

Article

Beyond Brexit? Public Participation in Decision-Making on Campaign Data During and After Referendum Campaigns

Julia Rone

Minderoo Centre for Technology and Democracy, University of Cambridge, UK; jr803@cam.ac.uk

Submitted: 8 September 2022 | Accepted: 22 December 2022 | Published: 31 January 2023

Abstract

While the Brexit referendum campaign has been extensively researched, media, regulatory bodies, and academics have often talked at cross-purposes. A strong focus on Cambridge Analytica's role in the 2016 referendum, despite official investigations concluding the company had only limited involvement in the campaign, has distracted attention from more mundane but highly controversial data practices, including selling voters' data to third parties or re-using campaign data without consent from data subjects. This empirical case study of data-driven referendum campaigning around Brexit raises two broader theoretical questions: First, moving beyond the current focus on transparency and accountability, can public participation in the ownership and management of campaign data address some of the problematic data practices outlined? Second, most academic literature on data-driven campaigning, in general, and referendum campaigns, in particular, has often overlooked the key question of what happens with campaigning data once campaigns are over. What legal safeguards or mechanisms of accountability and participation are there to guarantee consent when it comes to further re-use of people's data gathered during campaigns? Ultimately, the article raises the question of who should have a say in how "people's data" is used in referendum campaigns and afterwards and makes a case for democratising such decisions.

Keywords

Brexit; data-driven campaigning; digital democracy; participation; referendums; referendum campaigns

Issue

This article is part of the issue "Referendum Campaigns in the Digital Age" edited by Linards Udris (University of Zurich) and Mark Eisenegger (University of Zurich).

© 2023 by the author(s); licensee Cogitatio (Lisbon, Portugal). This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

1. Introduction

Data-driven campaigning has been the focus of public and academic attention already since the 2008 Obama campaign and even earlier (Stromer-Galley, 2019). Most existing research so far, however, has focused on election campaigns (Anstead, 2017; Bennett & Lyon, 2019; Chadwick & Stromer-Galley, 2016; Howard, 2005; Kefford et al., 2022; Montigny et al., 2019; Stromer-Galley, 2019), while referendum campaigns have been generally overlooked (see Udris & Eisenegger, 2023). Probably the one big exception from this common trend has been the highly prominent 2016 Brexit referendum campaign on whether the UK should leave the European Union. The Brexit referendum resulted in a surprising victory for Leave, leading to a protracted political crisis with multiple overlapping conflicts of sovereignty in the

UK. Cadwalladr's (2017) explosive investigations on connections between the Leave campaigns and the controversial firm Cambridge Analytica sparked a broad media debate on the role of psychological profiling and targeted advertising online. Within the UK, the number of articles discussing Cambridge Analytica skyrocketed, with almost 10,000 pieces mentioning Cambridge Analytica in 2018, before attention to the topic starkly declined in the following years (see Figure 1).

In the aftermath of the 2016 referendum, several official investigations into Brexit campaigning started collecting information on a wide range of issues such as the use of data analytics in political campaigning, funding irregularities, foreign interference, disinformation, and fake news. Academic research also explored the use of social media in Brexit-related campaigning (Brändle et al., 2022; Hänska & Bauchowitz, 2017), the broader impacts

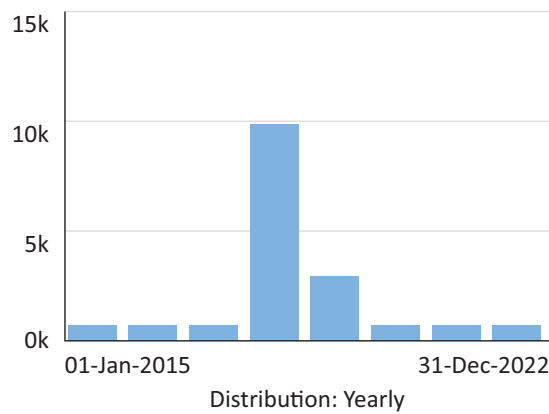


Figure 1. Mentions of “Cambridge Analytica” in UK media featured in the Factiva database. Source: Factiva (2023).

of data analytics use on democracy (Risso, 2018), as well as what types of regulations and oversight of data-driven campaigning would be needed (Dommett, 2020; Margetts & Dommett, 2020).

Despite the fact the Brexit referendum campaign has been so well and extensively researched, media, regulatory bodies, and academics have sometimes talked at cross-purposes, with little cross-pollination between their different perspectives and findings. Thus, even though the UK’s Information Commissioner’s Office (ICO) report on the use of data analytics in political campaigns established already in 2018 (on the basis of analysis of 42 computers, 700 terabytes of data, 31 servers, and more than 300,000 documents as part of their investigation) that Cambridge Analytica did *not* directly misuse data of UK voters to influence the Brexit referendum, references to the data practices of Cambridge Analytica as related to the Brexit referendum are still made in academic articles on Brexit (Brändle et al., 2022; Markussen, 2022; Ortega Martín & Sánchez Berrocal, 2022).

Furthermore, there has been an extensive research focus on the campaigns in the lead-up to the referendum, but we know almost nothing about post-referendum campaigns such as the People’s Vote, which campaigned for a second referendum. The few academic articles that have explored these campaigns or related online activity (Brändle et al., 2018, 2022; Rone, 2022) focus on issues such as citizenship, polarisation, and the instrumentalisation of sovereignty but have little to say about the data practices of these campaigns. This is a significant gap in the literature: The campaign for People’s Vote that unfolded in the aftermath of the 2016 referendum, for example, was one of the most significant campaigning efforts in the UK, responsible for two of the biggest marches in the country since 2000, comparable only with the march against the Iraq War in 2003.

Considering these two points, the current article offers a case study of the data practices of Brexit-related referendum campaigns with a special focus on who had a say in how citizen data was managed within these campaigns. I use this specific case study to raise two broader theoretical points that open directions for research on

other referendum campaigns as well. First, following original research that has dispelled the myths of digital campaigning (Anstead, 2018; Baldwin-Philippi, 2017; Kefford et al., 2022; Simon, 2019), I argue that despite overblown fears about psychological profiling and individualised targeted advertising, some of the most problematic occurrences in terms of data management actually resulted from bad organisational practices and the concentration of power in the hands of unelected businessmen. In both pro- and anti-Brexit campaigns, the people ended up being “spectators in their democracy” (Edelman, 1988, as cited in Stromer-Galley, 2019, p. 18) with no control over how their data was collected, managed, and sometimes misused. At the same time, attempts to address such problems through regulatory means have focused on improving transparency above all (regardless of how detailed demands for transparency are; Dommett, 2020), but have rarely even considered the possibility of democratic public participation in campaign data ownership and management.

