University of Victoria, BC., Canada

Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities

University of Victoria

Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities

Professor Colin J. Bennett
Department of Political Science
University of Victoria, BC. Canada
cjb@uvic.ca
www.colinbennett.ca

Smith Oduro-Marfo
Department of Political Science
University of Victoria, BC. Canada
soduromarfo@uvic.ca
www.privacyinafrica.com

Paper Commissioned by the UK Office of the Information Commissioner for presentation to the 2019 International Conference of Data Protection and Privacy Commissioners (ICDPPC).

Published October 2019.

ico.
Information Commissioner's Office

Contents

Executive Summary[1]

At the center of efforts to combat electoral manipulation and propaganda stands the question of how personal data on individual voters is being processed, and whether or not it is done so legally and ethically. Familiar data protection questions are now injected into this heated international debate about democratic practices, and international DPAs now find themselves at the center of a global conversation about the future of democracy.

There is a rich tradition of trying to understand the role played by effective privacy protection within different forms of democracy. For *liberal* democracy, privacy advances individual autonomy and self-fulfillment, and reinforces political competition. For *participatory* democracy, privacy bolsters participation and engagement: voting freely, speaking out, engaging in interest groups, signing petitions, participating in civil society activism and protesting. For *deliberative* democracy, privacy enhances the freedom to make choices under conditions of genuine reflection and equal respect for the preferences, values and interests of others.

We know that privacy is important *for democracy*. Until recently, we have known relatively little about how privacy has been compromised *by democracy*, and by the agents that seek to mobilise, engage and encourage us to vote – or not to vote. Modern political campaigns around the world are now meant to be "data driven" to consolidate existing support and to find potential new voters and donors. Some campaigns construct detailed profiles on individual voters to "micro-target" increasingly precise messages to increasingly refined segments of the electorate.

The balance between rights to privacy, and the rights of political actors to communicate with the electorate, will be struck in different ways in different jurisdictions depending on a complex interplay of legal, political, and cultural factors. Relevant legal provisions include: constitutional provisions and conventions relating to freedom of communication, information and association, particularly with respect to public and political affairs; data protection (information privacy) law; election law; campaign financing law; telemarketing and anti-spam rules; and online advertising

[1] The following privacy and election experts assisted in the preparation of various parts of this paper: Roger Clarke, Elizabeth Coombs, Robin Bayley and Fumio Shimpo. We are also grateful to Steven Wood and Mariam Boakye-Dankwa of the ICO for facilitating this work. Colin Bennett has been working on issues of "voter surveillance" for a number of years with the assistance of financial support from the Social Sciences and Humanities Research Council of Canada through: the *Big Data Surveillance Partnership Grant* (Grant No: 895-2015-1003) and an Insight Grant on *Micro-Targeting and Data Driven Elections in Canada* (Grant No: 435-2019-0403). We are grateful to UVIC grad students Didier Zuniga and Tim Charlebois for the research and translations on the French case below, and to Lauren Yawney and Jesse Gordon for research into micro-targeting and voter surveillance.

codes. The overall balance will also be affected by the party system, the electoral system, and campaign financing rules.

The balance will also be influenced by the political culture, and in particular the general acceptability of direct candidate-to-voter campaigning practices, such as door-to-door canvassing, or telephone polling. In some countries, it is not customary for voters to display symbols of political affiliation on their persons, their cars or their houses – as it is in others. In countries with recent memories of authoritarian rule, the sensitivity of data on political affiliation is particularly acute.

To make some sense of this complexity, we group jurisdictions depending on: 1) the strictness of regulation on the capture and processing of personal data on political opinions; and 2) the conditions under which personalised political communication is allowed. We can identify five general patterns of data-driven elections: *Permissive, Exempted, Regulated, Prohibited and Emerging*. We exemplify these patterns with reference to brief case studies on the U.S., Canada, Australia, UK, France, Japan, Kenya and Brazil.

It is widely argued that elections must now be data-driven to be effective, but there is nothing inevitable about these trends. The larger question is how much information should political parties and candidates have about those citizens in order to perform their essential roles? In general terms, how much should the political speaker be allowed to know about the audience, in order to speak effectively? In the United States, the answer is a great deal. In Japan, the answer is virtually nothing. Most other democracies fall somewhere along that continuum.

To the extent that contemporary elections are "data-driven", their worst effects have been apparent in countries whose data protection laws do not cover political parties. In most democratic countries where parties are covered by data protection law, and have been for decades, there is little evidence that these restrictions have impeded their ability to perform their basic democratic roles of political mobilization, elite recruitment and policy development.

Data protection authorities (DPAs) cannot assume that data-driven elections are confined to the United States. Increasingly, elections in other countries are data-driven, raising significant questions about the fair and accountable processing of personal data on political opinions within the "permanent campaigns" of modern democracies. These issues will require more proactive and comprehensive analysis and investigation in individual jurisdictions, as well as higher levels of international collaboration.

Introduction

In 2005, the Data Protection Authorities (DPAs) issued a joint Resolution at their international conference in Montreux and warned of "invasive profiling" and the unlawful collection of "sensitive data related to real or supposed moral and political convictions and activities."[2] The commissioners resolved that: "Any political communication activity, including those not related to electoral campaigns, which entails a processing of personal data, should respect fundamental rights and freedoms of interested persons, including the right to the protection of personal data, and should comply with data protection principles."[3]

Until relatively recently, however, most DPAs have not taken an active interest in the processing of personal data within the electoral process in their respective countries. There were some earlier guidance and rulings by the Italian Garante,[4] the French Commission de l'Informatique et Libertés (CNIL),[5] and the UK Information Commissioner's Office (ICO).[6] In most EU countries, and others in which political parties are regulated by data protection law,[7] to the extent that the DPAs have ventured into this "political" territory, their investigations and rulings have related to quite narrow issues, and have been prompted by individual complaints about the actions of particular parties and candidates during specific electoral contests.[8]

The global controversy surrounding the activities of Cambridge Analytica and Facebook has elevated questions about the use of personal data in contemporary elections to new levels, and to a far broader set of issues: the role of voter analytics in modern elections; the democratic responsibilities of powerful social media platforms; the accountability and transparency for targeted political ads; cyberthreats to the

[2] *See* 'Resolution on the Use of Personal Data for Political Communication' agreed at the International Conference of Data Protection and Privacy Commissioners, (16 September 2005), Montreux: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf

[3] Ibid.

[4] Garante per la protezione dei dati personali. (March 6, 2014). Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale. *Official Gazette of the Italian Data Protection Authority 71*. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267

[5] Commission Nationale de l'Informatique et Libertés. (November 8, 2016). *Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?*. https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.

[6] Information Commissioner's Office (ICO). (July 2018). *Democracy Disrupted: Personal Information and Political Influence.* https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf

[7] We use the term 'data protection law' throughout this paper as a shorthand for the entire family of data protection and information privacy statutes for which members of the ICDPPC are responsible.

