frontiers in Communication

ORIGINAL RESEARCH
published: 03 September 2020
doi: 10.3389/fcomm.2020.00067

Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting

*Vian Bakir**

School of Languages, Literatures, Linguistics and Media, Bangor University, Bangor, United Kingdom

This paper explores whether psychographic profiling and targeting married with big data and deployed in digital political campaigns is a form of psychological operations ("psy-ops"). Informed by studies on deception, coercion, and influence activities from propaganda, persuasion, policy making, cognitive psychology, information, and marketing scholarship, this proposition is examined and historically grounded in a politically important case study: the actions of now defunct political data analytics and behaviour change company, Cambridge Analytica, in the UK's 2016 referendum campaign on leaving the European Union. Based on qualitative analysis of documentation in the UK and USA from public inquiries, regulatory investigations, legal proceedings, and investigative journalists, as well as on revelations from digital political campaigners and Cambridge Analytica itself, this paper assesses the coercive and deceptive nature of Cambridge Analytica's psychographic profiling and targeting, concluding that it is a form of psy-ops. Observing the social unacceptability of such digital campaigning practices (ascertained from national surveys in the US, UK, and globally), this paper discusses the adequacy of measures since put in place to eliminate the risk of further psy-ops in digital political campaigning. It ends by elucidating areas in urgent need of further research.

Keywords: deception, coercion, influence activities, digital political campaign, psychographics, profiling, targeting, psychological operations

OPEN ACCESS

Edited by:
Tanner Mirrlees,
Ontario Tech University, Canada

Reviewed by:
Yik Chan Chin,
Xi'an Jiaotong-Liverpool University, China
Michael D. High,
Xi'an Jiaotong-Liverpool University, China

***Correspondence:**
Vian Bakir
v.bakir@bangor.ac.uk

Specialty section:
This article was submitted to Political Communication and Society, a section of the journal Frontiers in Communication

Received: *29 May 2020*
Accepted: *27 July 2020*
Published: *03 September 2020*

Citation:
Bakir V (2020) Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting. Front. Commun. 5:67. doi: 10.3389/fcomm.2020.00067

INTRODUCTION

The issue of psychographic profiling and targeting in political campaigning first rose to prominence with the practices of Cambridge Analytica, a now defunct political data analytics and behaviour change company. Whistleblowers from Cambridge Analytica claim that the company engaged in psychological operations ("psy-ops") in its electoral campaigning efforts across the world (Cadwalladr, 2018; Kaiser, 2019b; Wylie, 2019). This study theoretically and empirically assesses this claim. It does so by investigating whether psychographic profiling and targeting married with big data in election campaigns is a form of "psy-ops"; and by testing this proposition in a politically important case study—the actions of Cambridge Analytica in the UK's 2016 "Brexit" Referendum on leaving the European Union.

Psychographic research emerged in the 1960s, attempting to understand consumer (rather than political) behaviour, and moving beyond standard demographics into areas such as personality traits, activities, interests, opinions, needs, values, and attitudes to offer novel insights into large, representative samples of respondents (Wells, 1975). However, increasingly across the past decade, psychographic and neuromarketing tools are combined with data and tracking methods to determine the emotional impact of advertising campaigns, and how to tailor persuasive *political* messages to *profiled* audiences' psychological needs (Chester and Montgomery, 2017; Bakir and McStay, 2018, 2020). "Profiling" is defined in the European General Data Protection Regulation as: "any form of automated processing of personal data … to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements' (Privacy International, 2020). According to Cambridge Analytica's Chief Executive Officer (Alexander Nix), it is the techniques of psychographic targeting *married with big data analysis* that enable the marketer to understand the personality of people being targeted in order to tailor messages. Nix made this claim when explaining how Cambridge Analytica used such techniques in Ted Cruz's 2016 campaign to become nominated as the Republican US presidential candidate. Nix claims that big data analytics allows campaigners to know what sort of persuasive message needs to be delivered, on what issue, nuanced to what personality types, and to what group of people, or even individual, *before* the act of creating that message begins; and that addressable advertising technology further enables targeted, individualised adverts (Nix, 2016).

Psy-ops is a subset of "Information Operations" -the latter being a synonym for "information warfare," an umbrella term that encompasses psy-ops, electronic warfare, computer network operations and deception (Briant, 2015, p. 23). Simpson (1994) observes that psy-ops has long been used as a tactic of war or class struggle, as evidenced in military manuals and communist tracts. He defines psy-ops as explicitly linking mass communication with "selective application of violence (murder, sabotage, assassination, insurrection, counterinsurrection, etc.) as a means of achieving ideological, political, or military goals … through exploitation of a target audience's cultural-psychological attributes and its communication system" (Simpson, 1994, p. 11). Psy-ops, then, has a *coercive* nature in its application of *force* (violence, for Simpson). However, violence is not the only way of applying coercion: coercion can also take form in the deliberate *limitation of people's choices by making them feel or behave a certain way*. In this vein, Briant describes psy-ops as propaganda work designed to induce certain emotions and elicit certain behaviour in target audiences (Briant, 2015, p. 12–13). Under this definition, if psychographic profiling and targeting married with big data becomes coercive (for instance, by modulating people's exposure to information in ways that constrain their choices and behaviour), it would be accurate to describe it as psy-ops.

To better understand and assess the whistleblowers' claims on psy-ops, this paper situates Cambridge Analytica's actions on psychographic profiling and targeting within studies on deception, coercion, and influence activities from propaganda, persuasion, policy making, cognitive psychology, information, and marketing scholarship. This literature grapples with the question of when persuasive communication lapses into propagandistic influence and manipulation; highlights how political campaigners deploy digital marketing tools that lend themselves toward deceptive, coercive, influence activities; and discusses democratic implications. Adopting a case study methodology, this exposition is followed by an empirical examination of the coercive and deceptive nature of Cambridge Analytica's psychographic profiling and targeting. This is assessed with reference to the UK's "Brexit" referendum campaign in 2016 on leaving the European Union (EU). With recourse to published national surveys in the US, UK, and globally, the paper ends with a discussion on the social unacceptability of these practices; the adequacy of measures since put in place to address such practices; and urgent areas requiring further research.

LITERATURE REVIEW

Persuasion vs. Influence

When does persuasive communication lapse into propagandistic influence and manipulation, and when are such lapses democratically acceptable? Studies from propaganda and policy making have grappled with these questions.

The field of propaganda studies offers several integrative frameworks with criteria for distinguishing ethically and democratically legitimate persuasive communication from propaganda. The most enduring framework used is that of white, grey, and black propaganda that discusses honesty over message source (whether or not it is disguised) and truthfulness of message content (Jowett and O'Donnell, 2012). However, Bakir et al. (2019) posit that this framework, in directing attention toward deception alone, does not capture the full range of propaganda and therefore does not readily facilitate our ability to distinguish propaganda from persuasion. Addressing these deficiencies, Bakir et al. (2019) argue that persuasive communication, to avoid being propagandistic, should be guided by the principle of informed consent. This demands that three requirements be met. Firstly, sufficient information must be provided to enable informed judgments. Secondly, this information should be of a non-deceptive nature so that consent is not achieved on false premises. Thirdly, the process must not be coerced (such as through threats): rather, consent should be freely given. In short, in order to ethically persuade (rather than manipulate) people toward a particular viewpoint, the persuadee's decision should be both informed and freely chosen: each of these is disabled by *deception* and *coercion* (Bakir et al., 2019; also see Chappell, 2017).

Informed and freely chosen decisions are also disabled by *influence* activities that aim to change behaviour rather than attitudes. Influence activities are deployed for military and governmental purposes. Briant records how the British military has increasingly emphasised influence activities that combine propaganda with "deliberate manipulation of the circumstances or environment in which people act and make decisions": for instance, providing job opportunities in a country suffering from insurgencies, so that people who make bombs simply to earn

money stop making those bombs (behaviour change) but need not change their attitude toward the merits of insurgent bomb-making (Briant, 2015, p. 64). Not confined to the security state, influence activities, are also found at the heart of the British government. In the UK, the Behavioural Insight Team (or "nudge unit") was created in 2010, and by 2014 it had become a social purpose limited company (jointly owned by employees, UK Cabinet Office, and UK innovation charity Nesta). By 2020 its work spanned 31 countries in its efforts to "generate and apply behavioural insights to inform policy, improve public services and deliver results for citizens and society" (The Behavioural Insights Team, 2020).

Underpinned by insights from behavioural economics and cognitive psychology, a nudge is: "any aspect of the choice architecture that alters people's behaviour in a predictable way, without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid" (Thaler and Sunstein, 2008, p. 6). Mols et al. (2015, p. 84) reserve the term "nudge" for interventions that tap into psychological human failings that lead people to fall back on automatic rather than systematic information-processing strategies and decision making: for instance, tapping into people's propensity to choose options that demand the least effort, or to conform to prevailing group norms. An example of nudging is Facebook's get-out-the-vote button, first used in the USA in 2008 and in the UK in the 2014 Scottish referendum, and used repeatedly since in elections and referenda in these and other countries (Grassegger, 2018). This nudge to vote (a single message displayed in the user's Facebook feed on election day that encouraged the user to vote, provided a link to find local polling places, showed a clickable button reading "I Voted," and showed a counter indicating how many other Facebook users had reported voting) can be easily disregarded by Facebook users, but according to Facebook's own studies, is effective in slightly increasing voter turnout. Facebook's US-based experimentation on the format of the nudge finds that it is most effective when this voting message includes not just information reminding the user to vote, but also a "social message" with the profile pictures of up to six randomly selected Facebook friends who had clicked the "I voted" button; furthermore, such messages from "close" friends on Facebook were by far the most effective (Bond et al., 2012; Jones et al., 2017).

Nudging has been critiqued by scholars of public policy for various reasons (including lack of long-term effectiveness), but most relevant are critiques based on the ethical concern that nudging *precludes reflection and deliberation* by target individuals about the pros and cons of alternative courses of action (Hausman and Welch, 2010). Indeed, "nudges" are often covert attempts to trick citizens into certain behaviours. Under that reading, nudging is an "inherently elitist *choice-limiting technique*" used to achieve what those in positions of power and authority (Facebook, politicians, policy makers, and experts) consider "positive public good outcomes" (Mols et al., 2015, p. 87, emphasis added). Regardless of whether or not the outcome of the nudge is pro-social and desirable, such preclusion of reflection and deliberation, and limiting people's choices in order to change their behaviour, is coercive. Who wields this power, and to what ends, must therefore be carefully circumscribed. For instance, while Facebook's nudging experiments on its users appear to mobilise more voters, there are questions as to whether Facebook's get-out-the-vote button has unduly influenced elections. After all, there was no prior notification, and hence public discussion, that this button would appear on election day; different users are shown different versions of the message (dependent on message optimisation as well as which experimental group they are assigned to); not all voters are on Facebook, while Facebook users in certain electoral districts might disproportionately favour one party over another; and in all countries except the USA, Facebook is a foreign power and legally should not be interfering in their elections (Grassegger, 2018).