Following the classic definition by Smith (1983, as cited in Rowe Frewer, 2000, p. 6), public participation is understood in this article as “encompassing a group of procedures designed to consult, involve, and inform the public to allow those affected by a decision to have an input into that decision.” There has been a rise in interest in public participation since it can fulfil a number of purposes, including:

Fulfilling legal requirements; embodying the ideals of democratic participation and inclusion; advancing social justice; informing the public; enhancing understanding of public problems and exploring and generating potential solutions; and producing policies, plans and projects of higher quality in terms of their content. (Quick & Bryson, 2016, p. 160)

Furthermore, public participation is also “an important end unto itself in a democratic society” (Quick & Bryson, 2016, p. 160), often fostering citizens’ appreciation for and experience in democratic procedures through their involvement in participatory practices. Overlooking

participation when it comes to the ownership and governance of campaign data has narrowed down not only the range of possible solutions, but also the very interpretation of problems involved as related, above all, to fairness, accountability, and transparency rather than as problems of democracy as well.

Second, the literature on data-driven campaigning has often overlooked the key question of what happens with collected data once campaigns are over. What legal safeguards or mechanisms of accountability and participation are there in place to guarantee consent when it comes to further re-use of people's data gathered during campaigns? Posing this issue and acknowledging the complex after-life of data is an important first step to reasserting control and ensuring public consent over data usage beyond the stages of initial collection and campaigning.

The article is based on a qualitative thematic analysis of key official policy reports on the Brexit campaigning, including the 2018 ICO investigation into the use of data analytics in political campaigns and the 2019 Digital, Culture, Media and Sport Committee (DCMSC) parliamentary report on fake news and disinformation. I complemented these official policy sources with relevant media articles (identified through a combination of searching for the campaign names in Google, e.g., "Leave.EU," "Britain Stronger in Europe," "Leave Means Leave," "People's Vote," and snowballing from relevant articles) covering the internal politics and data use of pro-Brexit and anti-Brexit campaigns, as well as interviews with Richard Tice (associated with the Leave.EU and Leave Means Leave campaigns) and Tom Baldwin (communications director of the People's Vote campaign) from the UK in Changing Europe Brexit Witness Archive, and finally the books *The Bad Boys of Brexit* (on the Leave.EU Campaign, based on Aaron Banks' diary and emails on the 2016 referendum campaign) and *Unleashing Demons* (on the Britain Stronger in Europe campaign, written by Craig Oliver, David Cameron's director of communications). My goal was to triangulate these different types of sources on both pro-Brexit and anti-Brexit campaigns and to unearth different practices of data-driven campaigning. I did a thematic analysis (Braun & Clarke, 2006) of these sources, focusing specifically on two key themes that emerged from the sources: (a) Who owned citizens' data?; and (b) who had influence on how citizens' data was managed and used? In choosing these two topics to explore in Brexit-related referendum campaigning, I hope to enrich academic scholarship on the Brexit referendum, but also to open avenues for future thinking about the data practices of referendum campaigns, more generally.

2. Grounding Data-Driven Campaigning: Dangers, Myths, and the Role of Context

While the use of digital media for campaigning has been the focus of academic research already since the 1990s (Howard, 2005; Stromer-Galley, 2019), what has changed

over the last decade has been the advent of "computational politics," comprising six intertwined dynamics, namely:

The rise of big data, the shift away from demographics to individualized targeting, the opacity and power of computational modelling, the use of persuasive behavioural science, digital media enabling dynamic real-time experimentation, and the growth of new power brokers who own the data or social media environments. (Tufekci, 2014)

This complex assemblage of practices that includes micro-targeting but goes beyond it has been also referred to in the literature as "data-driven campaigning" (Anstead, 2017) or "data-driven elections" (Bennett & Lyon, 2019). As Bennett and Lyon (2019, pp. 10–11) emphasise, "data-driven elections" is a broad concept that includes the collection of voters' data, the performance of voter analytics, and, at a later stage, political micro-targeting. Their larger point is that:

These are all essentially surveillance practices. The data are being collected, analysed and used powerfully to influence certain populations: to convince them to vote, or not to vote; to persuade of the merits of one candidate, or the faults of an opposing candidate. (Bennett & Lyon, 2019, p. 11)

In this article, I have chosen to use the term "data-driven campaigning" to emphasise not only the computational aspect of novel data practices but also questions of data collection, management, and re-use.

The rise of data-driven campaigning has led to a substantial body of academic research drawing attention to the dangers associated with it. In their comprehensive overview of the literature on promises and threats of online micro-targeting, Borgesius et al. (2018) identified threats to citizens, political parties, and public opinion more generally. To begin with, citizens' "privacy could be invaded, and they could be manipulated or ignored" (Borgesius et al., 2018, p. 87). Crucially, political parties could present themselves as one issue parties to different citizens (Borgesius et al., 2018). And because of micro-targeting, voters could falsely assume that an issue was of primary importance to the party, while in fact, it was not. Furthermore, micro-targeting can be very expensive; thus it might consolidate the power of bigger parties at the expense of smaller ones, while also empowering new intermediaries such as social network platforms (Borgesius et al., 2018, p. 88). Microtargeting could also lead to a general fragmentation of public debate, with voters losing interest in overarching issues and focusing only on the issues that are of interest to them (Borgesius et al., 2018, p. 89). Emphasising deeper shifts in thinking and action, Ulbricht (2020) has also argued that the rise of data-driven campaigning has changed political epistemologies, leading to practices

such as “demos-scraping” where “increasing political participation” is defined as extracting consumer data rather than encouraging citizens to act politically in a conscious and intentional way.

On the other hand, several scholars have challenged the dystopias of data-driven campaigning by arguing that the importance and effects of using big data, psychological profiling, and micro-targeting in digital campaigns have been vastly oversold. Exploring the online self-presentation of the political data analytics industry, Simon (2019) argues that mass media reporting has uncritically accepted the marketing claims of data analysts who intentionally create an air of omnipotence and mystery behind their “highly scientific” methods—Indeed, the science behind the services they offer plays the role of a token, a fetish for attracting clients (Simon, 2019). And, in her analysis of the 2016 Trump and Clinton campaigns in the US, Baldwin-Philippi (2017, p. 631) argues that most fears related to micro-targeting are concerns of:

Theoretical impact rather than actual impact, with recent studies showing the following: the “micro” part of targeting is no more effective than using public records, and we not are stuck in filter bubbles; instead audiences duplicate and overlap frequently.

