Big data, small law: how gaps in regulation are affecting political campaigning methods and the need for fundamental reform

Bethany Shiner*

Technological developments, involving big data and data analytics, have enabled political parties and campaign groups to believe that they know or can accurately predict the political leanings of individual voters. Based on these developments, and coupled with psychological research deepening our understanding of decision making, campaign techniques involving individualised and targeted social media political advertisements have emerged. While research is not able to measure what impact, if any, these advertisements have there is a concern regarding the capacity of these techniques to influence in a non-transparent way by deceptively using personal data. In addition to protecting personal data, the law assumes that the electorate must maintain a 'free mind' and there must be a level playing field between political opponents. The current statutory framework is marked by an overlapping application of the Data Protection Act 2018, replacing the 1998 Act; the Political Parties, Elections and Referendums Act 2000; the Representation of the People Act 1983; and, the Communications Act 2005. As the evidence published in relation to several inquiries into these issues indicates, the gaps in the way this area is regulated means the law cannot adequately deal with the issues posed by the collection and use of personal data for the design and deployment of targeted social media political campaign advertisements. Further, the dependence upon these techniques by political parties and campaign groups mean that the necessary comprehensive reforms may never be made.

Introduction

In several related ways, the law attempts to regulate the electoral process and political campaigning to ensure fairness.[1] Apart from offences such as treating,[2] personation,[3] and those dealing with direct interference with voting,[4] electoral law regulates the electoral process by applying limits on the amount of money that can be spent during a referendum and election campaign.[5] The laws governing elections and political advertising assume that the electorate must maintain a 'free mind' and bans political advertisements from television and radio broadcasting (but not social media).[6] The law provides other measures such as preventing over-zealous campaigners from speed-dialling the electorate with automated messages without permission to do so.[7] Data protection laws aim to maintain privacy for individuals online protecting personal data and, more strictly, sensitive personal data which includes political opinions. In combination, these laws are meant to establish limits, boundaries and protections for the democratic process. However, new campaigning techniques reveal deficiencies in the law's aim of regulating and limiting the conduct of

* Lecturer in Law, Middlesex University. Sincere thanks to colleagues who have been generous enough to provide helpful feedback and encouragement including Alice Panepinto, Ciara Staunton, Damian Clifford, Joelle Grogan, John Adenitire and Laurence Diver. Special thanks to Carol Harlow, Daithi Mac Sithigh, David Kimani and Jennifer Cobbe. The author is also grateful for the formative feedback from the two anonymous reviewers.

[1] The discussion in this paper applies to elections and referendums. Although, there are differences between the two processes, they both use the same basic administrative and political structures and are based on the same political concept of informed democratic consent.

[2] *Erlam & Ors v Rahman & Anor* [2015] EWHC 1215 (QB)

[3] Representation of the People Act 1983, s 60

[4] Such as Representation of the People Act 1983, ss 65(1) and 66(3)

[5] Political Parties Elections and Referendums Act 2000 ss. 108-110; K.D. Ewing, "Transparency, accountability and equality: the Political Parties, Elections and Referendums Act 2000" (2001) PL 542-570

[6] Communications Act 2003 s. 321

[7] Privacy and Electronic Communications Regulations, reg. 19; *Scottish National Party v The Information Commissioner* [2006] EA/2005/0021

political parties, campaign groups, candidates and elected representatives during election and referendum campaigns.

Micro-targeting is generally perceived as a normalised[8] marketing and campaign strategy that uses data and demographics to create audience segments. The data includes personal information, actual behaviour and textual information about social interactions, conversations, reading and commenting history. This data is processed and analysed to determine political leanings and personal attributes with such precision that even information not explicitly given can be established.[9] These insight are used to identify which types of political campaign advertisements should be sent to which individuals over social media. Personality traits can be measured to inform tailored emotionalised political advertisements often described as psychographics.[10] However, the individual does not know they have been profiled based on their data or that they have been selected for targeting.[11] Micro-targeted advertisements are difficult to detect because by using dark advertisements only the sender, the social media platform and the receiver know what has been sent to whom.[12] The supposed aim of this practice is to influence and change voting behaviour for the benefit of the political party or group deploying these techniques.[13]

This paper will use these new campaign techniques to argue that the existing statutory regime, particularly regarding data protection and online direct marketing techniques,[14] cannot adequately and coherently respond to the issues that these methods raise.[15] To examine the potential detrimental effect of micro-targeting and other related online communication techniques this paper refers to legal, scientific and technological scholarship. It illustrates how the regulatory framework does not fulfil its purpose of maintaining fair, clean and free elections. This is highly problematic, particularly when trust in the democratic process is low and when the integrity of democracy as a system of governance is globally undermined and challenged. Finally, it critiques recent proposals for reform that offer piecemeal updates to the existing framework.

Micro-targeting as a form of political communication

---

[8] The Electoral Commission, "Political Finance Regulation and Digital Campaigning: A Public Perspective: GfK UK report for qualitative research findings" (April 24, 2018) *electoralcommission.org.uk* *https://www.electoralcommission.org.uk/__data/assets/pdf_file/0019/244540/Electoral-Commission-political-finance-regulation-and-digital-campaigning-a-public-perspective.pdf* [Accessed July 2, 2018]

[9] Z. Tufekci, "Engineering the public: Big data, surveillance, and computational politics" (July 2014) *First Monday*, *http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097* [Accessed July 24, 2018]

[10] Psychographics have been used in US elections but whether psychographics were used during the UK-EU referendum remains unestablished due to mixed accounts and documents recording conflicting evidence. See House of Commons. Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Interim Report Session 2017–19* (The Stationery Office, 2018) HC Paper No. 363 (Session 2017-19)

[11] M. Schroepfer, "An update on our plans to restrict data access on Facebook" (April 4, 2018) *Facebook Newsroom* *https://newsroom.fb.com/news/2018/04/restricting-data-access/* [Accessed 24 July 2018]

[12] Dark advertisements allow page owners to show non-public paid posts to selected users and as such are untraceable and can enable foreign advertisements on domestic matters.

[13] D. Tambini, S. Labo, E. Goodman and M. Moore, "The new political campaigning" *London School of Economics and Political Science* (March 2017) *http://eprints.lse.ac.uk/71945/* [Accessed July 24, 2018]

[14] Flaws in the regulation of campaign spending pose a critical weakness in the legal framework but there is not enough scope to tackle this here.

[15] This article does not turn on any specific allegation by any specific party or group but accepts, based on publicly available evidence cited throughout this paper, that in the whole these techniques exist and have been used on the electorate in the UK and globally.