Studies from propaganda and policy making agree, then, that persuasive communication lapses into influence and manipulation when *deception* and *coercion* (via *threats*, via *limiting people's choices*, and via *preclusion of reflection and deliberation*) prevail. This results in the opinions, decisions or behaviours of target audiences being uninformed and not freely chosen. While governments argue that such actions are sometimes in the national interest and produce positive public good outcomes (ranging from less insurgency to better public services), such stances are less defensible when it comes to political campaigning, which ultimately represents a bid for power. When campaigning for votes, deploying deception and coercion and encouraging lack of reflection, and deliberation are inimical to voters freely making informed decisions about who should govern.

Political Campaigns Meet Digital Marketing Tools: The Rise of Influence Activities

Political campaigners increasingly deploy digital marketing tools that lend themselves toward influence activities, and which have, in some cases, been demonstrably used for deceptive and coercive purposes. Across the past decade, digital marketing techniques have progressively supplemented the traditional focus of political campaigning on demographic market segmentation, opinion polling, targeted campaigning, and direct marketing. Increasingly, this involves a move to big data analytics to provide automated insights using data mining techniques and tools to discover hidden patterns in datasets. Drawing on a complex and opaque corporate ecosystem encompassing data brokers and data analytics companies, political campaigns now combine public voter files with commercial information from data brokers to develop highly granular and comprehensive voter profiles (Bartlett et al., 2018; Nadler et al., 2018; Privacy International, 2020). This has enabled the rise of influence activities in digital political campaigning via the use of digital marketing tools to identify and deploy the most persuasive advert online, and to target different audiences online with tailored messages.

For instance, "A/B" testing compares two versions of a single variable, typically by testing a subject's response to variant A against variant B and determining which of the two variants is more effective. While an old technique, there has been an

exponential increase in deployment of rapid "A/B" testing using Artificial Intelligence (AI) across the past decade. The 2012 Barack Obama presidential campaign ran 500 A/B tests on their web pages which reportedly increased donation conversion by 29% and sign up conversions by 161% (Formisimo, 2016). By the 2016 presidential election, Trump's digital campaign manager claims that his team tested typically around 50,000–60,000 advert variations a day using Facebook's tool, Dynamic Creative, to find optimal combinations based on engagement metrics (Beckett, 2017; Bartlett et al., 2018, p. 33).

Other digital marketing tools deployed by political campaigners include psychographic and neuromarketing tools combined with data and tracking methods (such as emotion-based profiling) to optimise the emotional impact of advertising messages to specific audiences' psychological needs (Chester and Montgomery, 2017; Kim et al., 2018; McStay, 2018). Psychographics, emotional testing and mood measurement have long been central to political campaigns (Key, 1974; Jamieson, 1996), but the rise of big data analysis and modelling has enabled access to psychological characteristics and political inferences far beyond the reach of traditional databases (Tufekci, 2014). For instance, Kosinski et al. (2013) developed an algorithm that, based on an individual's "likes" of public Facebook pages (a fraction of data available to data brokers), could automatically and accurately predict an individual's personality traits according to the "OCEAN" scale. OCEAN is the generally accepted model of personality: its "Big Five" personality traits are Openness to experiences, Conscientiousness, Extroversion, Agreeableness, and Neuroticism (McCrae and Costa, 1987; Gosling et al., 2003). The algorithm developed by Kosinski et al. (2013) also predicts other highly sensitive personal attributes including political and religious views, sexual orientation, ethnicity, intelligence, happiness, use of addictive substances, parental separation, age, and gender. Indeed, an increasing body of research in this young field confirms that digital footprints can be used to predict the "Big Five" personality traits. This was reaffirmed in 2018 by a rigorous, multidisciplinary, meta-analysis of the predictive power of digital footprints automatically collected from social media over Big Five personality traits (Azucar et al., 2018, p. 157). The meta-analysis also shows that with the exception of agreeableness, prediction accuracy for each trait was stronger when *more than one type of digital footprint* was analysed. Caution should be applied to the conclusions of Azucar et al. (2018) as their meta-analysis analyses just 16 studies, and most of these are limited to English speaking or Chinese users. Nonetheless, such findings point to the capacity for covert behaviour change campaigns by those with access to multiple data streams by profiling individuals, and tailoring adverts automatically displayed in individual users' profiles based on personality. Indeed, it was research such as that by Kosinski et al. (2013) that attracted the attention of Cambridge Analytica (Federal Trade Commission, 2019b, p. 3).

Digital marketing tools are also used to find and target specific voters. For instance, political digital marketing firms offer "lookalike modelling" to identify potential supporters, by matching millions of voters to their email addresses, online cookies and social media handles, as well as hundreds of other data points (such as culture, religion, interests, and political positions) to create detailed voter profiles. Notably, Brad Parscale, digital director of Trump's 2016 US presidential election campaign, used Facebook's advertising platform to automatically expand the number of people the campaign could target on Facebook by identifying voters who were not Trump supporters, but had "common qualities" that "look like" known Trump supporters on Facebook (Green and Issenberg, 2016). Similarly, since 2015 UK digital campaigning has seen increasing use of data analytics and data management approaches in order to profile and identify target audiences, including "persuadables" and swing voters (The Electoral Commission, 2018, p. 4). Behavioural data is also used by politicians to target voters with tailored messages that align with their daily activities, such as hearing a radio advert about education when dropping off one's child at school (Kaiser, 2019b, p. 82). According to Kaiser, Cambridge Analytica trademarked the term "behavioural microtargeting" to describe its practice of using analytic tools to understand individuals' complex personalities; using psychologists to determine what motivates these individuals to act; and using a creative team to tailor specific messages to those personality types (Kaiser, 2019b, p. 84).

While such efforts could be democratically lauded for increasing voter engagement and turnout, and making political campaigners more responsive to what voters care about, digital political marketing tools are also used for deceptive and coercive ends. Of course, deception is a long-observed tactic deployed during election campaigns in democracies (Herbst, 2016; Perloff, 2018). However, by the second decade of the twenty-first century, *deceptive manipulation of the digital media ecology* was increasingly evidenced, to the point where it could be considered *coercive*. For instance, in 2010, software "bots" on Twitter were used in "astroturf" campaigns (where campaigners try to create the perception of an upswell of grassroots support for a cause): in US midterm elections and the Massachusetts special election, they artificially inflated support for a political candidate and smeared opponents via thousands of tweets pointing to fake news websites (Ratkiewicz et al., 2011; Metaxas and Mustafaraj, 2012). The amplification of low-credibility sources by bots is demonstrated by Shao et al. (2017) in a study of 14 million messages spreading 400,000 articles on Twitter during and following the 2016 US presidential campaign. That election also saw increased micro-targeting of messages via social media platforms, often propagating through anonymous accounts deceptive, divisive or inflammatory messages most likely to influence votes in marginal constituencies (US Intelligence Community Assessment, 2017; Bakir and McStay, 2018; Kim et al., 2018). Indeed, according to investigative journalists, Cambridge Analytica supplied Trump's 2016 presidential campaign with statistical models to isolate likely supporters to then be targeted with adverts on Facebook. Furthermore, through micro-targeting, in the final days of the 2016 campaign, Trump's team tried to suppress turnout among three groups that Hillary Clinton needed to win overwhelmingly: idealistic white liberals, young women, and African Americans (Green and Issenberg, 2016; Kaiser, 2019b, p. 84, 222, 228–229; Wylie, 2019, p, 17). Such manipulation of the digital

media ecology is *coercive (choice limiting)* where it significantly modulates what information people are exposed to, in order to make them feel or behave in a certain way.

Democratic Implications of Digital Deception, Coercion, and Influence Activities

The previous sections show that influence activities involving deception and coercion are increasingly mainstream in digital political campaigning. Psychographic profiling is also part of the mix, with claims for accurate prediction of personality with big data, and the potential for even greater profiling and optimisation of political adverts. Against this, there is scepticism about Cambridge Analytica's claims and the novelty of its targeting approach (González, 2017, p. 10–11). As with all "media effects" research, the impact of such strategies is difficult to quantify (Aral and Eckles, 2019), but efforts to establish causal links between these strategies and voting behaviour have so far concluded that impacts are minimal (Marchal, 2020). Nonetheless, several empirical research strands allow reflection on the wider democratic implications of digital influence activities involving deception and coercion.

One such empirical research strand is on algorithmic filter bubbles, where algorithms applied to online content selectively gauge what information a user wants to see based on information about the user and their digital footprints (Pariser, 2011). For instance, various studies show that rather than spreading indiscriminately through social media, conspiracies online are concentrated within the communities who already agree with them (Douglas et al., 2019, p. 15). Computational approaches empirically demonstrate that the consequences of algorithmically created filter bubbles are limited exposure to, and lack of engagement with, different ideas, and other people's viewpoints (Bessi et al., 2016; Zollo et al., 2017). Filter bubbles make it likely that micro-targeting of political campaign messages results in the wider population and mainstream media being left unaware of the campaigner's micro-targeted messaging: *this makes it difficult to offer factual correctives to misinformation and disinformation circulating in filter bubbles*.

Another useful empirical research strand is on the impact of digital deception (encompassing fake news, disinformation, misinformation, and conspiracies). Vosoughi et al. (2018) find that false political news diffuses significantly farther, faster, deeper, and more broadly than the truth on Twitter, and that this is down to humans (rather than bots) spreading the false news. A study by Guess et al. (2019) of individual-level characteristics associated with sharing fake news articles on Facebook during the 2016 US presidential campaign finds that while sharing fake news was rare, users over 65 shared nearly seven times as many articles from fake news domains as the youngest age group (even after controlling for partisanship and ideology). Various computational studies empirically point to problems in correcting false information circulating in algorithmically created filter bubbles. For instance, a study by Bessi et al. (2016) examining information consumption patterns of 1.2 million Italian Facebook users find that those with a polarisation toward conspiracy are most inclined to spread unverified rumours. Other studies show that dissenting information is mainly ignored or may even increase group polarisation (Zollo et al., 2017). The injection of deceptive political messages into the digital media ecology by political campaigners is therefore of democratic concern in that *deception spreads faster than the truth; in misleading certain groups of citizens (older people and those prone to conspiracy theories); and in its resistance to being corrected*.