Most recently, an empirical study of data-driven campaigning in six-advanced democracies has shown that rather than causing a full-fledged disruption, data-driven campaigning has adapted to pre-existing campaigning techniques and is in practice much less sophisticated than what dystopian texts on democratic decline assume (Kefford et al., 2022).

Regardless of where they stand in their normative judgements, most researchers so far have agreed that data-driven campaigning does not unfold in the same way in different countries but is strongly determined by pre-existing legal regulations, political norms, and institutional set-ups (Anstead, 2017, 2018; Bennett & Lyon, 2019). Countries with laxer data protection laws, such as the US, Canada, or Australia (Kefford et al., 2022; Montigny et al., 2019), make much heavier use of data-driven campaigning, as compared to countries with stronger data-protection regulations, such as Germany, for example (Kruschinski & Haller, 2017). Also, in the UK, legal constraints and the low availability of useful voters’ data have been pointed out by different political parties as important obstacles to data-driven campaigning (Anstead, 2017).

To be sure, most of the research discussed in this section has focused above all on election campaigns, while there has been only limited attention to referendum campaigns, not to mention questions of data sharing between political parties and third actors (Rowbottom, 2020) across elections and referendum campaigns. In what follows, I hope to fill in this gap by focusing on data-driven referendum campaigning around Brexit.

3. Connections Between the Leave Campaigns and Cambridge Analytica: Beyond the Media Hype

Journalistic reports from 2017 and 2018, among which Carole Cadwalladr’s highly visible investigative journalism for *The Guardian* (Cadwalladr, 2017; Cadwalladr & Townsend, 2018), sparked a salient public debate about the involvement of Cambridge Analytica in the Brexit referendum campaign. Cambridge Analytica was in fact the trading name of SCLE Elections Ltd. and the responsibilities of the companies often overlapped. Both were subsidiaries of SCLE Group ([SCL] Information Commissioner’s Office, 2018, p. 8). There were two main points to the scandal: (a) Cambridge Analytica representatives had done data analytics work for the unofficial Leave.EU campaign; (b) the Canadian firm AggregateIQ (AIQ), closely related to Cambridge Analytica, had done data analytics for the official Vote Leave campaign as well as other Leave campaigns such as BeLeave and Veterans for Brexit. The initial journalistic reports, together with testimonies for the official investigations of the campaign, prompted a lot of academic research on the consequences of micro-targeting for political campaigns, often lumping together the election of Donald Trump and Brexit. Still, the results of the official investigations in the UK on both aspects of the scandal outlined above produced results quite different from what media reporting would have led us to expect.

Regarding the first point—Cambridge Analytica providing data analytics to the unofficial Leave.EU campaign—suspicions were very well founded. In his book *Bad Boys of Brexit*, Arron Banks (2017, p. 84), co-founder of Leave.EU, explicitly stated:

We’ve hired Cambridge Analytica, an American company that uses “big data and advanced psychographics” to influence people....With this information, you can tailor campaign material to particular groups to vote. It may sound a bit creepy, but these days it’s how most big political parties work.

Cambridge Analytica appeared at a Leave.EU press conference in November 2015. Yet, *The Bad Boys of Brexit* does not mention the company again after the press conference. Is this a strategic silence? The answer seems to be less nefarious. Banks later claimed:

Leave.EU did not receive any data or work from Cambridge Analytica. UKIP did give Cambridge Analytica some of its data and Cambridge Analytica did some analysis of this. But it was not used in the Brexit campaign. Cambridge Analytica tried to make me pay for that work but I refused. (Hern, 2019)

According to journalistic information, Banks paid UKIP for the data, but the money was never passed on to Cambridge Analytica (Hern, 2019). The ICO investigation into the use of data analytics states: “Based on our

enquiries, testimony and interviews, we conclude that this is indeed the case—there is no evidence of a working relationship between CA and Leave.EU proceeding beyond this initial phase” (ICO, 2018, p. 44). In 2020, the ICO closed the case after checking further evidence and re-iterated that Cambridge Analytica was *not* involved in the Brexit referendum (“Cambridge Analytica ‘not involved,’” 2020).

What about the connections between the official Leave campaign Vote Leave and Cambridge Analytica? Cambridge University employee Dr. Kogan and his company Global Science Research had illegally harvested the data of more than 80 million people worldwide, without their knowledge, and later shared a subset of this data with other organisations, including Cambridge Analytica (ICO, 2018, p. 39). Of these 80 million people, at least one million were UK citizens (ICO, 2018, p. 39). Did Cambridge Analytica share this data with Vote Leave? The way this could have happened was indirectly through the company AIQ. Whistle-blower Chris Wylie argued that AIQ and Cambridge Analytica were basically the same thing (Cadwalladr & Townsend, 2018). And AIQ was paid about £3.5 million by pro-Brexit campaign organisations, of which £2.7 million came from the official campaign Vote Leave and £675,000 from BeLeave (Baraniuk, 2018). Still, the ICO (2018, p. 42) investigation concluded that:

The relationship between AIQ and SCLE was a contractual one; AIQ supplied services as outlined above for work on US campaigns....To date, we have no evidence that SCLE and CA [Cambridge Analytica] were involved in any data analytics work with the EU referendum campaigns.

The DCMSC parliamentary report on fake news and disinformation, which was published a year later, in 2019, was more sceptical and argued that “there seems to be more to the AIQ/Cambridge Analytica/SCL relationship than is usually seen in a strictly contractual relationship” (DCMSC, 2019, Section 192). The DCMSC report inferred (but could not prove) a direct link between AIQ’s work and the data scraped by Cambridge Analytica: “Data matching Dr Kogan’s was found in the data used by AIQ’s Leave campaign audience files. Facebook believe that this is a coincidence, or, in the words of Mike Schroepfer, CTO of Facebook, an ‘effectively random chance’ ” (DCMSC, 2019, Section 175). Beyond this information, there has been no other evidence of sharing data between AIQ and Cambridge Analytica.

Certainly, AIQ “handled, collected, stored and shared UK citizen data, in the context of their work on the EU referendum” (DCMSC, 2019, Section 170), but considering that they were hired to do precisely this work, this is not surprising. The ICO also confirmed that AIQ had access to the personal data of UK voters, but the data was “given by the Vote Leave campaign” (ICO, 2018, p. 50), not by Cambridge Analytica. In addition, Facebook told

the UK Electoral Commission in May 2018 that “AIQ had made use of data file custom audiences—enabling AIQ to reach existing customers on Facebook or to reach users on Facebook who were not existing customers—website custom audiences and lookalike audiences” (DCMSC, 2019, Section 173). All in all, it seems that AIQ counted on data provided by Vote Leave, as well as custom audiences data. Conclusive evidence about Cambridge Analytica sharing data with AIQ is missing.