Big data is "high velocity, complex and variable" data and as such requires sophisticated technologies to capture, store, distribute, manage, and analyse the information.[16] The data set is too enormous to be efficiently processed manually by humans, so algorithms analyse the information to reveal trends, patterns and correlations.[17] It is this process that enables algorithms to make predictions or gain insights that are not otherwise made explicit.[18] Big data can turn unseen correlations into "objects of scientific inquiry and manipulation."[19] As such, techno-sociologists urge that big data needs to be regarded as a political process engaging issues of transparency, power and surveillance – particularly because it is a tool possessing the capacity to "engineer consent".[20] However, "predicting attributes is much easier than persuading people" and the idea that changing someone's opinion merely requires evaluating traits like openness or political attitude is not proven.[21]

Data from credit reference agencies, insurance companies or comparison websites, for example, can be bought legally from data analytics firms and data brokers.[22] The electoral register can be sold, in prescribed circumstances, to credit reference agencies[23] and commercial interests can buy an edited version of the register excluding those who object to their details being sold to third parties.[24] Tracking cookies[25] follow consumers online capturing individuals' digital movements for analysis[26] which can be broadly described as political profiling. This falls within the General Data Protection Regulations (GDPR) new

---

[16] TechAmerica Foundation, "Demystifying Big Data: A Practical Guide to Transforming the Business of Government" (2012) https://bigdatawg.nist.gov/_uploadfiles/M0068_v1_3903747095.pdf [Accessed 24 July 2018]

[17] A. Gandomi and M. Haidar, "Beyond the hype: Big data concepts, methods, and analytics" (2015) IJIM 35(2) 137-144

[18] See fn. 17. This process of analysis is referred to as 'reality mining' which is the collection and analysis of machine-sensed environmental data relating to human social behaviour, with the goal of identifying predictable patterns of behaviour.

[19] See fn. 9

[20] E. Bernays, "The Engineering of Consent" (1947) The ANNALS of the American Academy of Political and Social Science 250(1) 113-120 http://journals.sagepub.com/doi/pdf/10.1177/000271624725000116 [Accessed August 13 2017]

[21] A. Rogers, "The Cambridge Analytica data apocalypse was predicted in 2007" (March 25, 2018) *Wired* https://www.wired.com/story/the-cambridge-analytica-data-apocalypse-was-predicted-in-2007/ [Accessed July 31, 2018]

[22] ICO Investigation update report confirms that it is looking at credit reference agencies in respect of the services they promote to political parties and campaigns see ICO *Investigation into the use of data analytics in political campaigns* (June 21, 2018) https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf [Accessed July 26, 2018]

[23] Representation of the People (England and Wales) Regulations 2001 reg. 114; *R (on the application of Robertson) v Secretary of State* [2003] EWHC 1760 (Admin)

[24] Following *Robertson v Wakefield Metropolitan Council* [2001] [2001] EWHC Admin 915, [2002] QB 1052, the Representation of the People (England and Wales) Regulations 2001 were amended by the Representation of the People (England and Wales) (Amendment) 2002 to introduce an edited register for anyone opposed to their details being sold onto a third parties

[25] Privacy and Electronic Communications Regulations 2003, reg. 6

[26] D. Albright "How Your Data on Facebook Is Collected and Used to Win Elections" (March 22, 2018) *MakeUseOf*, https://www.makeuseof.com/tag/facebook-data-influence-elections/ [Accessed July 26, 2018]; J. Bartlett "Big Data is watching you – and it wants your vote" (March 24, 2018) *The Spectator* https://www.spectator.co.uk/2018/03/big-data-is-watching-you-and-it-wants-your-vote/ [Accessed July 26, 2018]

definition of profiling which considers that to establish whether a processing activity[27] can be deemed to monitor the behaviour of data subjects, it should determine whether

> "natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes". [28]

Regardless of whether the profiling of individuals to establish personality traits and political sympathies for micro-targeting does influence political views and real-world behaviour (voting), the intention is to do so, and this corrupts political communication.[29] The use of half-truths, bias, selective history and misleading information is not a new phenomenon. What is new is that these communications are much more precise, and "knowing"[30] and as such raise questions about individual privacy, agency and, potentially, thought.[31] Traditional advertising methods have been discarded because they are "incapable of affecting the type of mass opinion shifts necessary for social change".[32] As data analytics can extrapolate meaning from textual and semantic data such as social network feeds and emails to deduce individuals' opinions about current affairs, other people and events, a detailed and in-depth understanding can be gained.[33] Some accounts suggest that digital strategy firms are deploying tests to detect emotional attachments and values to produce political messages engineered to maximise emotional and psychological impact.[34] As Emotion Artificial Intelligence is developed this is possible and raises more concerns about how the law can preserve political agency.[35] On the horizon lie technologies that can detect individuals' emotional states through data surveillance and promote large-scale behaviour change

[27] Processing is broadly defined by article 4(2) of the GDPR as any operations(s) performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[28] GDPR, recital 24. GDPR, art. 4(4) is its corresponding substantive provision. GDPR, art. 3(2)(b) brings the monitoring of behaviour within the territorial scope as far as that behaviour happens in the EU.

[29] B. Shiner, "Integrity instead of deceit: how to improve the delivery and content of political campaigns" (July 18, 2018) *LSE Brexit* http://blogs.lse.ac.uk/brexit/2018/07/18/the-delivery-and-content-of-political-campaign-material/ [Accessed July 26, 2018]

[30] D. Beer, "Data-led politics: do analytics have the power that we are led to believe?" (March 3, 2017) *LSE Blog* http://blogs.lse.ac.uk/politicsandpolicy/the-politics-of-data-led-campaigning/#Author [Accessed July 26, 2018]

[31] Castells argues that power relationships "are largely constructed in people's minds through communication processes. The shaping of minds is a more decisive and lasting form of domination…", see M. Castells *Communication Power*, 2nd edn (Oxford: OUP, 2013) xix; K. Yeung, "'Hypernudge': Big Data as a model of regulation by design" (2017) ICS 118; S. Alegre, "Rethinking freedom of thought for the 21st century" (2017) EHRLR 221

[32] A. Nix "From Mad Men to Math Men" (Online Marketing Rockstars Keynote, Hamburg, 10 March 2017) *youtube.com* https://www.youtube.com/watch?v=6bG5ps5KdDo [Accessed July 26, 2018]

[33] See fn. 17; B. Liu, "Sentiment analysis and opinion mining" (2012) Synthesis Lectures on Human Language Technologies 5(1) 1-167

[34] E. Briant interview with Brittany Kaiser "Explanatory essays giving context and analysis to submitted evidence" (April 16, 2018) https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Dr%20Emma%20Briant%20Explanatory%20Essays.pdf 2 [Accessed July 26, 2018]