Indeed, by 2018, Nadler et al. (2018, p. 4–5) identified a "digital influence machine" consisting of technologies for surveillance, targeting, testing, and automated decision-making designed to make advertising more powerful and efficient. They argue that political and anti-democratic actors weaponise the digital influence machine by targeting selected audiences when they are most vulnerable to manipulation through three main strategies: mobilising supporters via identity threats; dividing an opponent's coalition; and leveraging influence techniques informed by behavioural science. They further argue that rather than attempting to change people's beliefs, such weaponised campaigns aim to amplify existing resentments and anxieties, raise the emotional stakes of particular issues, stir distrust among potential coalition partners, and subtly influence decisions about political behaviours (such as whether to vote) (also see Kim et al., 2018). As Nadler et al. (2018) point out, *combining psychological research and data-driven targeting to identify audience's vulnerabilities is the mainstay of digital marketers,* rather than an outlying technique undertaken only by rogue organisations. The proliferation of such techniques, whether or not ultimately influential on voting behaviour, is democratically problematic. As Marchal (2020) argues, *being on the receiving end of psy-ops and microtargeted ads geared towards voter suppression might well affect one's sense of electoral fairness, and potentially undermine belief in the integrity of electoral processes.*

With the negative implications for democracy in mind, the following sections examine the deceptive and coercive nature of Cambridge Analytica's psychographic profiling and targeting across the UK's 2016 Brexit Referendum campaign.

MATERIALS AND METHODS

A Case Study Approach

Through qualitative analysis, this paper aims to identify and understand key important features (deception, coercion, and influence activities) of a little understood area of digital political campaigning, while preserving their texture and detail. It adopts a case study approach, as it seeks to understand in depth, holistically, and in an exploratory fashion, a contemporary, real-world phenomenon (Gerring, 2018). This approach excels in maximising context and in making sense of contradictory details from multiple sources: these are ideal attributes for unravelling deceptive and secretive influence activities. This is an important case study because (a) Cambridge Analytica appears to have pioneered the application of psy-ops from the military wing to the political wing of the wider corporate structure within which it was embedded; (b) its practices have been extensively described by whistleblowers, and have been investigated by journalists, public inquiries, and regulators, thereby providing considerable

insight into normally hidden parts of the digital campaigning ecosystem; and (c) it enables reflection on the social acceptability of such techniques.

However, this is a difficult case study to examine empirically given lack of access to those producing the campaign messages, to the messages themselves, and to the target audience. Access to Cambridge Analytica staff for interviews is problematic given the company's collapse; staff non-disclosure agreements; and attempted prosecutions of key figures within the company by the UK Information Commissioners Office (over Brexit data misuse) (Information Commissioners Office, 2018); and by the US Federal Trade Commission (for deceptive harvesting of Facebook users' personal information) (Federal Trade Commission, 2019b). Meanwhile, journalists attempting to examine Leave.EU's campaign activities have been faced with chilling lawsuits from its founder and financier, Arron Banks (Bowcott, 2020). The digital campaign messages that Leave.EU produced are not publicly archived, as the Brexit referendum predates the political digital advertising archives since established by social media platforms. Audience research into their exposure to, and influence from, Leave.EU campaign messages is difficult because of lack of public records on who was targeted. Even if audience access was achievable, the targeted messages did not bear any campaign imprints, and hence audiences would not necessarily know that they were receiving political campaign messages; and with such ephemeral social media messages, recall of exposure is also likely to be unreliable. Given these impediments, this study relies on documents already in the public sphere.

Fortunately, there is extensive documentation (thousands of pages) from public inquiries, regulatory investigations, legal proceedings, and investigative journalists, as well as public revelations from Cambridge Analytica and UK Independence Party (UKIP, a hard Eurosceptic, right-wing UK political party). Specifically, this paper draws upon the UK Parliament's Digital, Culture, Media, and Sport (DCMS) Committee Inquiry into Fake News and Disinformation [a lengthy investigation (2017–2019) that attracted 170 written submissions, conducted 23 oral evidence sessions, took evidence from 73 witnesses, and asked over 4,350 questions at hearings]; regulatory investigations by The Electoral Commission (that regulates UK election spending) and the Information Commissioners Office [that regulates UK data protection, with this regulatory body noting that this was "the most complex data protection investigation we have ever conducted" (Information Commissioners Office, 2018, p. 15)]; legal proceedings by the US Federal Trade Commission against Cambridge Analytica; and books and stories by political and investigative journalists in the UK (Carol Cadwalladr; Channel 4 News; Sunday Times political editor, Tim Shipman) and USA (Wendy Siegelman, Joshua Green, Sasha Issenberg). It also draws on public or since-publicised private statements (in books and interviews) from political actors in the UK with links to Cambridge Analytica, especially Andy Wigmore (Director of Communications for Leave.EU during the 2016 EU Referendum) and Arron Banks (political campaign financier and founder for Leave.EU). Also relevant are statements from whistleblowers from UKIP (Dan Dennemarck, former UKIP data controller; David Soutter, former UKIP head of candidates). Finally, it draws on revelations from Cambridge Analytica itself (promotional literature; public statements from Chief Executive Officer, Alexander Nix); and material from whistleblowers, Chris Wylie (contractor at SCL Group and Cambridge Analytica 2013–14) and Brittany Kaiser (Director of Business Development, Cambridge Analytica, 2015–18).

These materials are read critically, alert to the possibility that accounts from individuals may be self-serving and omit uncomfortable facts. Statements from Cambridge Analytica and its Chief Executive Officer, Alexander Nix are particularly suspect: Cambridge Analytica is well-known within the industry for its sophisticated public relations strategy and relentless self-promotion (González, 2017). Similarly, Wigmore maintains that a statement he had made that Cambridge Analytica provided initial help and guidance to the Leave.EU campaign was deceptive: he told the Inquiry into Fake News and Disinformation that on this matter he was an "agent provocateur" and had merely provided boastful "spin" to get attention from journalists for the Leave.EU campaign, which had been necessary as he was a political outsider (Banks and Wigmore, 2018, p. 12).

Positioning the statements and actions of Cambridge Analytica and Leave.EU within this multi-perspectival archive helps parse their sometimes contradictory public statements, and sheds light on secretive influence activities involving deception and coercion in digital political campaigning efforts during the 2016 Brexit referendum.

RESULTS

The Rise and Fall of Cambridge Analytica

Cambridge Analytica and its various parent companies had a complex corporate structure. The company was operational in the UK across 2015–18 (as Cambridge Analytica UK Ltd.) and in the US (as Cambridge Analytica LLC operational from 2013, with other variations operational from 2014 and 2015). Since June 2016, Cambridge Analytica UK was owned by political consultancy SCL Elections Ltd., which also had several US affiliate companies. SCL Group Limited was the parent company of Cambridge Analytica UK Ltd. and SCL Elections Ltd (Siegelman, 2017; Kaiser, 2019b; UK High Court Judgement, 2019) (see **Figure 1**).

SCL Elections deployed psy-ops in more than 200 elections around the world, mostly in undeveloped democracies (Channel 4 News, 2018; DCMS, 2018, chapter 6; Kaiser, 2019b, chapter 3; Wylie, 2019, p. 134–135, 166; Briant, 2020). According to Cambridge Analytica whistleblower Brittany Kaiser, rather than engaging in blanket political advertising to persuade voters, "to get people to act, you created the conditions under which they would be more likely to do what you wanted them to do" (Kaiser, 2019b, p. 49). SCL Elections' parent company, SCL Group Limited, also operated in the defence sector, for instance, owning SCL Strategic Limited [formerly, SCL Defence Ltd Siegelman (2017)] where it, too, deployed psy-ops (Tatham, 2015; Wylie, 2018a, 2019, p. 39–57) (see **Figure 1**). Kaiser (2019b, p. 32) describes an SCL brochure proclaiming how it "used 'psy-ops' in defense and humanitarian campaigns." As Wylie, describes in evidence to the Inquiry into Fake News and Disinformation:

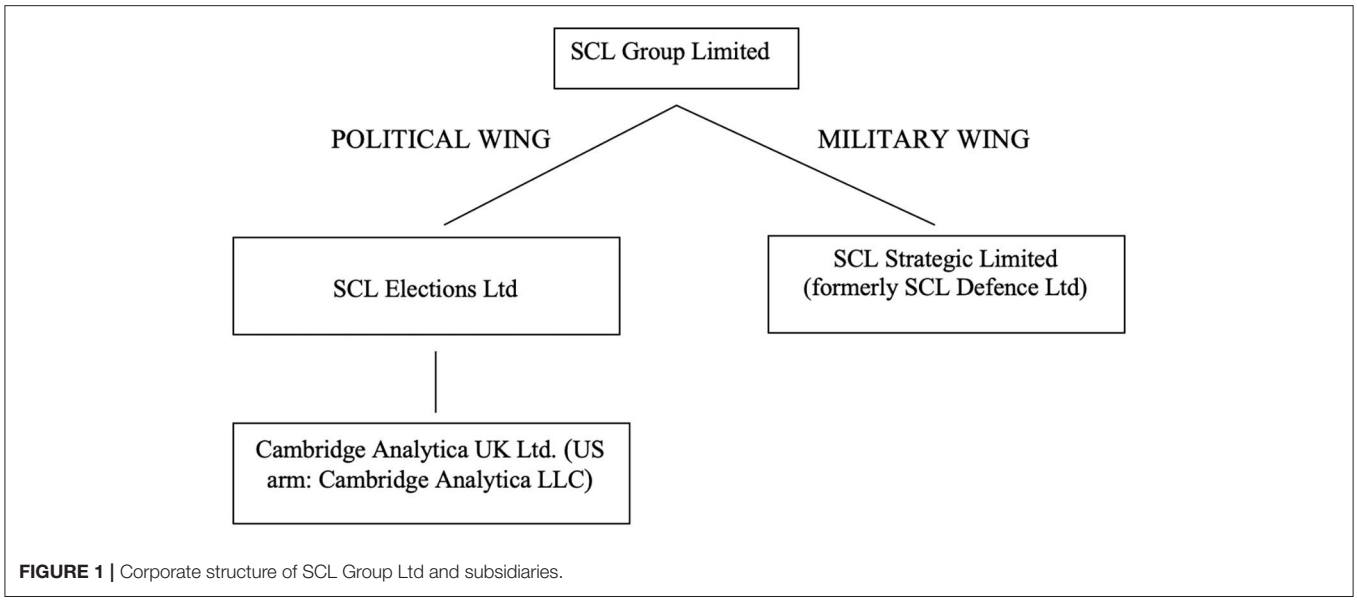

FIGURE 1 | Corporate structure of SCL Group Ltd and subsidiaries.

> Cambridge Analytica ("CA") was created by SCL Group with funding from Robert Mercer, an American billionaire … Mercer wanted to use the IO [Information Operations] tactics SCL had used on military projects for his political aims in the United States, and elsewhere, including the United Kingdom. CA's focus was to adapt these strategies for politics, as well as research ways to modernise and deploy IO approaches in online social networks (Wylie, 2018a, p. 8).