[8] These various cases are reviewed in: Bennett, C.J. (December 2016). Voter databases, micro-targeting and data protection law: can political parties campaign in Europe as they do in North America?. *International Data Privacy Law*, Vol. 6, No. 4, 261-75 and Bennett, C. J. (June 2013). Privacy, elections and political parties: emerging issues for data protection authorities. *Privacy Laws and Business International*, Issue 123.

integrity of electoral procedures; and the spread of misinformation and "fake news" through malicious actors and automated bots.[9]

In those countries where data protection law regulates political parties, innovative forms of digital campaigning are raising new concerns and pressures. In those in which political parties are largely exempted (such as in Canada, the United States and Australia), questions are being raised about whether such exemptions are appropriate and sustainable.

To stress the different and more severe nature of data protection violations in the electoral context, the European Commission (EC) has noted:[10]

> ... the development of micro-targeting of voters based on the unlawful processing of personal data as witnessed in the case of the Cambridge Analytica revelations is of a different nature. It illustrates the challenges posed by modern technologies, but also it demonstrates the particular importance of data protection in the electoral context. It has become a key issue not only for individuals but also for the functioning of our democracies because it constitutes a serious threat to a fair, democratic electoral process and has the potential to undermine open debate, fairness and transparency which are essential in a democracy. The Commission considers that it is of utmost importance to address this issue to restore public trust in the fairness of the electoral process.

In March 2019, the European Data Protection Board (EDPB) stressed:[11]

> Predictive tools are used to classify or profile people's personality traits, characteristics, mood and other points of leverage to a large extent, allowing assumptions to be made about deep personality traits, including political views and other special categories of data. The extension of such data processing techniques to political purposes poses serious risks, not only to the rights to privacy and to data protection, but also to trust in the integrity of the democratic process. The Cambridge Analytica revelations illustrated how a potential infringement of the right to protection of personal data could affect other fundamental rights, such as freedom of expression and freedom to hold opinions and the possibility to think freely without manipulation.

---

[9] See European Commission. (September 2018). *Code of Practice on Disinformation*. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

[10] European Commission. (September 2018). *Commission guidance on the application of Union data protection law in the electoral Context.* https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf

[11] European Data Protection Board (EDPB). (March 13, 2019). *Statement 2/2019 on the use of personal data in the course of political campaigns.* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

For the European Data Protection Supervisor (EDPS), "the diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere to essential to the health of democracy."[12]

DPAs do not have jurisdiction over the entire range of questions raised by these recent scandals, but they do regulate the conditions under which the legitimate processing of personal data can occur, and upon which modern forms of political communication often depends. For example, the delivery of so-called "fake news" has a direct relationship to programmatic advertising, and to the impersonal algorithms that are designed to detect and target individual consumers, often without their knowledge and consent.[13] The documented attempts at voter suppression, such as those by the Trump campaign in 2016, relied on personalised negative messages using Facebook advertising tools, "dark posts" and targeting individual voters on the basis of race, ethnicity and socio-economic status.[14]

At the center, therefore, of efforts to combat electoral manipulation and discrimination stands the question of how personal data on individual voters is being processed in campaigns, and whether or not it is done so legally and ethically. Familiar data protection questions are now injected into this heated international debate about democratic practice. And international DPAs now find themselves at the center of a global conversation about the future of democracy. Furthermore, elected officials over the world have gradually come to realise that the inappropriate processing of personal data within elections can hurt them where it hurts most – at the ballot box. Privacy and data protection have rarely in the past been "Big P" political questions. They are now.

Thus, the DPAs and the wider community of privacy experts and advocates have an extraordinary responsibility to ensure that democracy itself is not "disrupted" through the violation of the standard norms of data protection. According to the UK Information Commissioner, Elizabeth Denham:

> Engagement with the electorate is vital to the democratic process; it is therefore understandable that political campaigns are exploring the potential of advanced data analysis tools to help win votes. The public have the right to

[12] EDPS. (March 2019). *EDPS Opinion on online manipulation and personal data.* https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

[13] Chester, J. and Montgomery, K.C. (2017). The role of digital marketing in political campaigns." *Internet Policy Review* 6, no. 4.

[14] Green, J., & Issenberg, S. (October 2016). Inside the Trump bunker, with days to go. *Bloomberg Businessweek*. https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go

> expect that this takes place in accordance with the law as it relates to data protection and electronic marketing. Without a high level of transparency – and therefore trust amongst citizens that their data is being used appropriately – we are at risk of developing a system of voter surveillance by default. This could have a damaging long-term effect on the fabric of our democracy and political life.[15]

Political parties constitute a different category of organisation; they are neither governmental nor commercial. They perform unique and essential roles in political recruitment, policy development and political socialisation and mobilisation.[16] They are (still) the mechanisms that define electoral competition and political identification within modern democracies. It is, therefore, commonly asserted that the processing of personal data by parties for the purposes of "democratic engagement" is different, and that the public interest in "knowing the electorate" should allow a wide latitude to process personal data to educate and mobilise voters.[17]

But should it? Many of the current activities of political parties can barely be distinguished from current marketing organisations: they advertise online and offline; they employ data analytics companies; they purchase space on social media platforms to reach custom audiences; and they constantly test and retest their political messaging. Some now argue that the process of convincing voters, is essentially no different from convincing consumers. Parties now "shop for votes." And voters choose parties in the same way that consumers shop for products.[18] In this context, what is the appropriate balance between privacy rights and the obligations of legitimate political actors to educate and mobilise voters? With respect to data protection principles, is there any justification for treating political parties and political communication differently?

And what do we mean by "democratic engagement"? Facebook may mean one thing. Indeed "engagement" (measured by likes, shares, reposts) is the way that Facebook and other social media platforms determine the content we receive in our newsfeeds.[19] Democratic engagement means many other, less superficial, activities: voting in elections and referenda; joining political parties and interest groups;

---

[15] See pages 8-9 in: Information Commissioner's Office (ICO). (July 2018). *Democracy Disrupted: Personal Information and Political Influence.* https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf

[16] ACE. (2012). Roles and Definitions of Political parties. *Parties and Candidates.* https://aceproject.org/ace-en/topics/pc/pca/pca01/pca01a

[17] See for instance the testimony of representatives of the main political parties to the Canadian House of Commons Committee on Access to Information, Privacy and Ethics: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-17/

[18] Delacourt, S. (2015). *Shopping for Votes: How Politicians Choose Us and We Choose them*, 2nd ed. Madeira Park, BC: Douglas and McIntyre.

[19] See the analysis by Sir Tim Berners Lee (November 2016) on this point: 'Mark Zuckerberg is in denial about how Facebook is harming our politics'. *Vox*. https://www.vox.com/new-money/2016/11/6/13509854/facebook-politics-news-bad

organising and signing petitions; running for office; lobbying lawmakers; writing letters and online posts; taking part in protests and demonstrations. Whereas the political engagement, defined by Facebook, invariably depends on surveillance, these more substantial activities require, to a large extent, strong commitments to privacy.

Those tensions are at the heart of this paper which aims to:

1) Explore the relationship and tensions between data protection (or the right to privacy) and democratic rights and freedoms, including freedom of expression and freedom of association.
2) Provide a broad analysis of the legal and regulatory landscape in relation to data protection, electoral law and democratic engagement across member countries of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and
3) Through a series of brief case studies, examine how these tensions have recently played out in different jurisdictions.