[35] L. Goasduff, "Emotion AI Will Personalize Interactions" (January 22, 2018) https://www.gartner.com/smarterwithgartner/emotion-ai-will-personalize-interactions/

interventions through smart-phone prompts[36] and can even read and respond to thoughts.[37] Experts warn that it will be increasingly possible to stage "attacks" based on the analysis of human behaviours, emotions, and beliefs based on available data.[38] Technology already possesses the ability to manipulate information. Deep fakes are realistic (and often undetectable) digital manipulation of sound, images, or video to impersonate someone or make it appear that a person did something that they did not. The problem of foreign interference, as alleged in relation to the 2016 US presidential election and the 2016 UK-EU referendum, could worsen as technology becomes more sophisticated and can 'distort reality'. The potential for social harm (not just from malign states) may further erode trust in information, distort democratic discourse, manipulate elections, erode confidence in significant public and private institutions all of which challenge stable and democratic governance.[39] Combine that with the exponential increase in data sets[40] and the growing sophistication of big data analytics, there are grounds for an "ethical pause"[41] in the use of data in politics – but would a regulatory halt, or overhaul, be more appropriate? That another election or referendum campaign could run without the comprehensive root to branch reforms necessary is looking increasingly likely as suggested amendments to the system amount to a couple of tweaks that will not address the problems within the system as a whole.

The applicable legal framework

Data Protection

During an unfolding scandal around the use of data for political purposes in the US presidential election and the UK-EU referendum both in 2016, Facebook revealed that 87 million people had their profile information accessed by Cambridge Analytica, a data analyst and strategic communication firm.[42] Data from these profiles, including private messages,[43] was used to refine micro-targeting and other covert political campaigning techniques.

---

[36] N. Lathia, V. Pejovic, K. K. Rachuri, C. Mascolo, M. Musolesi and P. J. Rentfrow, "Smartphones for Large-scale Behavior Change interventions" (2013) IEEE Pervasive Computing 12(3) 66-73

[37] An MIT headset can read and transcribe thoughts (the internal voice) by measuring subtle neuromuscular signals that are triggered when a person verbalises internally. When someone says words inside his or her head, the device matches particular signals to particular words, feeding them into a computer with 92% translation success rate.

[38] Future of Humanity Institute, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation" (February 2018) *arxiv.org* https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf [Accessed July 26, 2018]

[39] R. Chesney and D.K. Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2018) *SSRN* https://ssrn.com/abstract=3213954 [Accessed July 23, 2018]

[40] The Internet of Things will increase the amount of data. In 2017, there were 8.4 billion connected devices in use worldwide projected to increase to 30 billion by 2020, see Demos "The Future of Political Campaigning" (July 18, 2018) *demos.co.uk* https://www.demos.co.uk/wp-content/uploads/2018/07/The-Future-of-Political-Campaigning.pdf 2 [Accessed July 20, 2018]

[41] ICO "Democracy disrupted? Personal information and political influence" (July 10, 2018) *ico.org.uk* https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf 11, 45 [Accessed July 12, 2018]

[42] M. Schroepfer, "An Update on Our Plans to Restrict Data Access on Facebook" (Facebook, April 4, 2018) https://newsroom.fb.com/news/2018/04/restricting-data-access/ [Accessed April 4, 2018]. In the wake of the scandal, Facebook altered its API settings to ensure third parties can no longer access Facebook user's data and violate user privacy.

[43] L. Kelion, "Facebook: Cambridge Analytica data had private messages" (April 10, 2018) *BBC News* http://www.bbc.com/news/technology-43718175 [Accessed May 18, 2018]

Investigations[44] are determining to what extent individuals in the UK were micro-targeted based on deceitfully or covertly gathered data. It is not the specific technique of micro-targeting that is unlawful rather the way in which the data is handled, who is it shared with and what data subjects are told, or not told, when they first grant access to their data. The ICO has investigated allegations of data misuse and have confirmed that social media platforms, data brokers and political campaign groups engaged in data misuse during the UK-EU referendum campaign. Furthermore, the ICO identified ongoing risks and concerns arising from the use of personal data by political parties specifically in relation to the purchasing of marketing lists and lifestyle information from data brokers without sufficient due diligence, a lack of fair processing, the use of third-party data analytics companies with insufficient checks around consent, and the provision of members contacts lists to social media companies. Indeed, eleven political parties were sent warning letters requiring action and Assessment Notices for audits by the ICO although regulatory action was also taken against Facebook and a data broker.[45]

The GDPR, implemented by the Data Protection Act (DPA) 2018 which replaced the 1998 Act, does not have retrospective effect. As such the DPA 1998 applies to the allegations of misuse of personal data for political purposes that occurred before May 2018, when the GDPR came into direct effect. Profiling and the use of big data is not unlawful but requirements under the DPA 1998, and now the DPA 2018, must be met. There are two categories of data: personal data; and, sensitive personal data (which includes political opinions).[46] There are also different uses of data in politics such as processing personal data for general promotional purposes and processing personal data to reveal political opinions for micro-targeting.[47] To lawfully and fairly process both types of data, at least one of the general conditions set out in schedule 2 DPA 1998 and now article 6 of the GDPR must be met. To process sensitive personal data at least one of the conditions previously set out in schedule 3 DPA 1998 and now article 9 GDPR and schedule 1 part 2 DPA 2018 must also be met.

When determining whether personal data is processed fairly and lawfully, it must be considered whether any person from whom the data was obtained was deceived or misled as to the purpose(s) for which the data is to be processed.[48] Fairness and transparency are fundamentally linked in the data protection regime. Unfairness can most starkly be seen when there is a disconnect between the initial cause for data collection or data provision and the subsequent use of that data. Individuals submit details online for various purposes, but the clincher is the deceptive retention and evaluation of personal information, including political views, for direct marketing.[49] One particular technique used before the UK-EU referendum vote was the gathering up of data through smartphone applications which targeted the users'

[44] The ICO investigation into the use of data analytics in political campaigns is examining over 30 organisations and individuals
[45] See fn. 22
[46] The GDPR now refers to 'special categories of data' but this paper will refer to sensitive data to mean the same thing
[47] The difference between sensitive personal data processing (processing revealing political opinions) and processing for political purposes warrants further exploration but is outside the scope of this paper.
[48] Data Protection Principle 1 as per DPA 1998, s. 1(1), Pt 2, Sch. 1; GDPR art. 5(1)(a)
[49] *Innovations (Mail Order) Ltd v Data Protection Registrar* (DA92 21/49/1)

contacts lists or Facebook friends' accounts.[50] Not only is this not transparent and unfair but the necessary consent for processing personal data is unlikely to be found because the consent is obtained from the user of the smartphone application rather than the people in their contacts list or their Facebook friends who remain unaware that their data is being accessed. Proactively, and in future, Data Protection Impact Assessments should highlight any potential privacy risks and points at which consent must be sought and notifications delivered. Another requirement is that data should be obtained only for one or more specified and lawful purposes and be processed compatibly with those purposes only.[51] To illustrate, the passing of personal data from an insurance company to a political group for political campaigning purposes is not in keeping with this requirement.[52]