It was the deceptive data-gathering that underpinned such Information Operations activities that led to Cambridge Analytica's collapse. Cambridge Analytica and its parent companies, SCL Elections and SCL Group went into administration in May 2018, after two events that raised public disquiet. The first event was public allegations made by Wylie that Cambridge Analytica had exploited personal data of Facebook users (Wylie, 2018b, p. 14): this contradicted evidence given to the Inquiry into Fake News and Disinformation by Cambridge Analytica's Chief Executive Officer, Alexander Nix (Nix, 2018a, p. 24–25, Nix, 2018b, p. 15, p. 18). The second event was Nix being caught on tape in an undercover story for Channel 4 News broadcast on 20 March 2018, bragging about using bribery, sexual "honey traps" and manipulation of social media on behalf of clients to influence elections around the world (Channel 4 News, 2018; DCMS, 2018).

Following its collapse, Cambridge Analytica was found to have breached principle one of the UK's Data Protection Act 1998 for unfairly processing people's personal data for political purposes, including purposes connected with the 2016 US Presidential campaigns. The breaches were so serious that by November 2018, the UK's data regulator, the Information Commissioners' Office, stated that it would have issued a "substantial fine" had the company not already gone into administration (Information Commissioners Office, 2018, p. 35).

The following year, in July 2019, as well as levying a record $5 billion civil penalty against Facebook for failing to protect users' privacy, the US Federal Trade Commission filed an administrative complaint against Cambridge Analytica LLC (the US arm) for deceptive harvesting of personal information from tens of millions of Facebook users for voter profiling and targeting. This personal information had been collected in 2014 from users of a Facebook app (the "GSRApp"); it had exploited Facebook's now notorious (and since 2015, ended) data portal ("Friends API") that enabled the app developer to share not only users' data but that of all their friends. The information comprised users' Facebook User ID, which connects individuals to their Facebook profiles, as well as other personal information such as their gender, birthdate, location, and Facebook friends list (Federal Trade Commission, 2019a; Wylie, 2019, p. 112–132). In April 2018, Facebook revealed that the maximum number of unique accounts that directly installed the GSRApp, as well as those whose data may have been shared with the app by their friends, comprised 70,632,350 in the USA, 1,175,870 in the Philippines, 1,096,666 in Indonesia, 1,079,031 in the UK, 789,880 in Mexico, 622,161 in Canada, 562,455 in India, 443,117 in Brazil, 427,446 in Vietnam, and 311,127 in Australia (Schroepfer, 2018).

This personal data had been collected *deceptively*: GSRApp users had been told that the app would not download identifiable information. The GSRApp asked its users to answer personality and other questions that Cambridge Analytica used to train an algorithm that generated personality scores for the app users and their Facebook friends. Cambridge Analytica, Nix, and the app's developer (Aleksandr Kogan) then matched these personality scores with US voter records. Cambridge Analytica used these matched personality scores for its voter profiling and targeted advertising services (Federal Trade Commission, 2019a). According to Kaiser, Cambridge Analytica's "prodigious and unprecedented" database (Kaiser, 2019b, p. 77) included data from Facebook, data vendors, and (in the USA) their client's proprietary data that they had produced themselves and was not purchasable on the open market: as such, Cambridge Analytica

held between 2,000 and 5,000 individual pieces of personal information on every person in the USA over the age of 18 years (Kaiser, 2019b, p. 12–13, 78, 82–83).

There are *coercive* elements to how this deceptively gathered data was then deployed. Speaking to the US context, Cambridge Analytica whistleblower, Christopher Wylie, testified about the company to the US Congress and the UK Parliament's Inquiry into Fake News and Disinformation (Wylie, 2019). He describes how, across 2014, using its massive trove of data, Cambridge Analytica had worked to develop detailed "psychographic profiles" for every US voter, and experimented with ways to stoke paranoia and bigotry by exploiting certain personality traits: In one exercise, Cambridge Analytica asked subjects whether they would approve of their daughter marrying a Mexican immigrant: those who denied discomfort with the idea were asked a follow-up question designed to provoke irritation at the constraints of political correctness: "Did you feel like you had to say that?" (Wylie, 2019, p. 129). As Wylie told the Inquiry into Fake News and Disinformation:

> If you can create a psychological profile of a type of person who is more prone to adopting certain forms of ideas, conspiracies for example, and you can identify what that person looks like in data terms, you can then go out and predict how likely somebody is going to be to adopt more conspiratorial messaging and then advertise or target them with blogs or websites or what everyone now calls fake news, so that they start seeing all of these ideas or all of these stories around them in their digital environment (Wylie, 2018b, p. 21–22).

Wylie claims that people who exhibited certain psychological characteristics could be "nudged" into more extreme beliefs and conspiratorial thinking. Psychological research on conspiracies agrees that conspiracy theories may influence people's attitudes, with the level of influence appearing to depend on pre-existing attitudes and possibly other unknown factors (Douglas et al., 2019, p. 18). Some psychological studies also find that exposure to anti-government conspiracy theories lowers intention to vote and decreases political trust among UK and US citizens (although in other countries, it increases intention to engage in political action) (Kim and Cao, 2016; Douglas et al., 2019, p. 20). Regardless of its actual impact, what Wylie is describing amounts to *coercive* (choice limiting) *attempted* manipulation of potential voters by psychologically profiling them in order to target them with a provocative morass of digital disinformation and significantly alter what they are exposed to in the digital media ecology. The question that this paper now turns to is whether such coercive and deceptive practices were deployed by Cambridge Analytica in the UK's Brexit Referendum.

The Brexit Referendum: Targeted, Coercive, and Deceptive Digital Campaigning

On 23 June 2016, UK Prime Minister David Cameron fulfilled an election pledge to hold a national referendum on whether or not the UK should remain in the EU or leave (the Brexit Referendum). The Leave campaign narrowly won: 51.9% voted to Leave, 48.1% voted to Remain. The "Remain" campaign had urged the British people to vote to stay in the EU, the prime benefits being a stronger economy. "Leavers" promoted the benefits of lowering immigration, reducing the risk of terrorism and regaining control over the national economy (Goodwin, 2018). The referendum generated strongly held "Brexit" identities that prevailed even several years later, with affective polarisation as intense as that of partisanship in terms of stereotyping and prejudice (Hobolt, 2018; Hobolt et al., 2018). The Leave and Remain referendum campaigns were replete with misuse of statistics and false information from both sides, as evidenced by *The Telegraph* and fact-checker *Full Fact* (Kirk, 2017). However, the Leave campaigns were particularly noteworthy for high levels of targeted deception. "Vote Leave" was the official campaign to leave the EU, led by Conservative Members of Parliament, Boris Johnson, and Michael Gove. There were also various unofficial Leave campaigns, including the Leave.EU group founded by Arron Banks and Richard Tice. This paper focuses on the Leave.EU group's campaign because, as demonstrated below, it was characterised by audience profiling and targeting that resulted in propagation of deceptive messages using coercive tools: at the heart of this was Cambridge Analytica.

Leave.EU's Secret Audience Profiling and Targeting

During the Brexit referendum, Leave.EU did not declare any expenditure on Cambridge Analytica, or any in-kind donations (these would have to be declared to the UK's Electoral Commission, which enforces election laws and spending limits). In his initial letter and in oral evidence to the Inquiry into Fake News and Disinformation in February 2018, Nix states that "Cambridge Analytica had no involvement in the referendum, was not retained by any campaign, and did not provide any services (paid or unpaid) to any campaign" (Nix, 2018b, p. 2, Nix, 2018c). However, across the ensuing months, Arron Banks (Leave.EU founder and financier) submitted evidence to the Inquiry that showed that Cambridge Analytica had prepared a detailed *pitch* to Leave.EU to choose their company to help make the case to the Electoral Commission that Leave.EU should become the official campaign group for Leave (Cambridge Analytica/SCL Group, 2015a). Banks maintains that although Cambridge Analytica made a pitch, Leave.EU did not go forward with the work (Banks, 2018a,b; Banks and Wigmore, 2018, p. 4). Banks does reveal, however, that "some UKIP data" was sent to Cambridge Analytica to do "some initial scoping work" which resulted in a large bill to UKIP; and that UKIP approached Banks to pay it, but that Banks refused (Banks and Wigmore, 2018, p. 10).

Contradicting these claims that no work was done for Leave.EU, whistleblower Britanny Kaiser submitted evidence to the Inquiry in April 2018, that Cambridge Analytica was initially engaged with Banks, Wigmore and Matthew Richardson (former UKIP party secretary) to design parallel proposals for Leave.EU, GoSkippy/Eldon Insurance (Banks' insurance companies) and UKIP. Kaiser raised concerns that the personal data of British citizens who merely wanted to buy insurance was being used for political purposes (Kaiser, 2018b, p. 3) and expressed "similar concerns about whether UKIP members consented to the use

of their data" (Kaiser, 2018b, p. 2, 2019b, p. 138). Over a year later, in July 2019, Kaiser, supplied ten documents dated from 2015 to the Inquiry that showed that Cambridge Analytica had engaged in some work for Leave.EU on the EU referendum. This included analysis of UKIP's membership data (whose members are hard Eurosceptics), and analysis of survey results, to model four key groups of persuadable British voters to target with Leave.EU messaging: the "Eager Activist," "Young Reformers," "Disaffected Tories," and "Left Behinds" (Kaiser, 2019a, p. 51–52). In December 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 referendum. David Soutter, UKIP's former head of candidates, also claims that a deal had been made as UKIP had faced financial meltdown following its unsuccessful election battle against the Conservatives in 2015: "UKIP was financially on the ropes. It was short of money. I understood at the time that an offer had been made by Arron Banks to take on that weight, to take on that role, and run the database. Run the membership function of UKIP" (Howker, 2019).

Whether or not chargeable work was done by Cambridge Analytica for Leave.EU, evidence suggests that Leave.EU greatly benefited from the work that went into Cambridge Analytica's pitch. The evidence indicates that actuaries from Banks' insurance company (Eldon Insurance) copied Cambridge Analytica's modelling to identify 12 areas in the UK that were most concerned about the EU, in order to target them with in-person visits from Nigel Farage (then leader of UKIP). This was revealed by Andy Wigmore when interviewed by propaganda scholar, Emma Briant on 4 October 2017 (her interview later submitted as evidence to the Inquiry into Fake News and Disinformation) (Briant, 2018, p. 4–5). When questioned by the Inquiry on this point, Wigmore accuses Briant of misinterpreting his interview (Banks and Wigmore, 2018, p. 33). Nonetheless, Leave.EU saw Farage as vital to turning out voters who had never voted before but were passionate about leaving the EU because of how immigration affected their lives (Banks, 2017, p. 309; Shipman, 2017, p. 412).