With respect to this last purpose, the paper proposes a broad comparative framework for the analysis of the relationship between privacy/data protection and the rights of political actors to communicate with the electorate. It compares the various rules and practices governing: 1) the capture and processing of personal data on political opinions: and 2) the conditions under which personalised political communication might occur. The framework is then applied to some brief country case studies.

Firstly, and primarily in the United States, the absence of a uniform data protection law, and the importance of the First Amendment that privileges political communication, produce a *permissive* context in which a voter analytics industry has flourished, and in which there are few statutory restrictions on the processing of personal data about political opinions, and the profiling of that data to deliver personalised communications to increasingly precise segments of the electorate. The voter analytics industry can of course be guilty of "unfair and deceptive trade practices," and like other commercial organizations, be regulated by the Federal Trade Commission.[20] In a second set of countries (such as Canada and Australia), political parties are generally *exempted* from data protection law. Thus, the capture of personal data on, and communication with, the electorate is constrained by other legal provisions, institutional constraints and resource limitations. In a third category of countries (mainly those governed by the GDPR or its equivalents), the capture and

[20] It was under this authority that the FTC filed an administrative complaint against Cambridge Analytica for employing "deceptive tactics to harvest personal information from tens of millions of Facebook users for voter profiling and targeting." See FTC. (August 2019). *Cambridge Analytica, LLC, In the Matter Of.* https://www.ftc.gov/enforcement/cases-proceedings/182-3107/cambridge-analytica-llc-matter

processing of personal data on sensitive "political opinions" is highly *regulated*, and personalised political communication is permitted only with the consent of the individual, or according to another clearly stipulated legal basis.

Fourthly, there are some societies (Japan is the obvious case) where both the capture of personal data on the electorate, and the communication of personalised political messaging is largely *prohibited*. In a fifth set of countries mainly in the Global South, whose democratic cultures are often more fragile, voter surveillance practices are *emergent*. In such countries, exemplified by Kenya and Brazil, personalised data capture on voters is often less regulated but also less common, and thus social media networks, and especially WhatsApp, have been employed to disseminate mass electoral propaganda.

There is no serious dispute about the importance of democratic engagement for the good of individuals, and for the good of society. The larger question, however, is how much information should political parties and candidates have about those citizens in order to perform that essential role? In general terms, how much should the political speaker be allowed to know about the audience, in order to speak effectively? In the United States, the answer is a great deal. In Japan, the answer is virtually nothing. Most other democracies fall somewhere in between those extremes.

Colin Bennett has argued elsewhere that the practices outlined in this paper constitute a form of surveillance. Just as we talk about consumer or employee surveillance, it is logical to isolate and examine *voter surveillance*, and consider its distinctive dynamics, risks and norms.[21] Voter surveillance, like surveillance more generally, is "Janus-faced"; neither simply good nor bad, but at the same time never neutral.[22] We should analyse the complex effects of these trends according to a different set of criteria than those used when we evaluate the security practices of the state, or the profit-driven consumer monitoring by the private sector. The analysis of the various cases will highlight the extent of voter surveillance in different countries, and how the range of legal, political, structural and cultural factors affect the balance between privacy and other democratic rights and practices. The paper begins with a broader discussion of the importance of privacy protection for different forms of democracy.

[21] Bennett, C.J. (2015). Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications. *Surveillance and Society*, *Vol. 13*, No. 3-4.
http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/voter_surv

[22] See page vii in Bennett, C. J., Haggerty, K. D., Lyon, D., & Steeves, V. (Eds.). (2014). *Transparent lives: surveillance in Canada*. Athabasca University Press.

The Significance of Privacy Protection for Democratic Rights

Just as there is no common agreement on the meaning of the word "privacy," there is no common agreement on the meaning of the word "democracy."[23] Both are multi-faceted phenomena; there are dimensions and types of democracy, just as there are dimensions and types of privacy.[24] The literature is replete with various categorisations of democracy: direct v. indirect (representative); parliamentary v. presidential; and procedural v. substantive.[25] There are also efforts to measure democracy and democratic practice based on complex statistical measures yielding indices of global democratic trends.[26] The relationship between privacy and democracy is obviously a complex and dynamic one.

It is obvious, however, that if privacy protection is essential for democracy, it must fulfil a public or collective purpose, rather than a mechanism just to protect the individual. Several scholars have made this point. Priscilla Regan, for example, has maintained that privacy, in addition to being a commonly held value, is also public value and collective value, precisely because it is important to a democratic political system: "Most privacy scholars emphasise that the individual is better off if privacy exists. I argue that society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public, and collective purposes."[27]

There is much contemporary thinking about the social dimensions of privacy, and how it operates as a social construction that, according to Valerie Steeves, allows us to negotiate our relationships with others.[28] Thus, Helen Nissenbaum has contended that privacy is really a social norm that dictates what information is appropriate to circulate in different social contexts.[29] And Julie Cohen insists that, in a globally networked environment, privacy is constitutive "of a particular type of civil society that prizes particular types of activities and particular types of subjects." It is best described as an

[23] Spicer, M. W. (2019). What do we mean by democracy? Reflections on an essentially contested concept and its relationship to politics and public administration. *Administration & Society, 51*(5), 724-748; Dalton, R. J., Shin, D. C., & Jou, W. (2007). Popular conceptions of the meaning of democracy: Democratic understanding in unlikely places. *CSD*. https://escholarship.org/content/qt2j74b860/qt2j74b860.pdf

[24] Solove, D. (2008). *Understanding Privacy*. Cambridge: Harvard University Press.

[25] Lijphart, A. (ed.). (1992). Parliamentary versus presidential government. Oxford: Oxford University Press; Schmitter, P. C., & Karl, T. L. (1991). What democracy is... and is not. *Journal of democracy*, *2*(3), 75-88.

[26] See, Economist Intelligence Unit. (January 8, 2019).Democracy Index. *The Economist*. https://www.economist.com/graphic-detail/2019/01/08/the-retreat-of-global-democracy-stopped-in-2018; Center for Systemic Peace. (n.d.). *The Polity Project*. http://www.systemicpeace.org/polityproject.html

[27] Regan, P. (1995). *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill: University of North Carolina Press.

[28] Steeves, V. (2009). Reclaiming the Social Value of Privacy. In Kerr, I. Steeves, V and Lucock, C. (eds). *Lessons from the Identity Frail: Anonymity, Privacy and Identity in a Networked Society*. New York: Oxford University Press, pp. 191-288.

[29] Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford: Stanford University Press.