Ultimately, while both Leave.EU and Vote Leave undoubtedly had some connections with Cambridge Analytica, the company did not play the key role in the Brexit referendum that it is still often assumed to have played. Nevertheless, the focus on the role of Cambridge Analytica in some digital communications academic research has distracted attention away from other more mundane, but still highly problematic, data practices that were discovered in the campaigns and had significant negative consequences for the democratic process. I outline some of these practices in the following section.

4. Selling Data, Buying Data: Political Parties (Mis)Using Party Data for the 2016 Referendum Campaigning

UKIP’s cooperation with Cambridge Analytica failed in the long run. But the process was fraught with problems already at an early stage. Data of UKIP party members was shared with a third party—Arron Banks as representing the Leave.EU campaign, who passed it on to Cambridge Analytica (even if not hiring them in the end), without any public accountability by UKIP and without any opportunity for party members to exercise control over the process.

Furthermore, the misconduct Leave.EU and Arron Banks were actually fined by the ICO was much more trivial than the Cambridge Analytica suspicions and yet highly indicative. The ICO announced its intent to fine Leave.EU and Arron Banks’s company Eldon Insurance each with £60,000, since more than a million Leave.EU subscribers received ads for Eldon’s insurance products, without consent. [Leave.EU](#) was to be fined an extra £15,000 for sending 300,000 emails with a Leave.EU newsletter to Eldon customers (ICO, 2018, pp. 44–49). This mixing of public and private business interests and political campaigning was made possible by the fact that the Leave.EU campaign was run as a private “bad boys club” of several businessmen, (Richard Tice and Arron Banks being the most prominent) who united forces with UKIP’s Nigel Farage (Banks, 2017; UK in a Changing Europe, 2020). Citizens who supported Leave.EU had their data used for advertising purposes by a private insurance company, with no knowledge or say over how their data was used.

Lack of accountability and undemocratic handling of data were problems encountered not only on the Leave side of the campaign. In 2018, the ICO report stated

that they had obtained information that the Liberal Democrats (LibDems) had sold the personal data of their party members to the Britain Stronger in Europe campaign for approximately £100,000 (ICO, 2018, p. 54). In response to the ICO's information notice, the LibDems and Open Britain (Britain Stronger in Europe changed its name after the referendum, in August 2016, to Open Britain) both argued that there was no wrongdoing and that the Remain campaign had bought electoral register information from the LibDems, enhanced by a third-party group with emails and phone numbers (ICO, 2018, pp. 54–55). This deal is even more interesting in light of the difficulty of obtaining voter data in the UK shared by political party representatives in relation to the 2015 elections, preceding the 2016 Brexit referendum campaign (Anstead, 2017)

A year later, on November 13, 2019, the progressive news outlet *Open Democracy* published a piece in which they argued that the ICO had new information on the case and was investigating further. ICO was concerned about why a simple enhancement of publicly available data would cost £100,000 (Cusick, 2019a). Once the *Open Democracy* article was published, the LibDems wrote to the media outlet to question why they had not been given the opportunity to comment. *Open Democracy* responded they had requested a comment, but the party had not replied. Two days later, the expensive legal firm Goodman Derrick sent *Open Democracy* a letter in which they required all derogatory content to be removed or the whole article taken down at the threat of legal action (Fitzgerald, 2019). After *Open Democracy* refused to comply since they had followed standard journalistic practice, an undisclosed employee from the LibDem office sent a forged email containing the supposed comment by the party.

Ultimately, a scandal ensued, and the LibDems fired a member of staff over the forged email, without providing clarity over the key question: What type of data had they sold to Britain Stronger in Europe? A follow-up investigation by Cusick (2019b) claimed that Tim Gordon, chief executive of the LibDems, supervised the data services sale and “is understood to have privately explained to colleagues that the data sale could be seen as sensitive and controversial, and so steps were taken to minimise the article trail for the deal.” While it is still unclear what exact data was sold for £100,000 and how it was enhanced, not only was there no transparency on the issue but there was also no chance for LibDem party members to influence this decision. Both the Leave.EU and the Britain Stronger in Europe cases are symptomatic for the UK context, where campaigners struggled to find relevant data during the campaigns, resorting to buying political party data without consulting voters' opinions on this. Still, the most dramatic example of the clash between top-down control of data and bottom-up mobilisation could be seen in the collapse of the People's Vote campaign, which mobilised only in the aftermath of the referendum.

5. The Collapse of the People's Vote Campaign: A Four-Dimensional Chess Game?

As already mentioned above, the Britain Stronger in Europe campaign was re-launched after the 2016 referendum as Open Britain. Crucially, Open Britain kept control of the data of Britain Stronger in Europe. The chairman of the board of Open Britain was Roland Rudd, founder and head of the Finsbury public relations company, as well as the brother of conservative politician Amber Rudd. Open Britain was initially not against Brexit but mainly wanted to keep the UK in the single market. After Theresa May's poor performance at the 2017 general elections, though, activists pushed for a more resolute position, and different Remain groups united forces (Mance, 2020). This is how the People's Vote campaign started with the aim of promoting a second referendum.

At the suggestion of Alastair Campbell, former spokesman of Tony Blair, Tom Baldwin, another former Labour party adviser, joined the campaign as director of communications (UK in a Changing Europe, 2021). Baldwin and the director of Open Britain, James McGrory, tried to bring together the different Remain groups in the People's Vote campaign, an experience Baldwin described as “building an aeroplane as you are taking off; there are bits falling off and you are going very, very fast” (UK in a Changing Europe, 2021). The campaign's focus, according to Baldwin, was to get a second referendum. People's Vote became one of the most successful political campaigns in British history, organising marches for a People's Vote that were attended by hundreds of thousands of people and raising £100,000 a week in small donations (Sabbagh, 2019).