There are at least two ways, then, in which Leave.EU may have used the UKIP database (that, according to whistleblowers, Banks had purchased) to find other pro-Brexit voters via social media platforms: by using tools from social media platforms such as Facebook's Lookalike audience builder (as described earlier); and/or by copying Cambridge Analytica's modelling using Banks' actuaries from his insurance company. Such data and insights would complement activities by the US strategy firm (Goddard Gunster) hired by Leave.EU to engage in large scale telephone polling (between 25,000 and 100,000 people) to understand voters' concerns, followed by population segmentation, micro-targeting identified groups, and then getting the vote out via "precision target-messaging" (Banks, 2017, p. 309; Shipman, 2017, p. 412–413).

Such opacity regarding the use made of Cambridge Analytica's work for Leave.EU raises as yet unanswered questions about what datasets were used to enable political profiling of the British population. Beyond this, even murkier aspects of Leave.EU's targeting techniques also emerged, revealing coercive and deceptive features of Cambridge Analytica's psychographic profiling and targeting.

Coercive Features of Leave.EU's Campaign

Cambridge Analytica's psychographic profiling tool had military origins. As described earlier, SCL Group operated a political arm (SCL Elections/Cambridge Analytica) and a defence arm, both of which deployed psy-ops tools. One such tool is Target Audience Analysis, a core methodology utilised by Strategic Communications Laboratories Group (which until June 2015 was the name of SCL Group Limited). A North Atlantic Treaty Organisation (NATO) Joint Warfare Centre publication (written in 2015 by a psy-ops specialist) describes Target Audience Analysis as a military psy-ops tool used to identify and influence influential target audiences in order to change their behaviour, and to model different interventions in this desired behaviour change. The article notes that the Target Audience Analysis methodology was soon to be used in a purpose-built NATO "Train the Trainer" Programme developed and delivered by Strategic Communications Laboratories Group and Information Operations Training and Advisory (IOTA) Services Global (Tatham, 2015, p. 51): IOTA Global Ltd. was owned by Nigel Oakes and Alexander Oakes, who both also had shares in, and were directors of, Strategic Communications Laboratories Group/SCL Group Limited (Siegelman, 2017). Strategic Communications Laboratories Group had spent over $40 million and 25 years, developing this group behaviour prediction tool. Its methodology: "builds up a detailed understanding of current behaviour, values, attitudes, beliefs and norms, and examines everything from whether a group feels in control of its life, to who they respect, and what radio stations they listen to. *TAA can be undertaken covertly*" (Tatham, 2015, p. 51, emphasis added).

Notably, the Target Audience Analysis methodology was an integral part of the pitch that Cambridge Analytica made to Leave.EU to help their campaign be selected as the official Leave campaign by the Electoral Commission (and that Banks maintains was never progressed) (Cambridge Analytica/SCL Group, 2015a,b). A Cambridge Analytica document detailing the pitch states:

> The first part of this phase, which will be centred on a particular geographic area (like a parliamentary constituency), will involve a programme of *Target Audience Analysis*, whereby qualitative and quantitative research is conducted in order to segment the population into target audiences according to their views, motivations and interests.
>
> The second part of Phase II, *Political Microtargeting*, involves the use of secondary data sources and advanced analytics to assign values on particular traits to the entire voting population of the area in question. This will allow for the target audiences to be resegmented and contacted as required over the course of the campaign, and the use of this data will be facilitated by the deployment of an online database utility created by Cambridge Anlaytica for Leave.EU

> … The end result of this process is a comprehensive plan for influencing voters likely to be receptive to Leave.EU's positions and messages (Cambridge Analytica/SCL Group, 2015a, p. 7).

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." As well as including "Psychographic clusters" and "Persuadability," another of these criteria is "Partisanship." As well as describing the "General Voter" and "Ideological Voter," this criterion describes the "Opposition Voter—*groups to dissuade from political engagement* or to remove from contact strategy altogether" (Cambridge Analytica/SCL Group, 2015a, p. 3, emphasis added). Part of this pitch, then, offered *voter suppression*.

Most of the pitch, however, was geared toward highlighting the individually tailored nature of its micro-targeting, exploiting what people care about. This would be possible because, as Kaiser told the Inquiry into Fake News and Disinformation, the tool that Cambridge Analytica developed for psychographic micro-targeting in the US used far more data than that used by Target Audience Analysis for military psy-ops purposes (as developed by Strategic Communications Laboratories Group) (Kaiser, 2018a, p. 20–21). The pitch states:

> *What this process offers is the opportunity to target communications at the scale of the individual.*
>
> In other words, Leave.EU will be able to ensure that every piece of digital or print advertising is directed at somebody who cares about the particular issue, or is likely to respond positively. This means that your campaign can save money that would otherwise have been spent contacting voters who are vehemently pro-EU, and direct those resources into making more frequent contact with swing voters and supporters you wish to mobilise as donors or volunteers. (Cambridge Analytica/SCL Group, 2015a, p. 8).

To summarise, Target Audience Analysis is a military-developed psy-ops tool used to identify and influence influential target audiences in order to change their behaviour, and to model different interventions in this desired behaviour change. Such behaviour change tools are coercive in that they aim to change people's behaviour via *covert psychological manipulation* rather than through freely chosen, deliberative decisions. Furthermore, Cambridge Analytica offered its profiling and micro-targeting services using far more data than that used by the Target Audience Analysis methodology developed for military psy-ops; and as noted earlier, a meta-analysis of relevant psychometrics research (Azucar et al., 2018) points to capacity for *covert behaviour change* campaigns by those with access to multiple data streams. On top of this, when Cambridge Analytica pitched for Leave.EU's business, part of that pitch offered voter suppression—which is coercive in that it actively seeks to constrain people's choices in dampening their volition to vote.

Deceptive Features of Leave.EU's Campaign

As noted earlier, Cambridge Analytica whistleblower Wylie, speaking to the US context, describes *coercive* (choice limiting) manipulation of potential voters by psychologically profiling them in order to target them with a provocative morass of digital disinformation, thereby significantly altering what they are exposed to in the digital media ecology. If Cambridge Analytica followed the same playbook in the Brexit referendum as Wylie claims that it used in the US elections, then it would also target psychologically profiled referendum voters with a morass of optimised digital disinformation. The absence of a complete database of digital ads from the 2016 referendum makes verification of any such claim difficult (Facebook only released ads to the Inquiry into Fake News and Disinformation from the other Leave groups rather than from Leave.EU) (Facebook, 2018). However, we can glean the following about Leave.EU's targeted deception.

We know from whistleblower Kaiser that in 2015, Cambridge Analytica had modelled four key groups of persuadable British voters to target with Leave.EU messaging, one of which was the "Left Behinds" (Kaiser, 2019a, p. 51–52). These are described (in an email to Kaiser dated 16 November 2015) as follows:

> Left Behinds…
>
> - 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 (Kaiser, 2019a, p. 51–52, emphasis added).

In her book, Kaiser states that if OCEAN personality trait scoring had been applied to the "Left Behinds," they "might have been found to be highly neurotic and, hence, most reachable when messaging appealed to their fears" (Kaiser, 2019b, p. 137). Given this modelling, the fact that net migration to the UK had rapidly increased since 2013 with the Syrian civil war generating an additional migrant crisis in 2015 (Shipman, 2017, p. 15, 20), and the fact that political campaigners have long appealed to identities and agitated anxieties around identity threats (Albertson and Gadarian, 2015), it is unsurprising that controlling immigration became a central message of the various Leave group campaigns.

Leave.EU emotively enhanced the immigration message through deceptive and outrageous claims (a strategy that Leave.EU's Wigmore copied from Trump). This enabled greater virality on social media and attracted mainstream press attention thereby generating free publicity and keeping immigration in people's minds (Banks, 2017, p. 282; Chappell, 2017; Shipman, 2017, p. 215, 391). For instance, UKIP's notorious billboard advert (that also ran in many northern regional newspapers) depicted a stream of migrants at the Croatian-Slovenian border, captioned "Breaking Point: The EU has failed us all" and "We must break free of the EU and take back control of our borders" (Shipman, 2017, p. 392). This is comparable to Nazi propaganda from the 1930s showing lines of Jewish people

flooding into Europe (Wylie, 2019, p. 167). On social media, Leave.EU targeted and spread particularly harsh and wholly deceptive anti-immigration messages, also targeting overt racists such as supporters of the British National Party and Britain First (until their strategy was discovered and publicised by the Remain group) (Shipman, 2017, p. 413). For instance, after 49 people were murdered in Orlando, Florida in a gay nightclub by a Muslim with an assault rifle, Leave.EU posted an advert depicting terrorists waving AK-47s captioned, "Islamist extremism is a real threat to our way of life. Act now before we see an Orlando-style atrocity" (Banks, 2017, p. 282). A typical Leave.EU Facebook post warned voters that "immigration without assimilation equals invasion" (Caesar, 2019). During the referendum campaign, Leave.EU also published a fake video as an "undercover investigation" on Facebook that went viral, with hundreds of thousands of views. The video claimed to show how easy it is to smuggle migrants into the UK from across the English Channel, but debunking this video several years later, satellite data shows that the footage was filmed in reverse (Channel 4 News, 2019). Such deceptive messages delivered via Facebook to targeted, profiled audiences would be difficult for the wider population to discern and counteract.

Public Feeling on Deception and Micro-Targeting in Digital Political Campaigning

This paper has discussed scholarship that points to capacity for covert behaviour change arising from digital campaigns by those with access to multiple data streams, by profiling individuals, and tailoring adverts automatically displayed in individual users' profiles based on personality. It has highlighted how Cambridge Analytica sought to deploy these techniques in the Leave.EU campaign, and how the Leave.EU campaign adapted modelling from Cambridge Analytica's pitch to engage targeted audiences with emotive, deceptive ads. Throughout his testimony to the Inquiry into Fake News and Disinformation, Nix, in defence of Cambridge Analytica's mode of operation, maintains that people are "not naïve" and understand how their data can be gathered, processed and used to support other campaigns (Nix, 2018b, p. 32). This begs the question, what is public awareness of, and feeling toward, deceptive micro-targeting for political campaigning purposes?

A US poll (conducted by Knight Foundation-Gallup across 3–15 December 2019) finds that people do not like deception in their online political advertising. Specifically, it finds that large majorities of Americans want social media companies to ban clearly false content in political ads. For instance, on adverts targeting supporters of an opposing candidate or cause and providing the wrong election date, 81% support banning the adverts; on adverts that say a politician voted for a policy that they did not actually vote for, 62% support banning the adverts; but where the false content is less clear cut, (namely, misrepresenting a candidate's position on an issue by providing some accurate facts or details but leaving out others), 45% support banning the adverts (McCarthy, 2020). This desire for action against deceptive online political adverts manifests not just in the USA, but globally. An international survey of digital news consumption of over 80,000 people across 40 countries finds that most people (58%) prefer platforms to block political adverts that could contain inaccurate claims, even if it means that technology companies ultimately get to decide what is true (Newman et al., 2020, p. 42) .