"interest in breathing room to engage in socially situated processes of boundary management."[30]

Privacy also, of course, tends to be one of the rights that is eroded when democracy is eroded. The excessive surveillance of citizens is a feature of more authoritarian regimes.[31] It may be a creeping reality in democratic countries, which may be "sleep-walking into a surveillance society" as Richard Thomas, the former Information Commissioner of the UK once warned,[32] but the "culture of surveillance" is certainly something to be resisted and controlled if democratic practice is to thrive.[33]

In *liberal democracies*, the notion of privacy as control over personal information rests on notions of a boundary between individuals and the collective. In John Stuart Mill's words, there should be certain "self-regarding" activities of private concern, contrasted with "other-regarding" activities susceptible to community interest and regulation.[34] Following Mill, Alan Westin argued in his classic text *Privacy and Freedom* that, in contrast to totalitarian regimes, "a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life… Liberal democratic theory assumes that a good life for the individual must have substantial areas of interest apart from political participation."[35]

Westin addressed the specific functions that privacy plays in liberal democratic societies. It promotes the freedom of association. It shields scholarship and science from unnecessary interference by government. It permits the use of a secret ballot and protects the voting process by forbidding government surveillance of a citizen's past voting record. It restrains improper police conduct such as "physical brutality, compulsory self-incrimination and unreasonable searches and seizures." It also serves to shield those institutions, such as the press, that operate to keep government accountable.[36]

These are largely U.S. perspectives on *liberal* democratic rights, and represent just one version of democratic theory. Carole Pateman has argued that there are two general traditions of democratic theory.[37] One is a liberal tradition rooted in 18th century natural rights theory; the other is derived from the view that the test of a democracy is

---

[30] See page 149 in Cohen, J.E. (2012). *Configuring the Networked Self: Law, Code and the Play of Everyday Practice.* New Haven: Yale University Press.

[31] Haggerty, K. and Samatas, M. (eds). (2010). *Surveillance and Democracy*. New York: Routledge.

[32] Ford, R. (August 16, 2004). Beware rise of Big Brother state, warns data watchdog. *The Times*. https://www.thetimes.co.uk/article/beware-rise-of-big-brother-state-warns-data-watchdog-hhv3qtwgswk

[33] Lyon, D. (2018). *The Culture of Surveillance*. Cambridge: Polity Press.

[34] Mill, J.S. (1869, 1991). *On Liberty and Other Essays.* John Gray (ed). Oxford: Oxford University Press.

[35] See page 24 in Westin, A.F. (1967). *Privacy and Freedom.* New York: Atheneum.

[36] Ibid. pp. 24-25.

[37] Pateman, C. (1975). *Participation and Democratic Theory*. Cambridge: Cambridge University Press.

less about the protection of individual or minority rights, or the degree of competition between centers of power. Rather, the test is the degree of participation, cooperation, trust, and community consciousness, values that are not necessarily promoted by asserting the "right to be let alone" in the Warren and Brandeis[38] famous formulation. Under this *participatory* theory of democracy, privacy protection policy serves more to bolster trust, to give citizens the guarantee that they can engage with their democratic institutions without fear that they will be unfairly monitored and persecuted. Privacy is not about erecting boundaries but about creating the conditions under which individuals can promote self-fulfilment as democratic citizens.

This view finds support among a number of privacy theorists. Ruth Gavison, for instance, argues: "Privacy is also essential to democratic government because if fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy."[39] And Daniel Solove points out: "Privacy permits individuals to contemplate and discuss political change, create counterculture, or engage in a meaningful critique of society… People have the opportunity to develop their views, political opinions, or artistic expressions without having them prematurely leaked to the world, where harsh judgements might crush them."[40]

These rights to "political privacy" are then inseparable from rights of free speech and association. Thus, as Rubinstein argues, "there is a very strong argument that campaign data practices and voter microtargeting undermine anonymous speech by subjecting voters to a form of political surveillance in which their beliefs and preferences are monitored and tracked."[41] The monitoring of political preferences and behavior creates a chilling effect and discourages participation. Anonymous communication, a crucial dimension of privacy, promotes both personal growth and self-fulfilment, and contributes to the free flow of ideas, opinions and critique, reflective of healthy democratic practice. According to Neil Richards, how we reach decisions, and especially political decisions, can be seen as an essential element of our "intellectual privacy."[42]

In this interpretation, privacy is less about seclusion or withdrawal, and more about engagement. Privacy (or the absence of surveillance) is a necessary (but not sufficient) condition for free participation in democratic societies: voting freely, speaking out, engaging in interest groups, signing petitions, participating in civil society activism and protesting. And those conditions are important whether the activities occur online, or offline.

---

[38] Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. *Harv. L. Rev., 4*, 193.

[39] Gavison, R. (January 1980). Privacy and the Limits of the Law. *The Yale Law Journal.* vol. 89, no 3, 455.

[40] See page 80 in Solove (2008).

[41] See page 906 in Rubinstein, I. S. (2014). Voter privacy in the age of big data. *Wis. L. Rev.*, 861.

[42] See pages 179-80 in Richards, N. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age.* Oxford: Oxford University Press.

A further perspective on democracy is advanced by those who stress its *deliberative* aspects. Deliberative democracy, normally associated with the theorising of Jurgen Habermas, insists that freedom of speech and association, in themselves, are insufficient for democratic practice. Deliberation requires a mutual communication that involves a genuine reflection and common respect for the preferences, values and interests of others. Deliberation is more than discussion, and it is more than the aggregation of preferences. It should take place in a context of equal recognition, respect, and reciprocity.[43] Legitimate deliberation requires information, substantive balance, diversity, conscientiousness, and equal consideration.[44]

Twenty years ago, Paul Schwartz warned of the dangers of the "silent collection of personal information in cyberspace" and that it was "bad for the health of deliberative democracy":[45]

> It cloaks in dark uncertainty the transmutation of Internet activity into personal data that will follow one into other areas and discourage civic participation. This situation also has a negative impact on individual self-determination; it makes it difficult to engage in the necessary thinking out loud and deliberation with others upon which choice-making depends. In place of the existing privacy horror show, we need multidimensional rules that set out fair information practices for personal data in cyberspace.

Of course, it is precisely these qualities of deliberative discussion that are challenged, some would say abandoned, by the prevailing discourses within contemporary social media, with its propensities to promote "filter bubbles" and for instantaneous and superficial comment and reaction. But deliberative democratic theory provides another useful theoretical foundation from which to critique excessive surveillance on the Internet.[46]

There is then a rich tradition of trying to understand the role played by effective privacy protection within democratic societies. It plays an essential role in advancing our individual autonomy and self-fulfillment, but it also plays an instrumental function in limiting state power and strengthening democratic engagement. If societies advance privacy rights, they enhance the trust in democratic institutions that facilitates democratic engagement, deliberation and participation. That message has been consistent in the privacy and surveillance literature.

---

[43] Bachtiger, A., John S. Dryzek, Jane Mansbridge and Mark E. Warren. (2018). *The Oxford Handbook of Deliberative Democracy*. Oxford: Oxford University Press.

[44] James, F. (2009). *When the People Speak: Deliberative Democracy and Public Consultation*. New York: Oxford University Press.

[45] Schwartz, P. M. (1999). Privacy and democracy in cyberspace. *Vand. L. Rev.*, *52*, 1607.

[46] Parsons, C., Colin J. Bennett and Adam Molnar. (2015). Privacy, Surveillance and the Social Web. In B. Roessler and D. Mokrosinska (eds.). *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Cambridge: Cambridge University Press.