As the political crisis deepened and a second referendum started to seem increasingly probable, McGrory and Baldwin felt that the organisational structure of the People's Vote campaign was inadequate. Baldwin decried “a lot of pride and angst and placeholding from people like Roland Rudd” (UK in a Changing Europe, 2021). Frustrated with Rudd's lack of meaningful engagement and desire to appoint friends at high positions, campaign members decided to move against him (UK in a Changing Europe, 2021). In October 2019, the *Daily Mail* published an article entitled “Alastair Campbell and Peter Mandelson use dark arts to try to seize control of the second referendum campaign and topple its multi-millionaire boss Roland Rudd” (Owen, 2019). The scoop was made possible because one of the plotters forwarded the email by mistake to Rudd himself (Owen, 2019).

In what ensued, Rudd moved first, took control over all the data and finances of the People's Vote campaign through his position in Open Britain, and sacked McGrory and Baldwin, thus paralysing the whole campaign. According to Rudd, the campaign was not run well enough: “We needed to do more to focus on digital and data operations, which had been hugely neglected” (Mance, 2020). The rank-and-file staff of the campaign, many of whom worked on a minimum London

living wage, walked out in protest against the decision and were threatened with legal action (Mance, 2020; Sabbagh, 2019). The campaign imploded, with staff using the campaign's Facebook and Twitter accounts to attack Rudd's coup. Ultimately, Rudd kept control over the campaign (and over all the supporters' data), even though he was forced to step down a month later due to the public controversy, leaving the position to a trusted figure (Mance, 2020).

In December 2019, the People's Vote campaign asked the Electoral Commission to investigate it over donations received during the time it was run by McGrory and Baldwin. The right-wing pro-Brexit political commentary website Guido Fawkes (2019) called this development in which the campaign itself asked to be investigated a "four-dimensional-chess move no one saw coming." This comment, pro-Leave bias notwithstanding, provides a good summary of the dramatic infighting in the People's Vote campaign that took place in front of the public, but with no involvement of the public. The hundreds of thousands of people who marched on the streets, the 500,000 registered supporters of the campaign who had provided their data, the staff itself—none of those participants in the People's Vote had any influence over how their data, donations, and enthusiasm would be used. The People's Vote campaign has recently re-branded itself as "Democracy Unleashed," with citizens' data treated as a valuable resource that could be reused again.

While the People's Vote was certainly digitally savvy, its use of "data-driven campaigning" was, according to both Baldwin and Rudd, not intensive. This is very much in line with Craig Oliver's book *Unleashing Demons* on the earlier Britain Stronger in Europe campaign, which mentions the word "digital" only 8 times in 408 pages (Oliver, 2017). The fact that Rudd got proof of the plot to oust him after an email was forwarded by mistake also shows that far from the highly scientific digital sophistication we expect from modern-day campaigning, most of it is still human, complicated, and messy. Again, the key data story of this campaign was the appropriation of campaign supporters' data by the head of a PR relations company. It is this type of non-democratic attitude that seamlessly merges business interests and political causes that was shared by the otherwise very different campaigns Leave.EU, Vote Leave, Britain Stronger in Europe, and People's Vote.

6. Regulatory Calls: Participation Over Time as a Missing Aspect

As official investigations of malpractices during the Brexit referendum were taking place, regulators started consultations on how to update (or even overhaul) existing regulations. A particularly relevant example for the purposes of this article is the 2019 ICO public consultation on a code of practice for using personal data in political campaigning. A number of academics also joined public debates on regulating data-driven campaigning. Margetts and

Dommett (2020, pp. 747, 749–750), for example, have recommended not only "a wholesale rewriting of electoral law," but also more coordination between key regulators, platforms expanding and regularising "their efforts towards transparency" and developing "systems for accountability and over-sight," and a "public awareness campaign to enable citizens to understand and scrutinise electoral processes and be able to navigate the landscape of political information both outside and during election periods." Importantly, Rowbottom (2020) drew attention to the need to update and harmonise legislation on third-party campaigners, understood as actors different from parties and candidates. Campaigns such as the People's Vote discussed above are a good example of such type of a "third-party campaigner" that has, in many respects, fallen through the cracks of existing legislation.

Academics have also been critical of some of the recommendations of existing regulators: Dommett (2020) observed that a key recommendation of all official investigations on the Brexit referendum was to increase transparency. Such demands, however, were often too general and did not specify the "type of transparency sought, or the form transparency should take" (Dommett, 2020, p. 433). There was often little detail on whether regulators meant *funding transparency* (who funded the campaign), *source transparency* (what is the source of campaign material), *data transparency* (what data is accessed and how it is being used), or *targeting transparency* (who is being targeted and why; Dommett, 2020). It was equally unclear what exact information should be published, in what format, how it should be made legible to citizens, etc. By not defining what they mean by transparency, regulators basically allowed companies such as Facebook to decide themselves what information they should disclose as well as how easy it is to discover, process, and understand (Dommett, 2020). At the same time, Shiner (2019, p. 14) argued that the focus on a few bad players, such as corporate and foreign actors using micro-targeting, overlooks the fact that "there would be no market for these techniques if politics did not invest in them." Shiner (2019, p. 13) rightly noted that:

The more fundamental issues do not relate to closing regulatory gaps but ensuring the political ecosystem balances out more fairly and imbues democratic principles like fairness and transparency which can help futureproof legal reforms. It seems that the scandal around data misuse for political purposes has served as an illustration of the huge distance between those elected to represent and those being represented—with companies exploiting that gap for profit.

While agreeing with the analyses and recommendations of all scholars mentioned above, this article argues first, that few of them raise the question of data-use by campaigners *after* a campaign (with the exception of Rowbottom, 2020). What happens with data after a referendum is over? For how long should data be

kept? Could it be re-used? In the cases analysed in this article, problematic data practices were associated with sharing election data with third-party referendum campaigners (UKIP and the LibDems both sold data to third parties), or with referendum campaigners continuing to use data even after a concrete campaign was over (the transformation of People's Vote to Democracy Unleashed case). As a result of the publicity around Brexit, some guidance on this issue in the UK context has been developed. The ICO's *Guidance for the Use of Personal Data in Political Campaigning*, published after the 2019 public consultation, has a special section titled "After a Campaign," which addresses questions such as "can we use personal data from one campaign to another?" Among the key considerations are "whether the personal data is necessary for future campaigns," "whether it would be in individuals' reasonable expectations that you keep the data," "what you told individuals at the point of collection," "whether the nature of future campaigns could amount to processing for a different purpose (e.g., a referendum campaign on EU membership to a local election)," "how long you have retained the data and whether it is still adequate, relevant or accurate," and "whether you are able to keep the data securely and whether keeping the data creates any unjustifiable risk of it being subject to unauthorised disclosure" (ICO Guidance, 2022, p. 73). The ICO also clearly states that if an organisation is disbanding, personal data should not be shared with other controllers unless this is done "in accordance with data protection law" (ICO Guidance, 2022, p. 74). One key problem with the ICO guidance is that it does not introduce new obligations or responsibilities but mainly establishes a code of practice, which is generally non-binding and cannot ensure compliance (Shiner, 2019, p. 18).