Personal data may be used for promotional purposes in order to campaign and effectively communicate ahead of an election or referendum. Section 8(e)[53] provides a lawful basis for the processing of personal data "that is necessary for the performance of a task carried out in the public interest" including "an activity that supports or promotes democratic engagement" such as communicating with electors, campaigning activities, and opinion gathering inside and outside election periods.[54] Although this basis will still be subject to the GDPR six data protection principles including lawful, fair and transparent processing, purpose minimisation and accountability, the ICO warned that there was no need for this additional and broad provision[55] because the consent[56] or the legitimate interests[57] legal bases under article 6 GDPR are more appropriate justifications for processing personal data. The legitimate interest basis enables a balancing test between whether the legitimate interests are overridden by the interests or fundamental rights and freedoms of the data subject. This is an important test to ensure that organisations do not use a broad legal basis to legitimise opaque micro-targeting and the other campaigning techniques the ICO was investigating at the time section 8(e) was inserted into the Bill. During the ICO's investigation, it was made clear that political parties and campaign groups pay private organisations to process data and the democratic engagement basis does not apply to them. Also, this basis does not get around the additional provisions applicable to sensitive personal data.

Sensitive personal data may also be used for political promotional purposes but it cannot be processed unless one or more of the applicable conditions are met including that the data

---

[50] See fn. 22; T. Peters, "Brexit? There was an app for that" (June 24, 2016) *Medium.com* https://medium.com/@uCampaignCEO/brexit-there-was-an-app-for-that-57d1d658b4f1 [Accessed July 30, 2018]

[51] Data Protection Principle 2 as per DPA 1998, Pt 1, Sch. 1; GDPR art. 5(1)(b)

[52] See the ICO's investigation of Leave.EU and Eldon Insurance Services Limited, fn. 22

[53] Recital 56 states that in relation to electoral activities, political parties may compile personal data on people's political opinions for processing provided that appropriate safeguards are established.

[54] DPA 2018 Explanatory notes, para 86

[55] Data Protection Bill, House of Commons Public Bill Committee: Information Commissioner's further written evidence (March 19, 2018) *ico.co.uk* https://ico.org.uk/media/about-the-ico/documents/2258462/data-protection-bill-public-bill-committee-ico-further-evidence.pdf [Accessed May 10, 2018]

[56] GDPR, art 6(1)(a)

[57] GDPR, art 6(1)(f)

subject has given explicit consent;[58] and, the processing is carried out by a registered[59] person or organisation and is necessary for the purpose of that person's or organisation's "political activities"[60] including campaigning, fund-raising, political surveys and case-work.[61] Although, the processing of sensitive personal data without consent is generally prohibited by the GDPR,[62] as it is democratically desirable for political parties, campaign groups, candidates and elected representatives to communicate with the electorate the data protection regime establishes some circumstances in which processing of sensitive data can be allowed for reasons of public interest.[63] Sensitive personal data may be processed, without consent, in limited circumstances by registered political candidates, political parties[64] and by elected members,[65] who are, by way of example, entitled to access the full electoral register and the marked register which identifies who has voted in previous elections and referendums.[66] Outside of these limited circumstances, consent becomes a necessary condition. However, the GDPR principles of purpose limitation; data minimisation; data accuracy; and lawfulness, transparency and fairness apply irrespective of the consent of the data subject. Consent under the GDPR is defined as

> "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[67]

The required conditions for consent are set out in four subsections to article 7 GDPR and contain specific provisions on: the data controller being able to demonstrate consent; the prominence and clarity of requests for consent in an easily accessible form; an easy right to withdraw consent at any time; and, freely given consent when a contract, including a service provision, is conditional on consent although not being necessary for the performance of that contract. Explicit consent, one of the conditions for lawful processing of sensitive personal data, cannot be implied and amounts to consent that was freely given; was specific and informed;[68] there was a level of transparency about what type of data would be collected; it was clear what the data will be used for and who it will be shared with;[69] and, details about how an individual may exercise their right to object or withdraw consent were provided.

It is clear from the ICO investigation that third-parties have become privy to vast amounts of personal data for political purposes and as such there must be a lawful basis for the processing and the processing must rely on the one the additional conditions necessary for the processing of sensitive personal data. Although data can be lawfully bought from data brokers for

---

[58] DPA 1998, Sch. 3; GDPR art. 9(2)(a)
[59] A person or organisation included in the register maintained under section 23 of the Political Parties, Elections and Referendums Act 2000
[60] The Data Protection (Processing of Sensitive Personal Data) Order 2000, section 8 uses the term "legitimate political activities" and does not refer to necessity; DPA 2018, section 10 and section 22(1), Pt 2, Sch. 1
[61] DPA 2018, section 22(4), Pt 2, Sch. 1
[62] GDPR, art. 9
[63] GDPR, recital 56
[64] The Data Protection (Processing of Sensitive Personal Data) Order 2000, s. 8
[65] The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002, s. 3-4
[66] Representation of the People Regulations 2001 (as amended), reg. 47
[67] GDPR, art. 4(11)
[68] European Data Protection Directive 95/46/EC art. 2(h)
[69] Also a requirement of privacy notices, see fn. 22

secondary use, valid consent for the sharing of personal data with third-parties must be obtained. Under the GDPR those third-parties will not be able to rely on assurances that consent was validly obtained by the data broker and will have to exercise their own due diligence.[70] The ICO's investigation into the use of data in politics found evidence of political parties purchasing datasets from data brokers that had not obtained valid consent for the data to be used for political purposes.[71] The transfer of data to a political party or group, without the consent or knowledge of data subjects, gives rise to potential causes of action for misuse of personal information and for failure to lawfully and fairly process data and failure to obtain data only for specified and lawful purposes and be processed compatibly with those purposes.

Although, the GDPR introduces a higher standard of consent to processing personal data[72] there remain issues around the process of giving consent. Consent for data collection is granted to data controllers, like Facebook or political parties, who pass it onto data processors such as data analytics companies, for secondary use. Consent is often on condition of the provision of services and cannot be withdrawn whilst still accessing those services. Therefore, even when consent is given, it may not be adequate to satisfy the freely given element of consent if the individual had no real choice about giving it, such as when having to agree with terms and conditions to set up a Facebook account. Before the GDPR came into force companies sent automated privacy policy emails to individuals seeking opt-in consent which in practice repeat or worsen the same consent problems that existed before the GDPR because explicitly consenting to terms and conditions free companies from certain requirements within the GDPR. This is particularly problematic when company terms of service and privacy policies are thousands of words long, and consent is presented as 'take-it-or-leave-it' – a pushing tactic subjected to a legal challenge arising hours after the GDPR took effect.[73] Research has noted that since the GDPR came into force, Facebook, Google and Microsoft have resorted to using a series of techniques to discourage or nudge users away from setting more robust privacy settings which have the effect of users unwittingly accepting, through an "illusion of control", more expansive privacy settings which enable intrusive data collection.[74] Due to the element of deception and manipulation, these techniques do not appear to be in accordance with GDPR data protection principles such as informed and freely given consent, data protection by design and data protection by default.