That said, virtually nowhere in the rich and extensive literature on privacy, data protection and personal surveillance has there been any discussion or analysis of the ways in which personal data are captured, used and processed *within* the electoral process. In a vast and sprawling literature, we find almost nothing on the monitoring of the electorate by political parties and their candidates. Almost exclusively, the focus has centered on the surveillance of citizens by agencies of the state, and/or the monitoring of consumers by the corporate sector. We know that privacy is important *for democracy*. Until recently, we have known relatively little about how privacy has been compromised *by democracy*, and by the agents that seek to mobilise, engage and encourage us to vote – or not to vote.[47]

The Secret Ballot and the Transparent Voter

Privacy protection is, of course, central to the conduct of elections. The secret (or Australian) ballot is now regarded as a test of effective administration of election procedures. It is typically defined as having four essential elements: an official ballot being printed at public expense; on which the names of the nominated candidates of all parties and all proposals appear; being distributed only at the polling place; and being marked in secret. With the introduction of postal voting and electronic (online) voting in some jurisdictions, these conditions are, of course, challenged. Continuing issues about voter privacy and the security and confidentiality of the election process, beyond the scope of this paper, are matters of enormous interest for privacy advocates.[48]

The secret ballot is normally justified in instrumental terms: it prevents or discourages attempts at bribery and intimidation. But there is a deeper, and more substantive, justification. As expressed by Anabelle Lever: "citizens' rights to vote does not depend on the approval of others, or on the demonstration of special virtues, attributes or possessions. While democratic rights to freedom of expression and association mean that citizens are free to consult anyone they want, the secret ballot means that they can share in collectively binding decisions without having to bare their souls to anyone who asks." The secret ballot, and the privacy upon which it depends, is constitutive of democratic practice. It marks our status as citizens. It is important in itself, regardless of what functions it performs.[49]

---

[47] Gordon, J. (2019). "When Data Crimes are Real Crimes: Voter Surveillance and the Cambridge Analytica Conflict," MA thesis, University of Victoria. Colin Bennett's student Jesse Gordon has canvassed this literature and found no more than one or two isolated references.

[48] See, for example, the campaign of the Electronic Privacy Information Center (EPIC) on "Voting Privacy." https://epic.org/privacy/voting/

[49] Lever, A. (2015). Privacy and democracy: What the secret ballot reveals. *Law, Culture and the Humanities*, *11*(2), 164-183.

Contrast these arguments with the sales pitch of a representative and very established voter analytics firm (Aristotle) in the U.S.:

> *Aristotle* provides the most comprehensive voter data, consumer files, and donor files anywhere — all with 24/7 Web access. Our national voter file contains over 192 million records, each with more than 500 attributes like voting histories, hobbies, demographics and more.[50]

This company does not know how people voted; in that strict sense, the secret ballot is not violated. But its products, and those of others in the voter analytics industry, surely serve as highly detailed surrogates from which actual voting might be inferred and predicted. These products, and many others, flow from a growing conventional wisdom, whether accurate or not, that modern political campaigns need to be "data driven" to consolidate existing support and to find potential new voters and donors. The capture and consolidation of these data permit the construction of detailed profiles on individual voters and the "micro-targeting" of increasingly precise messages to increasingly refined segments of the electorate. Despite the universal acceptance of the procedure of secret balloting, voters are becoming increasingly transparent to a variety of actors, public and private, in the U.S. and increasingly elsewhere.

In a recent report, the Tactical Tech collective has portrayed the contemporary political "influence industry." The overall message is that "political parties are using the same techniques to sell political candidates to voters that companies use to sell shoes to consumers."[51] There is nothing new about the practice of branding political candidates and messages,[52] although the granularity, speed and scale with which political messages can now be targeted is unprecedented.

The report makes a useful distinction between data as a *political asset*, as *political intelligence*, and as *political influence*. Political data operates as an asset through more traditional databases or voter relationship management systems, the sources for which include voter registration records, polling data, information from commercial data brokers and data collected by the parties themselves while campaigning (on the doorstep, over the phone, online). Data operates as *intelligence* when it is accumulated as a result of testing and experimentation.

---

[50] Aristotle. *Political Data.* http://aristotle.com/data/

[51] Tactical Tech. (March 2019). *Personal Data: Political Persuasion – Inside the Influence Industry. How it works.* Berlin: Tactical Tech. https://tacticaltech.org/#/projects/data-politics/

[52] Packard, V., & Payne, R. (1957). *The hidden persuaders*. New York: D. McKay Company.

Sasha Issenberg revealed the extent of these practices in *The Victory Lab* – "the secret science of winning campaigns."[53] A/B testing is common in campaign circles to understand the impact of website design, emails, text, design elements, slogans, direct mail as well as TV and radio ads. Data operates to *influence* when it is used to micro-target individuals to vote (or not vote), to donate, to volunteer and so on. A variety of micro-targeting practices are discussed: geofencing (promoting a message only to individuals inside a geographic perimeter); IP targeting (using location-based information from IP addresses); mobile or property geotargeting; robocalling and mobile texting; addressable TV; and psychometric profiling (the practice for which Cambridge Analytica became notorious).

Whereas it was once possible to distinguish the different kinds of organisations associated with political campaigning, the current network of institutions is now more complex and opaque. Research has demonstrated close alliances between political data brokers, digital advertising firms, data management and analytical companies, and political parties in the "campaign ecosystem." Increasingly the modern political campaign in the United States, and increasingly elsewhere, relies on a network or "campaign assemblage" to conduct and integrate all the roles perceived as necessary to getting elected: data collection; data analytics; polling; fund-raising; data analytics; digital advertising; TV advertising; email and text outreach; social media outreach; event management; volunteer coordination; and get-out-the-vote (GOTV) operations. Each of these roles requires careful coordination.[54]

Jeff Chester and Kathryn Montgomery trace the ongoing "marriage of politics and commerce" and the ongoing growth of data-driven political marketing.[55] They reviewed seven key techniques employed during the 2016 campaigns in the US, all of which point to massive efforts at consolidation in the digital marketing ecosystem: cross-device targeting; programmatic advertising; lookalike modelling, such as that offered through Facebook; online video advertising; targeted TV advertising; and psychographic, neuromarketing and emotion-based targeting. Political micro-targeting is then virtually indistinguishable from contemporary programmatic advertising practices of the adtech sector, including the highly controversial process of "real-time bidding" (RTB), which has come under recent scrutiny from DPAs.[56]

The picture is not solely one of the amalgamation and centralization of Big Data to the benefit of central party operations. These trends are offset by the development of campaigning techniques that have harnessed the more decentralizing powers of

[53] Issenberg, S. (2013). *The victory lab: The secret science of winning campaigns*. Portland: Broadway Books.
[54] Nielsen, R.K. (2012). *Ground Wars: personalised Communication in Political Campaigns*. Princeton: Princeton University Press.
[55] Chester and Montgomery (2017).
[56] ICO. (June 2019). *Update report into adtech and real time bidding.* https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

mobile applications. In recent election cycles, mobile apps have been used for: more traditional one-way political messaging; for door-to-door canvassing; for event management; for encouraging donations; and for broader civic engagement. The website Capterra.com lists over 50 products with a range of features designed to manage election campaigns, grassroots organising, fund-raising, advocacy, constituency building and so on.[57] Smart canvassing technologies facilitate the more widespread lateral sharing of personal information on who votes and for whom, and have the potential to place data on political affiliations, beliefs, and behaviour in the hands of ordinary campaign workers and volunteers who may have little privacy and security training.[58] They also, of course, permit the monitoring of the performance of those volunteers and workers. In this sense, those involved in electoral campaigns are also under surveillance.