Furthermore, the ICO guidance leaves all decision-making to parties and data controllers as key actors. As discussed above, these actors are encouraged to be transparent so that they could be held accountable. This article's second main theoretical argument is that the focus on transparency (on the part of both regulators and academics studying them), no matter how finely defined, has overlooked the political and institutional failures of Brexit-related campaigning as related not only to data protection but also as *democratic* failures. In their study of citizens' demands for transparency in European trade policy, Gheyle and de Ville (2017) argued that the European Commission has interpreted calls for transparency as calls for more information, but what activists actually demanded was more participation. Focusing on public participation might help address the gap between politicians and their electorate that Shiner (2019) rightly identifies as a core problem traversing the ecosystem of political communication. And it is precisely this focus on participation that has been notoriously absent from most discussions on the data practices of Brexit-related campaigns, in particular, but also of data-driven campaigning, more generally.

To be sure, there have been substantial critiques of the model of data protection embodied in the European Union's General Data Protection Regulation (GDPR), for example, which is widely held as a high standard for data protection. The GDPR has placed too much weight on transparency, accountability, and fairness as mechanisms of protecting rights understood above all as individual rights. Authors have argued instead for the need for systemic regulation or thinking about rights as collective, especially considering that often the harms addressed are of collective character (Cobbe, 2021; Mayer-Schonberger, 2010). Furthermore, as research on voter attitudes to data-driven campaigning in Australia has shown (Kefford, 2021), a significant number of voters have felt highly uncomfortable with political parties acquiring information about them from financial entities, companies they buy things from, or social media platforms. Such feelings of discomfort could hardly be assuaged by more transparency but would require a fundamental change of practice.

Including the public in decision-making over what type of data should be collected on them, for how long and whom it should be shared with could be a good way to guarantee public trust in elections as a foundational element of democratic systems. Indeed, as Rowe and Frewer (2000, p. 5) note, among the chief reasons for the rise in interest in public participation in technical policy matters are "a recognition of basic human rights regarding democracy and procedural justice," but also the "practical recognition that implementing unpopular policies may result in widespread protest and reduced trust in governing bodies." Extending this argument further, one could argue for ensuring mechanisms of ownership and management of voters' data that give more power to individuals or collective bodies of voters. Referenda, public inquiries, surveys, negotiated rulemaking, citizens' jury panels, advisory committees, and focus groups have all been experimented with to foster public participation. Each of these participatory practices comes with its own benefits and problems (Rowe & Frewer, 2000, pp. 8–9). Furthermore, party members, for example, could vote on how their own party should manage their data. Alternatively, there could be voters' data governance bodies (the same way we have authors' rights representative bodies) that allow their members to decide what uses of their data they agree with in the context of political campaigning. Recent years have seen the rise of innovative research on alternative regimes of data ownership and governance, placing emphasis on collective data ownership and/or giving more power to individuals vis-à-vis private companies (Fischli, 2022; Mills, 2019; Mukhametov, 2021; Muldoon, 2022; Singh & Vipra, 2019). But such innovative research has rarely focused on data used in political campaigns by political parties or third-party actors, not to mention cases in which political campaigns obtain and merge voter data from public registries and private corporations. While not aiming to resolve these questions, this article has the

more modest ambition of raising them, especially in light of the analysis of the Brexit referendum campaign.

Of course, participation is not a panacea. Four important objections could be raised to the proposal for more public participation in decision-making on campaign data. First of all, even completely bottom-up democratic movements such as the Spanish Indignados witnessed a lot of misuse of data, internal quarrels, trolling, and appropriation of citizens' information (Rone, 2019). Second, a focus on voters' participation in decision-making over their own data would be a substantial departure from current legally established mechanisms of accountability in key documents such as GDPR. While there have been critics arguing that "data protection doesn't work" (Cobbe, 2021), novel proposals with alternatives to the current data protection regime are still scarce. Third, the concept of participation is not less ambiguous or imprecise than transparency, for example. In his seminal text "Too Much Democracy in All the Wrong Places," Kelty (2017, pp. 86–87) has emphasised how participation has been interpreted in multiple ways depending on changing historical contexts:

Participation is always aspirational. One might say it wavers back and forth between two moods: optative and critical. In the optative mood, it signals an enthusiasm, a normativity, a happy hypothesis of change through the involvement of more people rather than fewer, poorer rather than richer, rural rather than urban, indigenous rather than colonial, or everyday experience rather than rarefied expertise. But in a critical mood, what is called participation becomes a false claimant: phony participation. By accusing participation of being false, phony, exploitative, or disappointed, it allows the optative mood in the next turn of phrase—a better, more authentic participation yet to come.

Participation thus presents itself as much as a challenge as a solution. More recently, we have seen rising concerns over "participation washing" in relation to technology design (Sloane et al., 2020). Finally, even if all these concerns can be addressed, it remains far from certain political parties would support changes to campaigning that facilitate voter participation in decision-making over the use of their data. As Bennett (2022) has shown in the Canadian context, political parties have acted as a cartel to prevent even basic data privacy legislation extending to them. There is every reason to believe political parties in various national contexts would resist more changes that encourage participation and give more power and voice to voters to decide how their data would be used in election campaigns.

7. Conclusion

To conclude, beyond dramatic tales of disinformation and micro-targeting, Brexit-related data-driven cam-

paingning was marked by several problematic undemocratic practices of sharing data with third parties and reusing data without any consent or input from the public. Despite the use of crowd-funding and active citizen involvement, neither the ownership of data nor its management were democratic in any sense of the word. The "people's data" was the domain not of people but of parties doing deals with campaigns run by businessmen.

Questionable data practices are a symptom of a broader lack of accountability and participation in increasingly professionalised campaigning in the UK, very different from bottom-up protest movements observed during the 2010s protest wave in Europe (Rone, 2022). Still, demands for citizen democratic participation in data ownership and governance (both during and after campaigns) are not a panacea. Such demands open all kinds of additional challenges that need to be carefully thought through and addressed. What this analysis has aimed to show is simply that, so far, citizen participation in data ownership and governance has remained a non-issue in both debates on Brexit-related campaigning and beyond. Yet, increasing participation might be an important way to address current malpractices in data-driven campaigning that involve not only a few bad actors but the political ecosystem as a whole.