Online campaign material

Online campaigning engages data protection regulations, electoral law and regulations on direct marketing. Political parties and groups are investing in micro-targeting by channelling

[70] GDPR art. 5(b), (c) and (e) 5 introduces a purpose limitation of data collection and GDPR art. 6(4) creates requirements for secondary or further processing must be compatible (not identical) with the original purpose for processing data.
[71] See fn. 22
[72] GDPR, art. 4(11), recital 32
[73] NOYB "GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook" (May 25, 2018) *noyb.eu* https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf [Accessed May 15, 2018]
[74] Norwegian Consumer Council, "Deceived by Design" (June 27, 2018) *forbrukertilsynet.no* https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf [Accessed July 2, 2018]

significant portions of their campaign funding into data analytics and social media advertising to try and ensure they get the most votes. Smaller sections of undecided and persuadable voters are particularly valuable as they can swing the outcome of a vote. Political parties spent £3.2 million, of £40 million, on direct Facebook advertising during the 2017 general election, up from £1.2 million during the 2015 general election.[75] During the UK-EU referendum, the Vote Leave campaign sent one billion digital advertisements during a ten-week campaign period, particularly before the closing dates to register for postal voting and the last ten days before the vote, accounting for 98 per cent of its budget.[76] Although the Remain campaign had substantial political resources, the Leave campaigners were tactical in encouraging people to vote, so the exact influence of varying campaign tactics remains unclear.[77]

Techniques that profile potential voters for targeting and the adoption of computerised databases containing personal data have been used in the UK at least since 2004. Ahead of the 2005 general election, the Conservatives[78] used the Voter Vault which combined demographic data with surveys from voters to create a model that identified people for targeting depending on: whether they lived in swing seats; they possessed 'conservative traits'; and, they did not vote Conservative in the previous election.[79] This methodology has been intensified. During the UK-EU referendum both the official Leave and Remain campaigns used third-party campaigning platforms that match political parties' databases with social media data. The Leave campaigns Voter Intention Collection System, and the Remain campaigns NationBuilder were able to assign each voter with scores based on how likely they were to vote and which way.[80] Smart mobile phone applications used for campaigning during the UK-EU referendum accessed the data of application users' contacts[81] to analyse the data of the non-consenting users' data to assess their political sympathies before sending them messages crafted to speak to issues predicted to have been at the forefront of their minds when deciding how to vote.[82]

---

[75] The Electoral Commission *electoralcommission.org.uk* *http://search.electoralcommission.org.uk/Search/Spending?currentPage=3&rows=30&query=facebook&sort=DateIncurred&order=desc&tab=1&open=filter&et=pp&includeOutsideSection75=true&evt=ukparliament&ev=3568&optCols=CampaigningName&optCols=ExpenseCategoryName&optCols=FullAddress&optCols=AmountInEngland&optCols=AmountInScotland&optCols=AmountInWales&optCols=AmountInNorthernIreland&optCols=DateOfClaimForPayment&optCols=DatePaid* [Accessed July 30, 2018]

[76] D. Cummings, "On the referendum #20: the campaign, physics and data science – Vote Leave's 'Voter Intention Collection System' (VICS) now available for all", (Dominic Cummings's Blog, October 29, 2016) *https://dominiccummings.com/2016/10/29/on-the-referendum-20-the-campaign-physics-and-data-science-vote-leaves-voter-intention-collection-system-vics-now-available-for-all* [Accessed July 17, 2017]

[77] For a selection of the micro-targeted adverts sent by Aggregate IQ on behalf of the Leave campaign groups see "Ads supplied by Facebook to the DCMS Committee" (July 26, 2018) *https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Fake_news_evidence/Ads-supplied-by-Facebook-to-the-DCMS-Committee.pdf* [Accessed July 26, 2018]

[78] Labour also relied on the use of sophisticated databases to target voters in the delivery of targeted messages, but it was reportedly inferior to the Voter Vault.

[79] J. Lees-Marshment and R. T. Pettitt, "UK political marketing: a question of leadership?" in J. Lees-Marshment, C. Rudd and J. Stromback (eds) *Global Political Marketing* (Abingdon: Routledge 2009)

[80] A. Mullen, "Leave versus Remain: the digital battle" in D. Jackson, E. Thorsen and D. Wring (eds) *EU referendum analysis 2016: media, voters and campaigners* (June 2016) *http://www.referendumanalysis.eu/*; M. Wallace, "Vote Leave versus Stronger In: How the referendum campaigns' ground operations measure up" (June 16, 2017) *ConservativeHome* *https://www.conservativehome.com/thetorydiary/2016/06/vote-leave-versus-stronger-in-how-the-referendum-campaigns-ground-operations-measure-up.html*

[81] See fn. 50 (Peters) and the previous section on consent

[82] See fn. 32

Social media exposes the rules on political advertising to be inconsistent and inadequate in meeting the stated aim of controlling political advertising. Paid political campaign advertisements are banned from television and radio broadcast, but party broadcasts are allowed because they are not classed as advertising.[83] Political advertisements sent to individual voters on social media, however, are unregulated because all non-broadcasting political advertising was specifically excluded from regulatory oversight under the Communications Act 2003. Non-broadcast political advertising was subject to the Advertising Code which was underpinned by the principle that all advertisements should be legal, decent, honest and truthful, and prepared with a sense of responsibility to consumers and society.[84] Although, the Neill Committee on Standards in Public Life recommended that a code of best practice should apply to political advertising in the non-broadcast media,[85] in 1999 the Committee of Advertising Practice (that writes the Advertising Code) excluded political advertising from regulatory oversight for fear that investigations, likely concluded after election results are announced, could create political instability; concerns around the application of article 10 ECHR; and, political disagreement.[86] In 2004, the Electoral Commission considered a legal framework for political advertisements but cautioned that the argument for a statutory code on political advertising is "unsustainable" because such regulation would be inconsistent with other non-broadcasting advertising regulation and because of the protections afforded to free speech.[87] Even a regulatory code was considered "inappropriate and impractical…given the often complex and subjective nature of political claims."[88] This anomaly means that an individual can complain about misleading claims on consumer and departmental[89] advertisements but political advertisements complained of being misleading, harmful or offensive cannot be investigated. The idea of a Code of Conduct to establish minimum standards online has recently re-emerged in the Committee on Standards in Public Life review of intimidation in public life;[90] the Constitution Society report on data and democracy;[91] and, the ICO's report on the use of data in politics.[92]