In summary, the formal confidentiality of the secret ballot is contrasted with the increasing surveillance of voters, donors and campaign workers. To a large extent, these trends are driven by new technologies and by the introduction of consumer marketing practices into political campaigning. But they are equally precipitated by the intense competitiveness of modern elections, and by a pervasive international assumption among political and technical elites that more and better data on the electorate can help win elections and consolidate political power.

From Mass-Messaging to Micro-targeting

The practices described above are all designed to facilitate a more personalised set of communications with voters. This practice, at least in the electoral world, typically gets described as "micro-targeting" and represents a shift from geographic-based targeting to individualized communication based on predictive models and scoring of an individual's propensity to support a particular party.[59]

Here is a representative definition: political micro-targeting involves "creating finely honed messages targeted at narrow categories of voters' based on data analysis 'garnered from individuals' demographic characteristics and consumer and lifestyle habits."[60] The ICO has noted that micro-targeting "describes targeting techniques that use data analytics to identify the specific interests of individuals, create more relevant

[57] http://www.capterra.com/political-campaign-software/

[58] On the need for a comprehensive approach to training in security and privacy, see McEnvoy, M. (February 2019). *Full Disclosure: Political Parties, Campaign Data and Voter Consent.* Investigation Report P19-01. https://www.oipc.bc.ca/investigation-reports/2278

[59] Endres, K., & Kelly, K. J. (2018). Does microtargeting matter? Campaign contact strategies and young voters. *Journal of Elections, Public Opinion and Parties*, *28*(1), 1-18.

[60] Gorton, W. (2016). Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy, *New Political Science*, no. 1. pp. 61-80. https://doi.org/10.1080/07393148.2015.1125119

or personalised messaging targeting those individuals, predict the impact of that messaging, and then deliver that messaging directly to them."[61] These individualised scores of voting intention, based on multiple layers of data, are then aggregated to inform the strategic decisions of the campaign.[62]

It is impossible to pinpoint an exact point at which micro-targeting techniques entered the world of politics, and disagreement over the term captures anything more than a classic form of behavioral advertising seen in the consumer world for decades.[63] Nevertheless, the skilled way that data analytics were employed in the two elections won by Barack Obama in 2008 and 2012 has led to a general assumption that all campaigns now need to be data-driven to be successful. The Obama campaigns did not just use the Internet to broadcast the candidates' messages, they also enabled supporters to connect and self-organise. By integrating social-networking features into the Obama websites, the campaign converted online energy into offline activism. The Obama campaigns became "prototypes," attracting new digital experts to political campaigning and reshaping their understanding of electoral politics.[64]

Political micro-targeting is now widely regarded as unprecedented in its scale and precision.[65] At one extreme, the "micro" may be so precise that one-on-one messaging is seen as possible. Jim Messina, Obama's campaign manager in 2008 and 2012, and a consultant to the UK Conservative Party in 2017, argued just days before the 2016 U.S. Presidential election: "Huge data sets are often less helpful in understanding an electorate than one or two key data points — for instance, what issue is most important to a particular undecided voter….. With "little data," campaigns can have direct, highly personalised conversations with voters both on- and offline, like an ad on a voter's Facebook page addressing an issue the voter is passionate about."[66] The company, NGP VAN, the main voter relationship management platform supporting the Democratic Party, presented a vision of a "Unified View" of any individual voter. The firm aspires to reveal, from multiple sources of data, a person in their whole – a person as a person, rather than as a collection of isolated variables.[67]

---

[61] See page 27 in ICO. (2018). *Democracy Disrupted.*

[62] See page 53 in Nickerson D.W. and Rogers T. (2014) Political Campaigns and Big Data. *The Journal of Economic Perspectives, 28* (2).

[63] Chester, J. and Montgomery, K, (December 2017). The role of digital marketing in political campaigns. *Internet Policy Review: Journal of Internet Regulation, Volume 6,* No. 4.

[64] See page 16 in Kreiss, D. (2016). *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy*. Oxford: Oxford University Press.

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

[66] Messina, J. (November 3, 2016). The Election Polls that Matter. *New York Times. https://www.nytimes.com/2016/11/03/opinion/campaign-stops/the-election-polls-that-matter.html*

[67] Quoted in Kreiss, D. (2016). *Prototype Politics*. See pages 215-216.

These blanket claims obscure the obvious reality that micro-targeting can be conducted across a number of different variables. The practice varies along a continuum with the "unified view" of the voter at one extreme end, and the mass general messaging to the entire population at the other. Most "micro-targeted" messages fall somewhere in between and are more or less "micro" depending on location, target audience, policy message, means of communication and so on. Thus, micro-targeted messages might be directed towards a precise demographic in many constituencies. But they may equally be directed towards a broader demographic within a more precise location. A precise and localised policy promise, for instance, might appeal to a very broad population within a specific region.

Furthermore, micro-targeting will only be as good as the modelling that drives the algorithms. If the assumptions about the electorate are incorrect, then the messaging will also be redundant. It is also presumed, in much of the recent literature, that micro-targeted messages are associated predominantly with Facebook. This is not necessarily true; micro-targeting might find audiences through many means of communication – email, text, phone, as well as paper leaflets and signage.[68] The effective message in an election campaign must account for content, audience, timing and means (the what, who, when and how). That is a complex and interactive set of variables.

Micro-targeting clearly has "macro effects."[69] However, we should not overstate the value of micro-targeting strategies to the modern election campaign. Popular writing about these technologies, as well as the corporate hype, typically oversells the impact of these practices. There is plenty of mythology surrounding data-driven campaigns, and evidence that these techniques are far more effective at mobilising adherents than in persuading voters to change their attitudes and behaviour.[70] Whether it works or not is largely besides the point. The practices still raise a host of critical privacy questions.

Models of Personal Data Capture and personalised Political Communication

Given the mythology and the complexity, how can we make sense of the use of personal data in elections in different jurisdictions, and the regulatory conditions that facilitate or constrain its use? It is possible to group jurisdictions depending on: 1) the strictness of regulation on the capture and processing of personal data on political opinions/affiliations; and 2) the conditions under which personalised political

[68] See pages 272-44 in Issenberg (2013)
[69] See page 3 in Hankey et. al (2018)
[70] Baldwin-Philippi, J. (2017). The myths of Data-Driven Campaigning. *Journal of Political Communication. Vol 34,* No. 4.

communication is permitted and accepted. From this, we have identified five general patterns: *Permissive, Exempted, Regulated, Prohibited and Emerging*. These are presented as "models" and they do obscure some considerable legal and political complexity. The aim of this framework is to provide a comparative reference point for the understanding of the current state of data-driven elections in different societies. Under each model, we briefly discuss one or two representative case studies.