Acknowledgments

I would like to thank the anonymous reviewers of this article for all their constructive comments and suggestions, including pointing out the importance of what happens to data in the aftermath of campaigns. Thanks also for all the useful comments that I received during the Open Lab Session, organised by the Minderoo Centre for Technology and Democracy, where I presented a draft version of this article.

Conflict of Interests

The author declares no conflict of interests.

References

- Anstead, N. (2017). Data-driven campaigning in the 2015 United Kingdom general election. *The International Journal of Press/Politics*, 22(3), 294–313.
- Anstead, N. (2018). Data and election campaigning. *Political Insight*, 9(2), 32–35. <https://doi.org/10.1177/2041905818779333>
- Baldwin-Philippi, J. (2017). The myths of data-driven campaigning. *Political Communication*, 34(4), 627–633.
- Banks, A. (2017). *The bad boys of Brexit: Tales of mischief, mayhem & guerilla warfare in the EU referendum campaign*. Biteback Publishing.
- Baraniuk, C. (2018, September 20). Vote Leave data firm hit with first ever GDPR notice. *BBC*. <https://www.bbc.com/news/technology-45589004>
- Cambridge Analytica "not involved" in Brexit referen-

- dum, says watchdog. (2020, October 7). *BBC*. <https://www.bbc.com/news/uk-politics-54457407>
- Bennett, C. (2022, March 31–April 1). *Privacy, profiling and federal political parties: The extent and limits of the “party cartel”* [Paper presentation]. Les D efis de la D emocratie des Donn ees, Laval, Canada.
- Bennett, C. J., & Lyon, D. (2019). Data-driven elections: Implications and challenges for democratic societies. *Internet Policy Review*, 8(4). <https://doi.org/10.14763/2019.4.1433>
- Borgesius, Z. F. J., M oller, J., Kruike-meier, S.,   Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, 14(1), 82–96.
- Br ndle, V. K., Galpin, C., & Trenz, H.-J. (2018). Marching for Europe? Enacting European citizenship as justice during Brexit. *Citizenship Studies*, 22(8), 810–828.
- Br ndle, V. K., Galpin, C., & Trenz, H.-J. (2022). Brexit as “politics of division”: Social media campaigning after the referendum. *Social Movement Studies*, 21(1/2), 234–253.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
- Cadwalladr, C. (2017, May 7). The great British Brexit robbery: How our democracy was hijacked. *The Guardian*. <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexite-robbery-hijacked-democracy>
- Cadwalladr, C., & Townsend, M. (2018, March 24). Revealed: The ties that bound Vote Leave’s data firm to controversial Cambridge Analytica. *The Guardian*. <https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions>
- Chadwick, A., & Stromer-Galley, J. (2016). Digital media, power, and democracy in parties and election campaigns: Party decline or party renewal? *The International Journal of Press/Politics*, 21(3), 283–293.
- Cobbe, J. (2021, July 5). *Data protection doesn’t work: Oversight failure in data processing figurations* [Paper presentation]. Minderoo Centre for Technology and Democracy Seminar, Cambridge, UK.
- Cusick, J. (2019a, November 13). New evidence that LibDems sold voter data for  100,000 held back till after election. *Open Democracy*. <https://www.opendemocracy.net/en/dark-money-investigations/new-evidence-that-libdems-sold-voter-data-for-100000-held-back-till-after-election>
- Cusick, J. (2019b, December 6). Breaking: Lib Dems admit they added information about voters in  100 k data sale. *Open Democracy*. <https://www.opendemocracy.net/en/opendemocracyuk/breaking-libdems-admit-they-added-information-about-voters-in-100k-data-sale>
- Digital, Culture, Media and Sport Committee. (2019). *Disinformation and “fake news.”* <https://publications.parliament.uk/pa/cm201719/cmselect/cmcomeds/1791/1791.pdf>
- Dommett, K. (2020). Regulating digital campaigning: The need for precision in calls for transparency. *Policy and Internet*, 12(4), 432–449.
- Factiva. (2023). *Search summary: Text “Cambridge Analytica”; date “01/01/2015–31/12/2022”; region “United Kingdom”; language “English”; results found “13,989”.*
- Fischli, R. (2022). Data-owning democracy: Citizen empowerment through data ownership. *European Journal of Political Theory*. Advance online publication. <https://doi.org/10.1177/14748851221110316>
- Fitzgerald, M. (2019, December 1). What are Jo Swinson’s Liberal Democrats so desperate to hide? *Open Democracy*. <https://www.opendemocracy.net/en/opendemocracyuk/what-are-jo-swinsons-liberal-democrats-so-desperate-to-hide>
- Gheyle, N., & Ville, F. (2017). How much is enough? Explaining the continuous transparency conflict in TTIP. *Politics and Governance*, 5(3), 16–28.
- Guido Fawkes. (2019). *People’s Vote campaign ask electoral commission to investigate themselves*. <https://order-order.com/2019/12/06/peoples-vote-campaign-ask-electoral-commission-investigate>
- H nska, M., & Bauchowitz, S. (2017). Tweeting for Brexit: How social media influenced the referendum. In J. Mair, T. Clark, N. Fowler, R. Snoddy, & R. Tait (Eds.), *Brexit, Trump and the media* (pp. 31–35). Abramis Academic Publishing.
- Hern, A. (2019, July 30). Cambridge Analytica did work for Leave.EU, emails confirm. *The Guardian*. <https://www.theguardian.com/uk-news/2019/jul/30/cambridge-analytica-did-work-for-leave-eu-emails-confirm>
- Hersh, E. (2015). *Hacking the electorate: How campaigns perceive voters*. Cambridge University Press.
- Howard, P. N. (2005). Deep democracy, thin citizenship: The impact of digital media in political campaign strategy. *The Annals of the American Academy of Political and Social Science*, 597, 153–170. <http://www.jstor.org/stable/25046067>
- ICO Guidance. (2022). *Guidance for the use of personal data in political campaigning*. <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-for-the-use-of-personal-data-in-political-campaigning-1>
- Information Commissioner’s Office. (2018). *Investigation into the use of data analytics in political campaigns: A report to Parliament 6 November 2018*. <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>
- Kefford, G. (2021). *Political parties and campaigning in Australia*. Palgrave Macmillan.
- Kefford, G., Dommett, K., Baldwin-Philippi, J., Bannerman, S., Dobber, T., Kruschinski, S., Kruike-meier, S., & Rzepecki, E. (2022). Data-driven campaigning and