Where people are aware of digital micro-targeting practices being used to attempt to persuade them, most do not like it. A YouGov survey commissioned by pro-privacy group Open Rights Group (ORG) in 2019 finds that a majority of the UK national sample (58%) said they were against targeting or tailoring adverts during an election based on analysis of personal data to segment people into groups (ORG, 2020). In the US, even more people are against micro-targeting through digital ads. The US poll (conducted by Knight Foundation-Gallup across 3–15 December 2019) finds that 72% of Americans say that internet companies should make *no* information about its users available to political campaigns in order to target certain voters with online adverts. Only 20% of US adults favour allowing campaigns access to limited, broad details about internet users, such as their gender, age or postal code. This is in line with Google's policy, which, in 2019, reined in the scope of information that political campaigns can use for targeting. Only 7% of Americans say that any information should be made available for a campaign's use. This is in line with Facebook's targeting policies, which do not put any such limits in place on advert targeting (although Facebook does give its users some control over how many adverts they see) (McCarthy, 2020).

Unfortunately, many people do not realise that digital micro-targeting tools are being employed for political purposes. The UK's 2016 Brexit referendum saw "dark ads" (namely, micro-targeted online adverts only seen by the recipient) being discussed in public for the first time. Following the referendum, Dominic Cummings (Vote Leave's Campaign Director) claimed that Vote Leave innovated, "the first web-based canvassing software that actually works properly in the UK and its integration into world-leading data science modelling to target digital advertising and ground campaigning" (Cummings, 2017). Although the accuracy of the profiling undertaken by British political parties is disputed (Crowe et al., 2020), the use of such canvassing tools has since become increasingly mainstream in the UK. For instance, "Nationbuilder" allows campaign managers to build profiles of supporters and activists, integrate that database with information from social media and electoral rolls, and organise canvassing according to target voters' location. "Ecanvasser" uses voter mapping, surveys, issue tracking and analytics to understand what voters are thinking in order to target them through emails (Ecanvasser, 2020). By the UK's 2019 General Election, just over half of the UK public were aware of digital micro-targeting tools with a majority disapproving of these practices: however, there were still large proportions unaware. YouGov survey research in 2019 commissioned by ORG shows that although 54% of the UK population were aware of how political parties target or tailor adverts based on analysis of their personal data (political microtargeting),

almost a third (31%) were not aware at all, or not very aware. Only 44% of the national sample were very or fairly aware of "dark ads" with a similar figure (41%) not very or at all aware (ORG, 2020). It is alarming that a significant proportion of the British electorate are still unaware of how parties may attempt to manipulate them through digital micro-targeting, given several years of public discussion and increasing deployment of these practices.

DISCUSSION

Cambridge Analytica's profiling offered to the Leave.EU campaign in the 2016 Brexit Referendum had deceptive and coercive features. On *deception*, Cambridge Analytica's big data gathering for its psychographic micro-targeting lied to people about using their personal data, resulting in maximum permissible fines to both Cambridge Analytica and Facebook by the UK's Information Commissioners Office, and attempts to sue by the US Federal Trade Commission. Cambridge Analytica's modelling of UKIP data to generate four key groups of persuadable British voters to be targeted with Leave.EU messaging, was not declared to the UK's Electoral Commission during the referendum. Finally, Leave.EU created highly deceptive, Facebook ads and videos propagating harsh anti-immigration messages.

On *coercion*, a core psy-ops methodology (Target Audience Analysis) designed to covertly generate behaviour change in target populations was developed by the defence arm of SCL Group; and Target Audience Analysis was deployed by the political arm of SCL Group for digital political campaigning purposes. Cambridge Analytica's Chief Executive Officer, whistleblowers, and the psychology literature pronounce the efficacy of psychographic targeting when combined with big data analysis. Such behaviour change tools are coercive in intention: they aim to make people change their behaviour via *covert psychological manipulation* rather than through freely chosen, deliberated decisions. Furthermore, when Cambridge Analytica pitched for Leave.EU's business, part of that pitch offered voter suppression—a technique that it also employed in Trump's 2016 presidential campaign. Voter suppression is coercive in that it actively seeks to constrain people's choices in dampening their volition to vote. Finally, that voters were *targeted* both with deceptive Facebook posts propagating harsh anti-immigration messages and with in-person visits from Farage suggests that their digital filter bubbles and real-world experiences were manipulated to maximise their exposure to this particular information stream.

It is well-understood that propaganda often involves deception, but its coercive elements are less often discussed. To ethically persuade people to a particular political point of view demands that the persuadee's decision should be both informed and freely chosen (Bakir et al., 2019). If people are *deceived* into agreeing with something then their viewpoint is not *informed*: rather, they have been manipulated. If people are *coerced* into agreeing with something not just via violence or threats, but via precluding opportunities for reflection and deliberation and by limiting people's choices (be this the use of optimised microtargeting to suppress a target audience's desire to vote, or to modulate its exposure to information that is important in informing voting choices), then their viewpoint has not been *freely* arrived at: rather, they have been manipulated. If micro-targeting means that the wider population are unaware of the deception and coercion, then the wider population are also *disabled* from having reflective and deliberative shared conversations about what political campaigners stand for, weakening the opportunity to correct false and/or emotive information.

To put it more formally, the *psy-ops* like features of campaigns using psychographics and big data is evident in that psychographic targeting exploits (a) the cultural-psychological attributes of profiled target audiences and (b) the digital mass communication system (especially social media and databases) to deliver (c) optimised messages to influence or nudge the target audience (constituting the application of force in precluding opportunities for reflection and deliberation and in limiting peoples' choices by making them feel or behave in a certain way) (d) in a covert manner (the target audience is unaware of the manipulation) that (e) also lends itself to deception (because of its covert nature).

A limitation of this study is its inability to demonstrate that deployment of such psy-ops campaigning tactics actually influenced targeted voters. This, unfortunately, is a general weakness of media "effects" research on the effectiveness of such digital political campaigning tactics, given the opacity and targeted nature of the messages; the absence of an independent, publicly accessible database of all digital adverts deployed; the absence of information on who specifically received these targeted messages, and on what basis, as well as the extent of organic information diffusion; and the impossibility of determining which messages proved decisive in influencing people's vote (Aral and Eckles, 2019; Marchal, 2020). However, these limitations do not invalidate efforts to understand attempted psy-ops in digital political campaigns. Whether or not such tactics work, they evidence sustained efforts by political campaigners to provide more efficient ways to influence human behaviour by using opaque data science methods that, as surveys show, many people are unaware of and which the majority dislikes. This matters because, as Marchal (2020) points out, it attacks fundamental democratic norms and values, such as having fair access to information about parties and candidates that are free from undue influence or coercion.

Understanding and combating deception and coercion practiced via micro-targeting in digital political campaigns is important. Not just a normative ethical claim, this is also the view of the majority of the British and American adult population. This raises the question of whether, under pressure from regulators and governments, globally dominant US social media companies have since put in place adequate measures to eliminate the risk of further psy-ops activities in digital political campaigning. The core issue is micro-targeted deception.

On deception, Twitter's solution, since October 2019, is not to accept *explicitly* political adverts (Glazer, 2019). Google takes down political adverts that clearly violate its advertising policies, including "deep fakes" (doctored and manipulated media), misleading claims about the census process, and adverts or destinations making *demonstrably* false claims that could significantly undermine participation or trust in an electoral or democratic process (Spencer, 2019). However, such moves by Twitter and Google do not prevent political actors from inserting "surreptitious political messaging" into social media streams (Brown et al., 2020, p. 105). Furthermore, Facebook refuses to police the internet for political speech. Rather, Facebook's (and also Google's solution), since 2018, is to create a library of social media election adverts, thereby increasing transparency so that people can inspect the adverts and make their own evaluations. These archives show information such as who funded the advert, a range of how much they spent, and the reach of the advert across multiple demographics (Facebook, 2020; Google, 2020).

On micro-targeting, in November 2019, Google said that while it had "never offered granular microtargeting of election ads," it was further limiting election adverts' targeting to the general categories of age, gender and general location (postal code level), as well as to contextual targeting (Spencer, 2019); that advertisers would no longer be able to target political messages based on users' interests inferred from their browsing or search histories (Glazer, 2019); and that this approach would be enforced worldwide form January 2020. However, Facebook continues to micro-target. Nowhere does its political advert archive disclose how those adverts were targeted. Also, as Angwin (2020) reports, Facebook still allows advertisers to use provocative targeting criterion, such as "interested in pseudoscience," thereby demonstrating that grouping users by their vulnerabilities continues. It is of concern, then, that a significant proportion of the British electorate are still unaware of how parties may attempt to manipulate them through micro-targeting.

Thus, on micro-targeted deception, while some progress has been made among dominant US social media companies to reduce this psy-ops feature, Facebook still enables it during elections. As Facebook has more than 2.45 billion monthly active users globally, with the majority of users outside the USA or Canada (Facebook, 2019), micro-targeted deception remains a significant democratic threat. This threat persists in the UK where there has been no significant change to electoral law since 2001 (pre-dating the rise of social media) (Information Commissioners Office, 2018; All Party Parliamentary Group on Electoral Campaigning Transparency, 2020). However, the threat is especially problematic in countries with weaker privacy and data protections and weaker electoral traditions (Brown et al., 2020; Privacy International, 2020). For instance, in a survey of Commonwealth countries, Brown et al. (2020, p. 98) find that, of the 25 countries that responded, by far the greatest proportion of reported cases of electoral misinformation on social media platforms is found on Facebook (>90%) and its service Whatsapp (>40%). Furthermore, this threat is unlikely to diminish as current practices of usage of big data analysis, targeted advertising and psychographics are likely to be intensified as AI further permeates political communications (Bartlett et al., 2018), while using AI to detect and restrict deceptive content struggles heavily as such content is value-laden, subjective and complex (Brown et al., 2020, p. 103).

There is thus a need for continuing scrutiny of this fast-developing area by interdisciplinary scholarship. In particular, more research is needed into:

- Technological claims, especially the predictive power of digital footprints automatically collected from social media over the Big Five personality traits beyond English speaking or Chinese users.
- Political practices, especially the routine (and not just rogue) practices of digital political consultancies, including their use of psychographics and big data analytics to profile and target citizens in all countries that operate elections.
- User studies, to examine; (a) to what extent targeted groups are subjected to choice-limiting coercion during elections, such as whether they are exposed to a significant stream of information designed to change their behaviour; (b) the media literacy, not just of British and American citizens, but of voters in all countries that operate elections when faced with attempts to influence them via deceptive and coercive digital political campaigns; (c) the social acceptability of micro-targeting for political purposes, and whether such practices are undermining confidence in democratic institutions and processes in all countries that run elections.

Addressing these questions will progress understanding of the scale and impact of psy-ops activities in digital political campaigning across the world.