Permissive personal data capture and personalised political communication (Case study: United States)

The overall constitutional, legal, political and cultural conditions in the United States make the most favorable environment for the capture and processing of personal data on individual voters, and the micro-targeting of precise messages using all the available digital techniques outlined above. The convergence of circumstances produce a unique context for the most permissive conditions for voter surveillance.

Constitutionally, political speech has always enjoyed extraordinarily high levels of protection under the U.S. Constitution. Under well-established doctrine, political speech is central to the very meaning of the First Amendment's guarantees of freedom of speech, especially during campaigns for political office.[71] Any attempts to regulate the collection, processing and communication of personal data for political campaign purposes would likely face a very high standard of "strict scrutiny" by the courts, because they would "limit the type and amount of personal data that could be captured on voters and affect the content and quality of political messaging"[72] There is even a larger debate about whether fair information principles are inherently violative of the First Amendment, in that they involve "troubling implications of a right to stop people from speaking about you."[73] The principle that my free speech rights are affected if I know less about the interests and beliefs of the listener is a strong one within First Amendment doctrine.

Other relevant constitutional principles implicate the regulation of the use of voter analytics in elections. The "third-party" doctrine articulated in U.S. v. Miller (1976) and Smith v. Maryland (1979) held that individuals have no reasonable expectation of privacy in records held by a third party.[74] Under this doctrine, if an individual provides information to a third party, the Fourth Amendment does not preclude the government from accessing it without a warrant. Although the doctrine is under challenge in the digital age, it is still the law that citizens enjoy no "reasonable

[71] See page 912 in Rubinstein (2014).
[72] Ibid.
[73] Volokh, E. (2000). Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You. *52 STAN. L. REV. 1049,* 1050–51.
[74] Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller , 425 U.S. 435 (1976)

expectation of privacy" when their information is held by a third party, such as a bank, telecommunications provider, or, one can infer, a data-mining company.[75] Further jurisprudence over the First Amendment protections for *commercial speech* affect the ability to regulate data mining companies, and restrict the massive economy in personal data profiling.[76]

From the point of statutory privacy protections, it is commonplace to point out that the United States has never passed a uniform or comprehensive privacy protection statute, opting instead for more reactive sectoral regulations, and according to separate analysis of the risks associated with the processing of particular types of data. Those were conscious policy choices made in the 1970s, which have had legacies and implications for domestic, and international, data protection policy. The obvious result has been a patchwork of inconsistent federal and state legislation, and areas of personal data collection that have fallen between the cracks.[77]

There are many defences and critiques of the U.S. model, and contemporary efforts to develop more omnibus approaches at federal, and most especially state levels. But combined with the constitutional protections of political data under the First Amendment, the patchwork has led to a situation where, as Rubinstein contends, "voter data may be the largest concentration of unregulated personal information in the U.S. today."[78] Daniel Kreiss also points out that "institutional political actors. . . such as parties, candidates, and advocacy organisations, currently enjoy wide latitude to collect and store political data under the auspices of political speech."[79]

Beyond information privacy law, two other major differences between the United States and other democratic countries bear emphasis. The first, of course, are the very permissive campaign financing rules. The spending of money on campaigns and candidates is protected by the First Amendment. This freedom extends to both individuals, and under a series of Supreme Court decisions (most notably, *Citizens United v. Federal Elections Commission*), to corporations and other organisations, which now operate SuperPacs through which campaign contributions can be channelled to candidates.[80] The complexities of U.S. campaign financing regulations are beyond the scope of this paper, but the comparative freedom to raise money from different

[75] See page 139 in Solove (2008).
[76] In *Sorrell v. IMS Health*, the U.S. Supreme Court invalidated a Vermont statute that prohibited data mining companies from using physician prescription data for marketing purposes, holding that governments could not engage in "content" or "viewpoint" discrimination against marketers by prohibiting the commercial use of this data while permitting its non-commercial use.
[77] O'Connor, N. (January 2018). Reforming the U.S. Approach to Data Protection and Privacy. *CFR*. https://www.cfr.org/report/reforming-us-approach-data-protection; Gellman, R. M. (1993). Fragmented, Incomplete and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions. *Software Law Journal* VI: 199-238
[78] See page 881 in Rubinstein (2014).
[79] Kreiss, D. (2011). Yes we can (profile you): A brief primer on campaigns and political data. *Stan. L. Rev. Online*, *64*, 70.
[80] Citizens United v. Federal Election Commission, 558 U.S. 310 (2010)

sources, and to spend it without the overall limitations on campaign spending common in most other systems, gives campaigns (presidential, congressional, and state) an enormous latitude to employ the technical consultants, software companies, and the data analysts necessary to engage in data-driven elections.

A second difference relates to the process of voter registration in the U.S. There is no automatic registration process. By and large, the individual voter has to take the initiative to register at the appropriate place, and appropriate time, before voting day. Under the 1993 National Voter Registration Act, states are required to make the process of voter registration easier, including allowing citizens to register when they renew their drivers' licenses. But state registration rules still vary considerably. Some have same-day registration; others require registration weeks beforehand. Some require complex form-filling, others are simpler.

States have diverse requirements on who is eligible to request a list of voters, what information the list contains, what information is kept confidential, and how the information contained in voter lists may be used. In some states the lists are confined to "non-commercial" purposes. In others, there are no restrictions. Most states list categories of personal data (such as the social insurance number, date-of-birth, drivers licence number) that must be kept confidential. In others, the availability is more open. What is common, and unique, however, is the collection of data on party affiliation – Democratic, Republican or Independent. This is mainly necessary because of the system of primary elections, which require states to regulate who may vote in which Republican or Democratic primary. In some states, both voter status and voter history are also available.[81]

The availability of voter registration data was also facilitated by the Help America Vote Act (HOVA) of 2002, passed in the wake of the irregularities and inefficiencies in the 2000 elections. HOVA requires states, among other things, to maintain a "single, uniform, official, centralised, interactive computerised statewide voter registration list."[82] This legislation helped lay the groundwork for political parties to build massive databases on voters, and also for commercial data brokers to get into the business of compiling, analysing and selling voter intelligence data. In standardising lists of voters, HOVA made it easier to merge voter lists with other sources of personal data — public and commercial.[83]

The scandal concerning the harvesting of Facebook data by Cambridge Analytica has, of course, prompted a flurry of investigative activity in Congress and some highly

[81] National Conference of State Legislatures. *Access to and Use of Voter Registration Lists*. http://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx

[82] See Section 303 of the Help America Vote Act (HAVA). http://www.eac.gov/assets/1/workflow_staging/Page/41.PDF

[83] See page 64 in Hersh, E. (2015). Hacking the Electorate: How Campaigns Perceive Voters. Cambridge: Cambridge University Press.