- democratic disruption: Evidence from six advanced democracies. *Party Politics*. Advance online publication. <https://doi.org/10.1177/13540688221084039>
- Kelty, C. (2017). Too much democracy in all the wrong places: Toward a grammar of participation. *Current Anthropology*, 58(S15), 77–90.
- Kruschinski, S., & Haller, A. (2017). Restrictions on data-driven political micro-targeting in Germany. *Internet Policy Review*, 6(4). <https://doi.org/10.14763/2017.4.780>
- Mance, H. (2020, August 7). How the People’s Vote fell apart. *Financial Times*. <https://www.ft.com/content/e02992f6-cf9e-46b3-8d45-325fb183302f>
- Margetts, H., & Dommett, K. (2020). Conclusion: Four recommendations to improve digital electoral oversight in the UK. *Political Quarterly*, 91(4), 745–750.
- Markussen, H. (2022). After Cambridge Analytica: Rethinking surveillance in the age of (com)modification. In H. B. Jaffel & S. Larsson (Eds.), *Problematising intelligence studies: Towards a new research agenda* (pp. 201–219). Routledge.
- Mayer-Schonberger, V. (2010). Beyond privacy, beyond rights—Toward a “systems” theory of information governance. *California Law Review*, 98, 1853–1885.
- Mills, S. (2019). *Who owns the future? Data Trusts, Data Commons, and the future of data ownership*. SSRN. <https://doi.org/10.2139/ssrn.3437936>
- Montigny, E., Dubois, P., & Giasson, T. (2019). On the edge of glory (...or catastrophe): Regulation, transparency and party democracy in data-driven campaigning in Québec. *Internet Policy Review*, 8(4). <https://doi.org/10.14763/2019.4.1441>
- Mukhametov, D. R. (2021). Collective data governance for development of digital government. In *2021 International Conference on Engineering Management of Communication and Technology (EMCTECH)* (pp. 1–5). Institute of Electrical and Electronics Engineers.
- Muldoon, J. (2022). *Platform socialism: How to reclaim our digital future from big tech*. Pluto Press.
- Oliver, C. (2017). *Unleashing demons: The bestselling inside story of Brexit*. Hodder.
- Ortega Martín, D., & Sánchez Berrocal, A. (2022). Nobody can trust or believe anything: Brexit, populism and digital politics. *Dilemata*, 38, 83–102.
- Owen, G. (2019, October 19). People’s Vote coup plotters: Alastair Campbell and Peter Mandelson use dark arts to try to seize control of the second referendum campaign and topple its multi-millionaire boss Roland Rudd. *Daily Mail*. <https://www.dailymail.co.uk/news/article-7592265/Alastair-Campbell-Peter-Mandelson-use-dark-arts-try-seize-control-referendum-campaign.html>
- Quick, K., & Bryson, J. (2016). Public participation. In C. Ansell & J. Torfing (Eds.), *Handbook on theories of governance* (pp. 159–168). Edward Elgar.
- Risso, L. (2018). Harvesting your soul? Cambridge Analytica and Brexit. In C. Jansohn (Ed.), *Brexit means Brexit? The selected proceedings of the symposium, Akademie der Wissenschaften und der Literatur, Mainz 6–8 December 2017* (pp. 75–87). Akademie der Wissenschaften und der Literatur.
- Rone, J. (2019). Fake profiles, trolls, and digital paranoia: Digital media practices in breaking the Indignados movement. *Social Movement Studies*, 21(1/2), 25–41.
- Rone, J. (2022). Instrumentalising sovereignty claims in British pro- and anti-Brexit mobilisations. *The British Journal of Politics and International Relations*. Advance online publication. <https://doi.org/10.1177/13691481221089136>
- Rowbottom, J. (2020). The regulation of third party campaigning in UK Elections. *Political Quarterly*, 91(4), 722–730.
- Rowe, G., & Frewer, L. (2000). Public participation methods: A framework for evaluation. *Science Technology Human Values*, 25(1), 3–29.
- Sabbagh, D. (2019, November 20). How People’s Vote collapsed after Roland Rudd’s boardroom coup. *The Guardian*. <https://www.theguardian.com/politics/2019/nov/20/how-peoples-vote-collapsed-after-roland-rudds-boardroom-coup>
- Shiner, B. (2019). Big data, small law: How gaps in regulation are affecting political campaigning methods and the need for fundamental reform. *Public Law*, 2019(2), 362–379.
- Simon, F. M. (2019). “We power democracy”: Exploring the promises of the political data analytics industry. *The Information Society*, 35(3), 158–169. <https://doi.org/10.1080/01972243.2019.1582570>
- Singh, P. J., & Vipra, J. (2019). Economic rights over data: A framework for community data ownership. *Development*, 62, 53–57. <https://doi.org/10.1057/s41301-019-00212-5>
- Sloane, M., Moss, E., Awomolo, O., & Forlano, L. (2020). *Participation is not a design fix for machine learning*. ArXiv. <https://doi.org/10.48550/arXiv.2007.02423>
- Smith, L. G. (1983). *Impact assessment and sustainable resource management*. Longman.
- Stromer-Galley, J. (2019). Introduction: The paradox of digital campaigning in a democracy. In J. Stromer-Galley (Ed.), *Presidential campaigning in the internet age* (2nd ed., pp. 14–20). Oxford University Press.
- Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*, 19(7). <https://doi.org/10.5210/fm.v19i7.4901>
- UK in a Changing Europe. (2020). *Brexit interview: Richard Tice*. <https://ukandeu.ac.uk/interview-pdf/?personid=42575>
- UK in a Changing Europe. (2021). *Brexit witness archive—Tom Baldwin*. <https://ukandeu.ac.uk/brexit-witness-archive/tom-baldwin>
- Udris, L., & Eisenegger, M. (2023). Referendum campaigns in the digital age: Towards (more) comparative analyses in hybrid media systems. *Media and Communication*, 11(1), 1–5.
- Ulbricht, L. (2020). Scraping the demos: Digitalization, web scraping and the democratic project. *Democratization*, 27(3), 426–442.

About the Author



Julia Rone is a postdoctoral researcher at the Minderoo Centre for Technology and Democracy at the Centre for Research in the Arts, Social Sciences and Humanities (CRASSH), University of Cambridge. Her research focuses on the dilemmas of digital sovereignty and the democratisation of trade and tech governance. She is the author of *Contesting Free Trade and Austerity in the EU: Protest Diffusion in Complex Media and Political Arenas* (Routledge, 2021).