DATA AVAILABILITY STATEMENT

All datasets used in this study are available via the References list.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

FUNDING

This article was funded by *Emotional AI in Cities: Cross Cultural Lessons from UK and Japan on Designing for An Ethical Life,* UK Research and Innovation (ESRC)-Japan Science and Technology Joint Call on Artificial Intelligence and Society. Grant Ref. ES/T00696X/1.

REFERENCES

Albertson, B., and Gadarian, S. K. (2015). *Anxious Politics: Democratic Citizenship in a Threatening World*. Cambridge: Cambridge University Press. doi: 10.1017/CBO9781139963107

All Party Parliamentary Group on Electoral Campaigning Transparency (2020). *Defending Our Democracy in the Digital Age*. Available online at: https://fairvote.uk/wp-content/uploads/2020/01/Defending-our-Democracy-in-the-Digital-Age-APPG-ECT-Report-Jan-2020.pdf (accessed March 26, 2020).

Angwin, J. (2020). *Probing Facebook's Misinformation Machine. The Markup*. Available online at: https://www.getrevue.co/profile/themarkup/issues/probing-facebook-s-misinformation-machine-241739 (accessed March 26, 2020).

Aral, S., and Eckles, D. (2019). Protecting elections from social media manipulation. *Science* 365, 858–861. doi: 10.1126/science.aaw8243

Azucar, D., Marengo, D., and Settanni, M. (2018). Predicting the big 5 personality traits from digital footprints on social media: a meta-analysis. *Pers. Individ. Dif.* 124, 150–159. doi: 10.1016/j.paid.2017.12.018

Bakir, V., Herring, E., Miller, D., and Robinson, P. (2019). Organized persuasive communication: a conceptual framework. *Crit. Sociol*. 45:3. doi: 10.1177/0896920518764586

Bakir, V., and McStay, A. (2018). Fake news and the economy of emotions: problems, causes, solutions. *Digit. J*. 6:2. doi: 10.1080/21670811.2017.1345645

Bakir, V., and McStay, A. (2020). "Empathic media, emotional AI and the optimization of disinformation" in *Affective Politics of Digital Media: Propaganda by Other Means*, eds M. Boler, and E. Davis (Routledge).

Banks, A. (2017). *The Bad Boys of Brexit: Tales of Mischief, Mayhem and Guerrilla Warfare in the EU Referendum Campaign*. London: Biteback Publishing.

Banks, A. (2018a). *Written Evidence Submitted by Arron Banks*. Available online at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/written/81902.pdf (accessed March 26, 2020).

Banks, A. (2018b). *Written Evidence Submitted by Arron Banks*. Available online at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/written/80126.pdf (accessed March 26, 2020).

Banks, A., and Wigmore, A. (2018). *Oral Evidence: Fake News, HC 363*. Available online at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/85344.html (accessed March 26, 2020).

Bartlett, J., Smith, J., and Acton, R. (2018). *The Future of Political Campaigning. Demos*. Available online at: https://ico.org.uk/media/2259365/the-future-of-political-campaigning.pdf (accessed March 26, 2020).

Beckett, L. (2017). "Trump digital director says Facebook helped win the White House," in *The Guardian*. Available online at: https://www.theguardian.com/technology/2017/oct/08/trump-digital-director-brad-parscale-facebook-advertising (accessed March 26, 2020).

Bessi, A., Petroni, F., Del Vicario, M., Zollo, F., Anagnostopoulos, A., Scala, A., et al. (2016). Homophily and polarization in the age of misinformation. *Eur. Phys. J.* 225, 2047–2059. doi: 10.1140/epjst/e2015-50319-0

Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., et al. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature* 489, 295–298. doi: 10.1038/nature11421

Bowcott, O. (2020). "Arron banks drops two parts of libel claim against Carole Cadwalladr," in *The Guardian*. Available online at: https://www.theguardian.com/uk-news/2020/jan/23/arron-banks-drops-two-parts-of-libel-claim-against-carole-cadwalladr (accessed July 14, 2020).

Briant, E. L. (2015). *Propaganda and Counter-Terrorism: Strategies for Global Change*. Manchester: Manchester University Press. doi: 10.7765/9781847799630

Briant, E. L. (2018). *Transcripts: Oakes, Wigmore, Patten and Gunster Submitted to DCMS Inquiry into Disinformation and Fake News*. Available online at: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Dr-Emma-Briant-Audio-File-Transcripts-with-links.pdf (accessed March 26, 2020).

Briant, E. L. (2020). *Propaganda Machine: Inside Cambridge Analytica and the Digital Influence Industry*. Available online at: https://www.propagandamachine.tech/ca-map (accessed March 26, 2020).

Brown, I., Marsden, C. T., Lee, J., and Veale, M. (2020). *Cybersecurity for Elections. A Commonwealth Guide on Best Practice*. Available online at: https://thecommonwealth.org/sites/default/files/inline/Commonwealth%20cybersecurity%20for%20elections%20guide.pdf (accessed March 26, 2020). doi: 10.31228/osf.io/tsdfb

Cadwalladr, C. (2018). "The Cambridge Analytica files, "I made Steve Bannon's psychological warfare tool": meet the data war whistleblower," in *Guardian*. Available online at: https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (accessed March 26, 2020).

Caesar, E. (2019). "*Banks, the "Bad Boy of Brexit*," in *The New Yorker*. Available online at: https://www.newyorker.com/magazine/2019/03/25/the-chaotic-triumph-of-arron-banks-the-bad-boy-of-brexit (accessed March 26, 2020).

Cambridge Analytica/SCL Group (2015a). *Leave.EU: Profile Raising and Outreach*. Available online at: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Arron-Banks-appendix.pdf (accessed March 26, 2020).

Cambridge Analytica/SCL Group (2015b). *Leave.EU: Psychographic Targeting for Britain*. Available online at: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/BK-Background-paper-CA-proposals-to-LeaveEU.pdf (accessed March 26, 2020).

Channel 4 News (2018). *Broadcast 20 March 2018*. Available online at: https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation (accessed March 26, 2020).

Channel 4 News (2019). "Revealed: how Leave.EU faked migrant footage," in *Channel 4 News*. Available online at: https://www.channel4.com/news/revealed-how-leave-eu-faked-migrant-footage (accessed March 26, 2020).

Chappell, S. G. (2017). "Political deliberation under conditions of deception: the case of Brexit," in *OpenLearn*. Available online at: https://www.open.edu/openlearn/history-the-arts/philosophy/political-deliberation-under-conditions-deception-the-case-brexit (accessed March 26, 2020). doi: 10.1017/S147717561600021X

Chester, J., and Montgomery, K. (2017). The role of digital marketing in political campaigns. *Internet Policy Rev*. 6:4. doi: 10.14763/2017.4.773

Crowe, P., Rice, M., and Santi, M. D. (2020). "Who do they think we are? Political parties, political profiling, and the law," in *ORG*. Available online at: https://www.openrightsgroup.org/publications/who-do-they-think-we-are-report/ (accessed July 13, 2020).

Cummings, D. (2017). *On the Referendum #22: Some Basic Numbers for the Vote Leave Campaign*. Available online at: https://dominiccummings.com/2017/01/30/on-the-referendum-22-some-numbers-for-the-vote-leave-campaign/ (accessed March 26, 2020).

DCMS (2018). *Disinformation and 'Fake News': Interim Report. Digital, Culture, Media and Sport Committee, House of Commons 363*. Available online at: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf (accessed March 26, 2020).

Douglas, K. M., Uscinski, J. E., Sutton, R. M., Cichocka, A., Nefes, T., Ang, C. S., et al. (2019). Understanding conspiracy theories. *Adv. Polit. Psychol*. 40, 3–35. doi: 10.1111/pops.12568

Ecanvasser (2020). *The 20 Best Campaign Tools for 2020 [Updated]*. Available online at: https://www.ecanvasser.com/campaignblueprint/political-campaign-tools-2018/ (accessed March 26, 2020).

Facebook (2018). *Letter from Rebecca Stimson, UK Head of Public Policy, Facebook. Digital, Culture, Media and Sport Committee*. Available online at: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Fakenewsevidence/Letter-from-Rebecca-Stimson-Facebook-to-Chair-re-question-29-19-July-2018.pdf (accessed March 26, 2020).

Facebook (2019). *Facebook Q3 2019 Results*. Available online at: https://s21.q4cdn.com/399680738/files/docfinancials/2019/q3/Q3-2019-Earnings-Presentation.pdf (accessed March 26, 2020).

Facebook (2020). *What is the Facebook Ad Library and How Do I Search It?* Available online at: https://www.facebook.com/help/259468828226154 (accessed March 26, 2020).

Federal Trade Commission (2019a). *FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer*. Available online at: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer (accessed March 26, 2020).

Federal Trade Commission (2019b). *United States of America Before the Federal Trade Commission. In the Matter of Cambridge Analytica, LLC, a Corporation. DOCKET No. 9383*. Available online at: https://www.ftc.gov/system/files/documents/cases/1823107cambridgeanalyticaadministrativecomplaint7-24-19.pdf (accessed March 26, 2020).

Formisimo (2016). *Digital Marketing and CRO in Political Campaigns*. Available online at: https://www.formisimo.com/blog/digital-marketing-and-cro-in-political-campaigns/ (accessed March 26, 2020).

Gerring, J. (2018). "The Case Study: What It is and What It Does," in *The Oxford Handbook of Political Science*, ed R. E. Goodin (Oxford: Oxford University Press).

Glazer, E. (2019). *Facebook Weighs Steps to Curb Narrowly Targeted Political Ads. The Wall Street Journal*. Available online at: https://www.wsj.com/articles/facebook-discussing-potential-changes-to-political-ad-policy-11574352887?mod=followfacebook (accessed March 26, 2020).

González, R. J. (2017). Hacking the citizenry? Personality profiling, 'big data' and the election of Donald Trump. *Anthropol. Today* 33, 1–12. doi: 10.1111/1467-8322.12348

Goodwin, M. (2018). *The Perceived Costs and Benefits of Brexit. In Brexit and Public Opinion. The UK in a Changing Europe*, 24–26. Available online at: https://ukandeu.ac.uk/wp-content/uploads/2018/01/Public-Opinion.pdf (accessed March 26, 2020).

Google (2020). *Google Transparency Report*. Available online at: https://transparencyreport.google.com/about?hl=en (accessed March 26, 2020).

Gosling, S. D., Rentfrow, P. J., and Swann, W. B. (2003). A very brief measure of the big-five personality domains. *J. Res. Pers.* 37, 504–529. doi: 10.1016/S0092-6566(03)00046-1

Grassegger, H. (2018). "Facebook says its 'voter button' is good for turnout. But should the tech giant be nudging us at all?" in *The Guardian*. Available online at: https://www.theguardian.com/technology/2018/apr/15/facebook-says-it-voter-button-is-good-for-turn-but-should-the-tech-giant-be-nudging-us-at-all (accessed July 14, 2020).

