Leave.EU was behind a fake video "undercover investigation" that went viral on Facebook. The video purported to show how easy it is to smuggle migrants into the UK from across the English Channel. Debunking this video several years later, satellite data seen by Channel 4 News shows that the footage was filmed in reverse.

3. Democratic Harms

It is hard for society to rebut and correct false, emotive claims when such messages are micro-targeted, in digital echo chambers. Furthermore, once people have made up their minds on an issue, it is hard to persuade them change their opinions. Indeed, evidence from computational approaches shows that users accept confirmatory information on Facebook even if containing deliberately false claims. Furthermore, legacy technology companies such as Facebook, Google, Microsoft, Intel, NEC and Amazon are becoming much more active with "emotional AI" technologies that aim to read and react to emotions through text, voice, computer vision and biometric sensing. A tipping point to mass profiling of emotional life is likely by the early 2020s, enabling far greater profiling of audiences' emotional and affective states.

We have already reached a phase where opacity in the use of these profiling technologies has become problematic, and this is likely to worsen with the increasing use of AI in political campaigning alongside the rise of mass profiling of emotional life. This brings with it at least four harms to democracy.

> ***1. Capacity to negatively impact citizens' ability to make informed choices.*** The UK's data regulator, the Information Commissioners Office warns that, "If voters are unaware of how their data is being used to target them with political messages, then they won't be empowered to exercise their legal rights in relation to that data and the techniques being deployed, or to challenge the messages they are receiving". This is already an issue with current levels of technological deployment in digital political campaigns but could become far worse. A report commissioned by the Information Commissioners Office flags the coming

problem of creation by private companies of new forms of personal data via probabilistic data inferences from metadata arising from people’s device use and behaviour. The report suggests that political campaigns will be particularly interested in our *persuadability* to certain messages, whether about immigration or other issues, and that it is hard to see how the user would know that this data exists or exercise their rights to have it removed or corrected.

2. Fragmentation of national conversations and our ability to hold political campaigners to account. If deceptive micro-targeting takes place, and if this is not scrutinised by national authorities and media, then there is little chance of those elected on such platforms being held to public account. As all political parties increase their use of algorithmic marketing techniques, the scale of algorithmically optimised messages could overwhelm regulators, with deleterious consequences for the transparency and political accountability of campaigns.

3. Increased potential for targeted voter suppression. As described earlier, Cambridge Analytica/SCL Group offered voter suppression as part of its pitch for Leave.EU’s business. Similarly, in the 2016 Trump presidential campaign, Brad Parscale, the campaign’s digital director in 2016 (and also for 2020), used Facebook’s Lookalike Audiences ad tool in 2016 to expand the number of people the campaign could target by identifying voters who were not Donald Trump supporters, and targeting them with psychographic messaging designed to discourage them from voting. Such voter suppression was aimed at three targeted groups that Hillary Clinton needed to win overwhelmingly: idealistic white liberals, young women and African Americans.

4. Enabling exploitation of people’s psychological vulnerabilities. Again, these were services offered by Cambridge Analytica/SCL Group to Leave.EU. Documents supplied by whistleblower Britanny Kaiser to the UK Parliament’s Digital, Culture, Media and Sport Committee on Fake News showed that Cambridge Analytica analysed UKIP membership data and survey results to model four key groups of persuadable UK voters to be targeted with Leave.EU messaging: the “Eager Activist”, “Young Reformers”, “Disaffected Tories” and “Left Behinds”. “Left Behinds” are described as follows:

- “Feels increasingly left behind by society and globalisation
- Unhappy with the economy and the NHS, but immigration is most important issue
- Suspicious of the establishment including politicians banks and corporations
- Worried about their economic security, deteriorating public order and the future generally.”

People in this folorn “Unhappy”,”Suspicious”, “Worried” state are arguably psychologically vulnerable, and should be protected from streams of highly targeted messages designed to exploit such vulnerabilities (such as anti-immigration messages).

4. Towards an Ethical Code of Conduct for Digital Political Campaigns

To combat this state of affairs, we need an ethical code of conduct for transparent, explainable, civil and informative digital political campaigns (see Table 1).

Table 1. Ethical Code of Conduct for Digital Political Campaigns

Transparency	Make clear if political messages online come from a party, how much campaigners spend on digital campaigning, and on what.
Explainability	In campaigns that extensively use AI to profile voters, give all voters an explanation of the profiling.
Civility	Campaign material should be civil (e.g. not nasty, aggressive, disrespectful, or pitched to provoke anger and outrage) and must not incite others to commit crimes (e.g. making false statements of fact about candidates' personal character or conduct). If campaigners deliberately breach civility codes to become righteously uncivil (for moral reasons), then rationally justify why.
Informativeness	Campaigns should give voters enough information to freely make informed judgments. The information provided should be true, complete, undistorted and relevant.

On transparency. Following the political outcry arising from the opacity and associated fears of foreign influence over the 2016 Brexit Referendum, and also the 2016 US presidential campaign, the large US social media platforms have worked to improve the transparency of digital political campaigns. Since 2018, Google and Facebook have provided publicly searchable libraries of election ads and spending on their platforms: each Facebook ad also says who paid for it. These are good moves, although more should be done.

On explainability. Facebook's political ad library includes information on broad geographic targeting (e.g. in the UK, whether England, Scotland, Wales or Northern Ireland was targeted), broad demographic targeting (age, gender), reach and amount spent on ads. Since February 2019, users can click on a Facebook button 'Why am I seeing this ad?' that tells them the brand that paid for the ad, some biographical details targeted, if and when the brand or its agency/developer partners uploaded the user's contact information, and when access was shared between partners. However, there is no information on finer-grained targeting such as use of psychographics and probabilistic data inferences from metadata; or to what campaign end they were targeted (e.g. voter mobilisation, suppression).
More positively, on 20 November 2019, Google announced that targeting of election ads would be limited to general categories (age, gender, post code location); and advertisers would no longer be able to target political messages based on users' interests inferred from browsing or search histories.

On ***civility*** and ***informativeness***. Our ethical code also has demands for political campaigners to run civil and informative campaigns. We include these demands for completeness, while recognising that they are unlikely to be met given that extensive use of deceptive appeals to emotion in political campaigns have been evident since the start of research into political communication. It is well understood that political campaigns manipulate a politics of spectacle and fear to spread populist messages; and to mislead and distract electorates from their core interests. Nonetheless, for completeness, we include civility and informativeness in our ethical demands.

5. Policymakers Should ….

While politicians may feel unable to meet the ethical demands for civility and informativeness, the ethical demands for transparency and explainability must be met if we are to avoid the democratic harms already evident from the increased use of AI in political campaigns.

On transparency, while the large US social media platforms have worked since 2016 to improve the transparency of digital political campaigns, policymakers should consider creating an independent, searchable, public register of online political adverts to facilitate analysis of entire digital campaigns. Policymakers should also require political campaign messages (including digital) to bear imprints to clearly show who produced them; and provide details on how much the campaign spent on digital campaigning, and where this money was spent (including on data analytics and consultants).

On explainability, policymakers should encourage the social media platforms to provide more information to users on the use of finer-grained targeting in political campaigns such as psychographics and probabilistic data inferences from metadata. Finally, policymakers should encourage political campaigners to explain to what campaign end users were targeted (e.g. voter mobilisation, suppression).

These greater levels of transparency and explainability would better equip voters to assess the campaign messages to which they have been exposed. This should positively impact citizens' ability to make informed choices; enable greater scrutiny and evaluation of fragmented national campaigns; decrease the likelihood of secretive, targeted voter suppression; and alert people to any exploitation of their own psychological vulnerabilities.