---

[83] Communications Act 2003, ss 319(2)(g), 321(2), 333. The broadcast has to comply with section 6 of the Ofcom Broadcasting code (2017)

[84] The Electoral Commission, "Political advertising: report and recommendations" (June 2004) *electoralcommission.org.uk* https://www.electoralcommission.org.uk/__data/assets/pdf_file/0007/213784/Political-Advertising-report-and-recommendations-June-2004.pdf [Accessed August 13, 2017]

[85] Committee on Standards in Public Life, *The Funding of Political Parties in the United Kingdom*, (The Stationery Office, 1998), Cm 4057-I Recommendation 96

[86] ASA News, "Political Advertising (ASA)" (July 21, 2014) *asa.org.uk* https://www.asa.org.uk/news/political-advertising.html [Accessed August 31, 2017]

[87] See fn. 84, p. 4

[88] See fn. 84, para. 4.2

[89] Government advertisements are caught by Rule 7.2 of the Non-broadcast Code as far as they are distinct from party policy. See ASA, "ASA Adjudication on Home Office" (October 9, 2013) *asa.org.uk* www.asa.org.uk/rulings/home-office-a13-237331.html [Accessed August 17, 2017]

[90] Committee on Standards in Public Life, *Intimidation in Public Life: A Review by the Committee on Standards in Public Life* (The Stationery Office, 2017) Cm 9543

[91] J. K. Morrison, R. Naik and S. Hankey ,"Data and Democracy in the Digital Age" (The Constitution Society, July 2018) *consoc.org.uk* https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf [Accessed July 10, 2018]

[92] See fn. 41, p. 44

The practice of social media political advertising may be caught to a limited extent by section 11(3) DPA 1998 which provides that direct marketing includes political communications directed to an individual.[93] The political party or group commissioning the marketing must tell people at the point of collection how their data will be used. Even if information is publicly accessible as a result of steps taken by the data subject, this does not automatically mean that it can be reused for other (political) purposes without providing fair processing information. Political parties must provide privacy notices to individuals when data about them has been taken from publicly available sources if they intend to use that data.[94] In addition, information that is not explicitly offered but revealed after analysis of public data is still personal data and as such the consent requirements apply. Political parties, however, have been operating on the incorrect assumption that inferred information is not personal data.[95] The DPA 1998, 2018 and the PECR 2003 prohibit direct marketing through automated telephone calls, fax, email, text messages and post, unless the receiver has given consent. No provision explicitly applies to social media direct marketing but the right to object to direct marketing applies.[96]

The Facebook Custom Audience tool allows advertisers to target selected groups of people with specific advertisements for a fraction of the price of direct mail by methods such as uploading lists of email addresses, phone numbers and user IDs. When using the Custom Audience tool, political parties act as data controllers and should conform to the data processing principles which require transparency of the use of data[97] although they are not required to include information about who is responsible for the production of the material because imprints are only required for printed election material.[98] Under the GDPR it is also necessary to actively provide people with the information in an accessible way, meaning putting up a privacy notice on a website without informing individuals it is there will not be satisfactory. The GDPR imposes the need to keep records of consent and strengthens the need to notify data subjects of the collection and use of their personal data, the purpose of data processing and the legitimate interests pursued by the controller or by a third party, the retention periods for that personal data, and who it will be shared with.[99] This creates a more robust context for the right to object, which is an absolute right if processing is for direct marketing purposes which Facebook advertisements and other electronic mail are.[100]

The core issue raised by this institutionalised form of political communication is much broader than political advertising requirements. This form of communication forces what necessarily must be a public political process into private and inscrutable spheres. The law's aim of preserving the integrity of the election process through the regulation of certain

[93] *Scottish National Party v Information Commissioner* [2006] EA/2005/0021
[94] DPA 1998, s. 27(5), GDPR arts. 9(2)(e), 14
[95] See fn. 22
[96] GDPR art 21(2), (3). The Draft Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications ('ePrivacy Regulation'), if enacted by the UK following its departure from the European Union, will apply to all electronic communications that amount to direct marketing, including targeted advertisements.
[97] *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, in the presence of Facebook Ireland Ltd* (Case C-210/16); The ICO found that political parties were using this tool but in non-transparent ways, see fn. 41, p. 35
[98] Representation of the People Act 1983, s.110
[99] GDPR arts 13, 30
[100] GDPR art 21(1); DPA 2018, s. 99

practices, like paid party political advertisements, is undermined by the ease in which such parties can pay for advertisements, and other material, to be shared online.[101] That hundreds of varieties of the same advertisement can be monitored for effectiveness in real-time by sophisticated algorithms and software monitoring to identify the most successful messages in a constant iterative process to ensure maximum impact, raises new questions about how to preserve the electorate's 'free mind'.[102] Further, this fragmented form of tailored political communication erodes at the concept of open, public debate where policies, pledges and politicians are held accountable. Delivering separate messages to separate sections of the electorate, free from competing or opposing messages, means that contradictory or inconsistent promises can be made to different people and a full picture of political intentions and policy positions is harder to see and scrutinise. This, in turn, lends itself to delivering messages containing only what individual members of the electorate want to hear and facilitates information asymmetry.

Reforming digital political communications

In response to breaches in electoral law and data protection; the use of micro-targeting as a strategic political tool; and, the spread of 'fake news' (better described as disinformation),[103] there have been numerous inquiries, investigations and reports on how to reform the regulatory system and update the law. The current emphasis upon a few bad players (corporate and foreign interests) skews the narrative, for there would be no market for these techniques if politics did not invest in them. There is a general sense of alarm in public discourse around these practices,[104] which is not unwarranted but, throughout history new technologies have disrupted traditional forms of social and political communication and the law and society have generally adapted. It remains important to examine these issues not only from a regulatory perspective but also a broad perspective. The more fundamental issues do not relate to closing regulatory gaps but ensuring the political ecosystem balances out more fairly and imbues democratic principles like fairness and transparency which can help future-proof legal reforms. It seems that the scandal around data misuse for political purposes has served as an illustration of the huge distance between those elected to represent and those being represented - with companies exploiting that gulf for profit. Tweaking the regulatory system will not fix this problem. Focusing on whether, how or why the electorate is influenced misses the opportunity to think about how to make political communication more transparent, more honest, and more respectful of the electorate. Until we tackle this fundamental issue - whether through codes, regulations, or civil or criminal sanctions – the same campaign practices are likely to continue dominating the relationship the electorate has with its representatives. But, the likelihood of the Government, with no clear majority, introducing the required electoral reform legislation in this Parliament is slim.