Green, J., and Issenberg, S. (2016). "Inside the Trump Bunker, with days to go," in *Bloomberg*. Available online at: https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go (accessed March 26, 2020).

Guess, A., Nagler, J., and Tucker, J. (2019). Less than you think: prevalence and predictors of fake news dissemination on Facebook. *Sci. Adv.* 5:eaau4586. doi: 10.1126/sciadv.aau4586

Hausman, D. M., and Welch, B. (2010). To nudge or not to nudge. *J. Polit. Philos.* 18, 123–136. doi: 10.1111/j.1467-9760.2009.00351.x

Herbst, S. (2016). "The history and meaning of public opinion," in *New Directions in Public Opinion*, ed A. J. Berinsky (New York, NY; London: Routledge).

Hobolt, S. B. (2018). Brexit and the 2017 UK general election. *J. Common Mark. Stud.* 56, 39–50. doi: 10.1111/jcms.12751

Hobolt, S. B., Leeper, T., and Tilley, J. (2018). "Emerging Brexit identities," in *Brexit and Public Opinion. The UK in a Changing Europe*, 18–20. Available online at: https://ukandeu.ac.uk/wp-content/uploads/2018/01/Public-Opinion.pdf (accessed March 26, 2020).

Howker, E. (2019). "Arron Banks and the UKIP data hijack," in *Channel 4 News*. Available online at: https://www.channel4.com/news/arron-banks-and-the-ukip-data-hijack (accessed March 26, 2020).

Information Commissioners Office (2018). *Investigation into the Use of Data Analytics in Political Campaigns*. Available online at: https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf (accessed March 26, 2020).

Jamieson, K. H. (1996). *Packaging the Presidency: A History and Criticism of Presidential Campaign Advertising*. New York, NY: Oxford University Press.

Jones, J. J., Bond, R. M., Bakshy, E., Eckles, D., and Fowler, J. H. (2017). Social influence and political mobilization: further evidence from a randomized experiment in the 2012 U.S. presidential election. *PloS ONE* 12:4. doi: 10.1371/journal.pone.0173851

Jowett, G., and O'Donnell, V. (2012). *Propaganda and Persuasion, 4th Edn*. Thousand Oaks, CA: Sage.

Kaiser, B. (2018a). *Oral Evidence: Fake News, HC 363*. Available online at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/81592.html (accessed March 26, 2020).

Kaiser, B. (2018b). *Written Evidence Submitted by Brittany Kaiser*. Available online at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/written/81556.pdf (accessed March 26, 2020).

Kaiser, B. (2019a). *Additional Submissions to Parliament in Support of Inquiries Regarding Brexit*. Available online at: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Britanny-Kaiser-July-2019-submission.pdf (accessed March 26, 2020).

Kaiser, B. (2019b). *Targeted. My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy*. New York, NY: HarperCollins.

Key, W. B. (1974). *Subliminal Seduction*. New York, NY: Berkeley Press.

Kim, M., and Cao, X. (2016). The impact of exposure to media messages promoting government conspiracy theories on distrust in the government: evidence from a two-stage randomized experiment. *Int. J. Commun.* 10, 3808–3827. Available online at: https://ijoc.org/index.php/ijoc/article/view/5127/1740

Kim, Y. M., Hsu, J., Neiman, D., Kou, C., Bankston, L., Kim, S. Y., et al. (2018). The stealth media? Groups and targets behind divisive issue campaigns on Facebook. *Polit. Commun.* 35, 515–541. doi: 10.1080/10584609.2018.1476425

Kirk, A. (2017). *EU Referendum: The Claims that Won it for Brexit, Fact Checked. The Telegraph*. Available online at: http://www.telegraph.co.uk/news/0/eu-referendum-claims-won-brexit-fact-checked/ (accessed March 26, 2020).

Kosinski, M., Stillwell, D., and Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proc. Natl. Acad. Sci. U.S.A.* 110, 5802–5805. doi: 10.1073/pnas.1218772110

Marchal, N. (2020). *Conceptualizing the Impact of Digital Interference in Elections: A Framework and Agenda for Future Research*. SSRN. doi: 10.2139/ssrn.3536281

McCarthy, J. (2020). "In U.S., most oppose micro-targeting in online political ads," in *Gallup Blog*. Available online at: https://news.gallup.com/opinion/gallup/286490/oppose-micro-targeting-online-political-ads.aspx (accessed March 26, 2020).

McCrae, R. R., and Costa, P. T. (1987). Validation of the five-factor model of personality across instruments and observers. *J. Pers. Soc. Psychol.* 52, 81–90. doi: 10.1037/0022-3514.52.1.81

McStay, A. (2018). *Emotional AI: The Rise of Empathic Media*. London: Sage.

Metaxas, P. T., and Mustafaraj, E. (2012). Social media and the elections. *Science* 338:6106. doi: 10.1126/science.1230456

Mols, F., Haslam, S. A., Jetten, J., and Steffens, N. K. (2015). Why a nudge is not enough: a social identity critique of governance by stealth. *Eur. J. Polit. Res.* 54, 81–98. doi: 10.1111/1475-6765.12073

Nadler, A., Crain, M., and Donovan, J. (2018). "Weaponizing the digital influence machine: the political perils of online ad tech," in *Data and Society*. Available online at: https://datasociety.net/wp-content/uploads/2018/10/DSDigitalInfluenceMachine.pdf (accessed March 26, 2020).

Newman, N., Fletcher, R., Schulz, A., Andi, S., and Nielsen, R. K. (2020). *Reuters Institute Digital News Report 2020*. Available online at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf (accessed July 13, 2020).

Nix, A. (2016). "The power of big data and psychographics in the electoral process," in *The Concordia Annual Summit* (New York, NY). Available online at: https://www.youtube.com/watch?v=n8Dd5aVXLCc (accessed March 26, 2020).

Nix, A. (2018a). "Fake news, HC 363," in *Digital, Culture, Media and Sport Committee*. Available online at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/84838.pdf (accessed March 26, 2020).

Nix, A. (2018b). *Oral Evidence: Alexander Nix. Fake News, HC 363. 2018. Digital, Culture, Media and Sport Committee*. Available online at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/

digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/79388.pdf (accessed March 26, 2020).

Nix, A. (2018c). *Letter from Alexander Nix, Chief Executive, Cambridge Analytica to Damian Collins, Chair of the Committee. Digital, Culture, Media and Sport Committee*. Available online at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/written/79053.pdf (accessed March 26, 2020).

ORG (2020). *Public are Kept in the Dark Over Data Driven Political Campaigning, Poll Finds*. Available online at: https://www.openrightsgroup.org/press/releases/2020/public-are-kept-in-the-dark-over-data-driven-political-campaigning,-poll-finds (accessed March 26, 2020).

Pariser, E. (2011). *The Filter Bubble: What the Internet is Hiding from You*. New York, NY: Penguin Press.

Perloff, R. M. (2018). *The Dynamics of Political Communication: Media and Politics in a Digital Age*. New York, NY; London: Routledge. doi: 10.4324/9781315624426

Privacy International (2020). *Why We're Concerned About Profiling and Micro-Targeting in Elections*. Available online at: https://privacyinternational.org/news-analysis/3735/why-were-concerned-about-profiling-and-micro-targeting-elections (accessed March 26, 2020).

Ratkiewicz, J., Conover, M. D., Meiss, M., Goncalves, B., Flammini, A., and Menczer, F. (2011). "Detecting and tracking political abuse in social media," in *5th International AAAI Conference on Weblogs and Social Media* (Barcelona), 297–304. Available online at: http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/view/2850 (accessed March 26, 2020).

Schroepfer, M. (2018). "An update on our plans to restrict data access on Facebook," in *Facebook*. Available online at: https://newsroom.fb.com/news/2018/04/restricting-data-access/ (accessed March 26, 2020).

Shao, C., Ciampaglia, G. L., Varol, O., Flammini, A., and Menczer, F. (2017). The spread of fake news by social bots. *arXiv:1707.07592*. doi: 10.1038/s41467-018-06930-7

Shipman, T. (2017). *All Out War: The Full Story of Brexit*. London: William Collins.

Siegelman, W. (2017). "SCL group - companies and shareholders," in *Medium*. Available online at: https://medium.com/@wsiegelman/scl-companies-shareholders-e65a4f394158 (accessed March 26, 2020).

Simpson, C. (1994). *Science of Coercion: Communication Research and Psychological Warfare 1945-1960*. Oxford: Oxford University Press.

Spencer, S. (2019). *An Update on Our Political Ads Policy*. Available online at: https://www.blog.google/technology/ads/update-our-political-ads-policy (accessed March 26, 2020).

Tatham, S. (2015). Target audience analysis. *The Three Swords Magazine* 28, 50–53. Available online at: http://www.jwc.nato.int/images/stories/threeswords/TAA.pdf (accessed March 26, 2020).

Thaler, R., and Sunstein, C. (2008). *Nudge: Improving Decisions About Health, Wealth and Happiness*. London: Penguin.

The Behavioural Insights Team (2020). Available online at: https://www.bi.team/about-us/ (accessed March 26, 2020).

The Electoral Commission (2018). *Digital Campaigning: Increasing Transparency for Voters*. Available online at: https://www.electoralcommission.org.uk/sites/default/files/pdffile/Digital-campaigning-improving-transparency-for-voters.pdf (accessed March 26, 2020).

Tufekci, Z. (2014). Engineering the public: big data, surveillance and computational politics. *First Monday* 19:7. doi: 10.5210/fm.v19i7.4901

UK High Court Judgement (2019). *[2019] EWHC 954 (Ch)*. Available online at: https://www.judiciary.uk/wp-content/uploads/2019/04/17.04.19-cambridge-judgment.pdf (accessed March 26, 2020).

US Intelligence Community Assessment (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. Available online at: https://www.dni.gov/files/documents/ICA201701.pdf (accessed March 26, 2020).

Vosoughi, S., Roy, D., and Aral, S. (2018). The spread of true and false news online. *Science* 359:6380. doi: 10.1126/science.aap9559

Wells, W. D. (1975). Psychographics: a critical review. *J. Mark. Res.* 12, 196–213. doi: 10.1177/002224377501200210

Wylie, C. (2018a). *Supplementary Written Evidence: A Response to Misstatements in Relation to Cambridge Analytica*. Available online at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/written/81874.pdf (accessed March 26, 2020).

Wylie, C. (2018b). *Oral Evidence: Fake News, HC 363*. Available online at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/81022.pdf (accessed March 26, 2020).

Wylie, C. (2019). *Mindf*ck: Inside Cambridge Analytica's Plot to Break the World*. London: Profile Books.

Zollo, F., Bessi, A., Del Vicario, M., Scala, A., Caldarelli, G., Shekhtman, L., et al. (2017). Debunking in a world of tribes. *PLoS ONE* 12:e0181821. doi: 10.1371/journal.pone.0181821

Conflict of Interest: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.