---

[101] The High Court's considered the ban on paid party political broadcast advertising in *R. (on the application of Animal Defenders International) v Secretary of State for Culture, Media and Sport* [2006] EWHC 3069 (Admin); [2007] E.M.L.R. 6 (DC)

[102] See fn. 13, p. 12

[103] European Commission, "A Multi-Dimensional approach to disinformation: Report of the independent High Level Expert Group on Fake News and Online Disinformation (March 12, 2018) *https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation* [Accessed July 31, 2018]

[104] The DCMSC interim report on disinformation states "we are faced with a crisis concerning the use of data, the manipulation of our data, and the targeting of pernicious views." See fn. 10, p. 3

Review of suggested reforms

The Electoral Commission has recommended a legislative amendment using powers under s143(6) of the Political Parties, Elections and Referendums Act 2000 to require imprints on digital campaign material so that individuals know the source of the material and it will assist the tracking of donations and spending.[105] Thousands of political adverts, and other material like videos or memes, are disseminated online every day. How will this content be regulated to ensure political material conforms to the imprint requirement? Facebook will not readily accept this burden which may require expensive human moderators to make subjective and contextual judgements calls. Also, how will material that does not include an imprint be removed considering that it is not possible to delete all traces of a post, especially if it gets shared a lot? There are ways around the imprint requirement such as paying people to post messages of support as ordinary users or by relying on the organic spread of material on social media without paying for it.

The Electoral Commission's other recommendations amount to a collection of modifications. It repeats a recommendation to amend schedule 8 of the Political Parties, Elections and Referendums Act 2000 which lists the requirements on spending returns to include a specific category of social media spending (currently reported as 'advertising' or 'unsolicited material to voters'). It calls for more detailed and meaningful invoices for digital activity to close a loophole which enables the much higher national spending limit to be directed locally towards swing seats and key constituencies breaching the lower local spending limits.[106] The Commission requested an increase in the fine it can sanction for breaching electoral law; executive clarification on foreign donations and campaign spending; social media action on paid-for political advertisements originating from outside the UK; and, an improvement on the rules and deadlines for reporting spending for scrutiny during or shortly after elections or referendums. The Commission proposed a social media online database of paid-for political adverts, which social media companies already said they would implement,[107] instead of endorsing a more robust idea of creating a central public register of online political advertisements that would not be left to social media companies.[108] Considering the rate of micro-targeted advertisements during the UK-EU referendum, there could be billions of advertisements registered.

Modern election law[109] continues to be founded upon practices such as intimidation, bribery, corruption or coercion that were rife in Britain until the introduction of several Acts of Parliament in the late 19th Century.[110] Electoral offences are still framed in the language of the

---

[105] The Electoral Commission, "Digital campaigning: Increasing transparency for voters" (June 2018) *electoralcommission.org.uk* https://www.electoralcommission.org.uk/find-information-by-subject/political-parties-campaigning-and-donations/digital-campaigning paras 27 - 31

[106] The Electoral Commission, "UK Parliamentary General Election 2015: Campaign spending report" (February 2016) *electoralcommission.org.uk* http://www.electoralcommission.org.uk/__data/assets/pdf_file/0006/197907/UKPGE-Spending-Report-2015.pdf paras 3.26 – 3.32 and recommendation 3; see fn. 105

[107] Facebook's new View Ads mechanism will enable users to view all of the advertiser's material.

[108] See fn. 105 and fn. 10

[109] The Representation of the People Act 1983, Representation of the People Act 2000 and the Political Parties Elections and Referendums Act 2000

[110] The Corrupt Practices Act 1854, THE Parliamentary Elections Act 1868, The Ballot Act 1872, Corrupt and Illegal Practices Act 1883 and The Corrupt Practices Act 1883. The Representation of the People Act came in 1918.

19th century when votes were bought, elections rigged for favours, and the ballot could be coerced.[111] Election law must reflect the reality of contemporary political campaigning, the behaviour of elected representatives, political candidates and parties as well as the way in which people can be coerced or manipulated, which is much more than physical intimidation. A wholesale review must go further than the Law Commissions' 2016 recommendations for reform which prioritised unifying the pieces of electoral legislation, modernising procedures and processes and improving the way to challenge election outcomes.[112] Although these are important reforms, a complete overhaul is needed to ensure electoral offences reflect the 21st century.

The Digital, Culture, Media and Sport Committee's (DCMSC) proposed a ban on micro-targeted political advertising through Facebook 'lookalike audiences' where users have requested not to receive political adverts, and a national minimum limit for the number of voters sent individual political messages. This was a compromise on the suggestion of a total ban.[113] But, should digital political advertisements and micro-targeting be banned entirely? As explained in relation to imprints, there are ways around moderate or partial bans on political digital content and regulations can quickly become out of date. Yet, a ban could dampen down political engagement as people would be forced to return to traditional media when every other part of our life is becoming digitalised. The DCMSC also called for the Electoral Commission to establish a code for advertising through social media during election periods and consider whether social media campaigning should be restricted during the regulated period to registered political organisations or campaigns.[114] This could work in tandem with the suggestion that social media companies and intermediaries work closely with regulators and advise political parties on transparency and accountability when using data to target voters on those platforms,[115] and that social media companies improve their policies on campaign material and advertising for elections and referendums in the UK. Social media platforms are being urged to introduce transparency features with the ICO and the Electoral Commission being consulted on those features and completing evaluations.[116] The DCMSC targets intermediaries and proposes a new category for technology companies which is neither platform or publisher, but something in between that establishes some liability to act against "harmful and illegal content".[117] How intermediaries can monitor this while preserving freedom of speech and not enforcing rules unfairly or in a discriminatory way and whether such power should be delegated needs to be given much more consideration by the DCMSC.[118]

---

[111] B. Watt, "UK Election Law: A Critical Examination" (London: Cavendish Publishing, 2006)
[112] Law Commission, Scottish Law Commission and Northern Ireland Law Commission "Electoral Law: interim report" (February 4, 2016) *lawcom.gov.uk* *http://www.lawcom.gov.uk/app/uploads/2016/02/electoral_law_interim_report.pdf* [Accessed July 31, 2018]
[113] See fn. 10 paras 141 - 142
[114] See fn. 10
[115] See fn. 41, p. 42
[116] See fn. 41, recommendation 6
[117] See fn. 10 paras 51 - 60
[118] S. Levin, "Civil Rights Groups Urge Facebook to Fix 'Racially Biased' Moderation System," (Guardian, January 18, 2017) *https://www.theguardian.com/technology/2017/jan/18/facebook-moderation-racial-bias-black-lives-matter* [Accessed May 27, 2018]; D. Keller "Internet Platforms: Observations on Speech, Danger, and Money" (2018) Aegis Series Paper No. 1807

Facebook already engages in political narrative sharing, information control and emotional manipulation.[119] A randomised controlled trial of political mobilisation messages delivered to 61 million Facebook users during the 2010 US congressional elections showed that the Facebook messages "directly influenced political self-expression, information seeking and real-world voting behaviour of millions of people. The messages not only influenced the users who received them but also the users' friends, and friends of friends".[120] Such digital interventions can be heralded as promoting democratic engagement, especially when perceived as being neutral or civic. However, the same techniques can be used to suppress democratic engagement or shape democratic discourse according to malign or corporate interests. Another example being Facebook's intervention in the campaign on the Irish referendum on the Eighth Amendment when, after public pressure, it blocked advertisements that originated from outside of Ireland. Google blocked all advertisements on its search engine and on YouTube that related to the referendum.[121] Such an intervention is in the gift of intermediaries that at once recognise the influence of foreign advertisements by banning them whilst maintaining that although they are not publishers,[122] they are responsible enough to make the right judgement calls as moderators. The potential for inconsistency grows if such action becomes the basis for a much broader range of online interventions. This action came late in the campaign cycle and was an unforeseen intervention disadvantaging some campaign groups because it disrupted campaign strategies. Interventions such as this should be predictable, consistent and transparent. Facebook has said it is developing tools to increase transparency in political advertisements which includes a verification process requiring advertisers to be resident in the country holding an election. However, it is straightforward to alter the location as recorded on a Facebook account or to change the IP address of the device being used to access Facebook or any other online platform.

The ICO called on Government to develop a statutory Code of Practice for the use of personal information in political campaigns which will form part of a broader legislative vehicle and contain guidance. The ICO seeks to promote dialogue between the regulators and the Government, and encourages a comprehensive reflection on corporate and political practices.[123] Hopefully, there will be meaningful engagement from the legislative although, elected representatives are captured by these techniques that help disseminate their message, and maximise their outreach and vote share. Whether politicians will willingly usher in effective limits of political micro-targeting, and other persuasive campaign techniques, is uncertain. From the perspective of the political establishment, the capacity to effectively persuade is critical to promoting their agenda and reaching out to voters in an increasingly polarised and fast-paced political ecosystem. For the sake of promoting the core principles of open debate, transparency, trust, respect, responsibility and fairness something needs to give.

---

[119] See fn. 13, p. 13; A. D. I Kramer, J. E. Guillory and J. T. Hancock, "Experimental evidence of massive-scale emotional contagion through social networks" (2014) PNAS 8788

[120] R. M. Bond, C. J. Fariss, J. J. Jones, A. D. I. Kramer, C. Marlow, J. E. Settle and J. H. Fowler, "61-million-person experiment in social influence and political mobilization" (2012) Nature 489 295-298.

[121] C. Nuttall, "Google and Facebook ban Irish vote ads" (Financial Times, May 10, 2018) https://www.ft.com/content/c6ffc5d8-544d-11e8-b3ee-41e0209208ec [Accessed July 26, 2018]

[122] The crux of the issue around the status of internet intermediaries as platforms or publishers comes down to the reach of their responsibilities, and liability, as platforms that host, package, select and disseminate content. There are segments of specific regulations that chip away at the status of internet giants as intermediaries by creating duties to remove illegal content. DCMSC's interim report concludes that an intermediary is neither a publisher nor a platform but falls within a category of its own, with distinct responsibilities and legal liabilities.

[123] See fn. 41

Reform based only on commercial and individual wrongs neglects to fully embrace these principles and introduce them back into political communication with the electorate. Further, presenting Codes of Practice as a solution to the issue is problematic. Codes of Practice are generally non-binding, they cannot impose sanctions and there is no available remedy for breaching the Code of Practice. They are meant to explain the law while going further by laying out 'good practice'. As Bob Watt argues, it would be "an unacceptable constitutional departure to allow private parties to agree a species of law between themselves" which Codes of Practice settled between political parties and overseen by the Electoral Commission (or any other regulator) would do.[124] This may be even more concerning when Codes include agreements with corporate parties as well. As Watt states, a Code of Practice is of low value, as far as Codes differ from guidance, because "signing-up people not to break the law is nugatory because it is redundant".[125] Another deeper problem relates to the chilling effect of Codes that can discourage certain behaviours that are not unlawful but are ruled-out of 'best practice' codes.[126] It is the law that must be obeyed and Codes cannot act as substitutes in the absence of laws.

Conclusion

It is certain is that a new approach to shaping political discourse and influencing democratic decision-making is emerging. The complex legal framework is characterised by overlapping, out-dated provisions and a failure to think wholesomely about protecting the democratic process in contemporary circumstances. Notwithstanding the gaps within the regulatory framework, caution should be exercised when deciding if and how to respond to the issues posed. Despite the anomaly of political advertising in the non-broadcast media, to avoid the danger of introducing restrictive codes or regulations that could affect democratic discourse, the extent to which political communication should be monitored and regulated must be carefully considered. In particular care must be exercised when delegating the judgement of what can and cannot be communicated online to corporate interests rather than independent regulators.

The GDPR does introduce more data rights and restrictions on the use of personal data as well as proactive principles and requirements. The coincidence of the GDPR coming into force with the public attention given to the scandal of Cambridge Analytica, Facebook and political campaign groups (and by implication Government Ministers) has helped to increase public awareness of data privacy. It should be clearer to political parties, groups, elected representatives and technology companies what consent amounts to and the circumstances in which sensitive personal data can be processed. However, it remains unclear how the "democratic engagement" lawful basis for processing personal data contained in section 8(e) DPA 2018 will apply to future political campaigns. In any case the matter of consent plays a critical role in attempting to re-balance the relationship between data subjects and data controllers - as long as individuals are able to realise and act upon the misuse of their data. The requirement to notify data subjects of the intended use of their data should, in theory, encourage individuals to exercise their data rights. Article 80(2) GDPR provides any body,

[124] R. A. Watt "Reflections on a New Structure for the United Kingdom's Electoral Law: A Report prepared for the Electoral Commission" (June 26, 2013) *electoralcommission.org.uk* *http://www.electoralcommission.org.uk/__data/assets/pdf_file/0007/162178/Reflections-on-a-New-Structure-for-the-UKs-Electoral-Law.pdf* [Accessed September 21, 2018] para 3.8.10.6
[125] See fn. 124, para 3.8.10.7
[126] See fn. 124, para 3.8.10.8

organisation or association the right to lodge a complaint with the supervisory authority, independent of a data subject's mandate, if data rights may have been infringed as a result of processing. Yet, section 187 DPA 2018 excludes article 80 and limits organisations or bodies to acting on behalf of data subjects only when data subjects have authorised them to do so. Article 80(2) GDPR, if incorporated into the DPA 2018 after the statutory review period (or sooner),[127] would provide a much more effective mechanism for holding controllers to account, through lodging complaints and seeking judicial remedies and compensation, where individual data subjects may not be able to or may not even know there are grounds to do so.[128]

[127] DPA 2018, s. 189 - 190
[128] See fn. 91