publicized rulings by the Federal Trade Commission. The FTC has fined Facebook $5 billion for repeated deceptive trade practices. In a separate administrative complaint, they initiated a separate legal action against CA for deceptively harvesting the personal information of millions of users through a personality app, and matching against U.S. voter records.[84] There has been a number of separate laws suits at state and federal levels. Most recently, a suit by the Attorney-General of the District of Columbia has alleged that Facebook knew about Cambridge Analytica's "improper data-gathering practices" months before they were first publically reported, and violated DC's consumer protection laws.[85]

In summary, the regulation of personal data in the electoral context in the U.S. is virtually inseparable from the wider approach to consumer privacy protection. Strong penalties are available if litigation can prove "unfair and deceptive trade practices." Further regulatory action is dependent on a myriad of federal and state laws that tend to protect personal data on a sectoral level. However, the statutory law on the use of personal information in election campaigns remains essentially the same. As a response, Senator Feinstein has introduced a *Voter Privacy Act* to give voters more control over the personal information used by parties and candidates in federal election campaigns. The Bill would provide rights of access, notice and deletion, and would prohibit the transfer of data, and targeting. The requirements would not apply to information obtained from state and local voter registration databases.[86] It is not expected to pass.

Nowhere are elections more "data-driven" than in the United States. Nowhere else has the world of consumer and political marketing been so thoroughly merged. Nowhere else is the political "influence industry" more extensive. Nowhere has the divisive effects of the non-transparent, digital campaign ads as part of the "stealth media"[87] and its potential to reinforce "echo-chambers"[88] and "filter bubbles" been more acutely felt. To a large extent the legal, constitutional, political and cultural conditions of the U.S. are exceptional. It is important, therefore, not to generalise from the U.S. experience, even though the larger story about data-driven elections is very much one about the export of practices pioneered in the U.S. to other political systems.

---

[84] For an overview of these decisions see the EPIC Facebook pages: https://epic.org/foia/ftc/facebook/#

[85] Romm, T. (June 2019). D.C. attorney general's lawsuit against Facebook can proceed, judge rules. *Washington Post*. https://www.washingtonpost.com/technology/2019/06/01/dc-attorney-generals-lawsuit-against-facebook-can-proceed-judge-rules/?noredirect=on

[86] *Feinstein Bill would give voters control over their data*. (July 31, 2019). https://www.feinstein.senate.gov/public/index.cfm/press-releases?id=B4FBA307-B050-4623-8EAF-841DCDCAFDA4

[87] Kim, Y. M., Hsu, J., Neiman, D., Kou, C., Bankston, L., Kim, S. Y., ... & Raskutti, G. (2018). The stealth media? Groups and targets behind divisive issue campaigns on Facebook. *Political Communication*, *35*(4), 515-541.

[88] Harris, L., & Harrigan, P. (2015). Social media in politics: The ultimate voter engagement tool or simply an echo chamber? *Journal of Political Marketing, 14*(3), 251–283.

Exempted political parties and personalised political communication (Case studies: Canada and Australia)

Both Canada and Australia represent examples of federal countries where privacy protection laws have been passed incrementally at federal and state or provincial levels, and sequentially to cover first the public sector, and then the private. As a result, certain data controllers, including political parties, have slipped through the cracks of the overall privacy protection framework. These regulatory gaps have allowed the introduction of a variety of data-driven campaigning practices, which have gradually come to the attention of the media, civil society groups and the wider public.

Canada

The Supreme Court of Canada has determined that political parties occupy a special role under the *Canadian Charter of Rights and Freedoms* as they act as "both a vehicle and outlet for the meaningful participation of individual citizens in the electoral process."[89] The Charter provides citizens the right to engage in democratic participation through political parties, and in turn ensures that political parties are free from unreasonable restrictions on their interactions with citizens.

Political parties in Canada, like in the US, and unlike in Europe, are generally not subject to federal or provincial privacy laws. Therefore, the extent to which candidates, parties and their local associations abide by commonly enforced principles of information privacy protection is largely a matter of choice, rather than compulsion. For the most part, individuals have no legal rights to learn what information is contained in party databases, to access and correct those data, to remove themselves from the systems, or to restrict the collection, use and disclosure of their personal data.[90]

The vast majority of public and private organisations in Canada are regulated by federal and/or provincial privacy protection legislation; the fact that political parties are not is attributable to the piecemeal process through which these laws developed at federal and provincial levels. Unlike countries with uniform data protection regimes, Canada's experience was incremental, thus leaving some categories of organisation unregulated.[91] Political parties stand as the principal example of those

[89] Figueroa v. Canada (Attorney General), 2003 SCC 37, [2003] 1 S.C.R. 912 para 37, 39

[90] Bennett, C.J. and Bayley, R.M. (March 2012). Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis. *Office of the Privacy Commissioner of Canada*. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/#toc3a; Judge, E. and Pal, M. (2014). Privacy and the Electorate: Big Data and the personalization of Politics. *University of Ottawa Center for Law, Technology and Society*. http://techlaw.uottawa.ca/sites/techlaw.uottawa.ca/files/judge_pal_privacyandtheelectorate_ksg_report_oct_14_final.pdf.

[91] See, Office of the Privacy Commissioner of Canada. (January 2018). Overview of Privacy Legislation in Canada. *Office of the Privacy Commissioner of Canada*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.

agencies that "fell through the cracks" of a privacy regime that regulates either public bodies, or organisations involved in commercial activity.

The exception to this trend is British Columbia, whose Personal Information Protection Act (PIPA) applies broadly to "organisations" (other than public bodies) regardless of whether or not they are engaged in commercial activity. Therefore, the Office of the Information and Privacy Commissioner of BC (OPICBC) has jurisdiction over political parties, and has already conducted three investigations. One involving the BC New Democratic Party (BC NDP), and the other involving the BC Liberals, served to establish that the OIPCBC did indeed have jurisdiction in this area.[92] Those precedents led to a broader analysis of compliance with PIPA by all major political parties in BC, published in 2019.[93] This report concluded that BC political parties needed to be more transparent about how they collect data on voters; too much was being gathered without the individual's consent. The parties are now expected to revise their privacy policies and reform their practices in consultation with the OIPC BC and the Chief Electoral Officer. The investigation stands as the only comprehensive review of political parties' processing of personal data, outside the UK.

The additional question is whether or not BC PIPA applies to federal political parties to the extent that they campaign in BC. The Commissioner has adjudicated that question and rejected arguments by a federal political party that federal law is paramount, and that constitutionally PIPA should not regulate federal elections. The actual facts of the case have yet to be decided, but the decision does pave the way for the riding associations affiliated with federal political parties to be subject to exactly the same privacy rules as their provincial counterparts, to the extent that they operate in BC. The issue is not settled by any means, but this decision is likely to have wider ramifications.[94]

Canadian political parties do have legislative responsibilities for the protection of personal information mandated by the federal *Canada Elections Act*, which provides that no person may knowingly use personal information that is recorded in a list of electors for a purpose other than the one specified above or at a federal election (or referendum), and there are penalties for failing to comply in Part 19 of the Act.[95] The problem, however, is that these regulations only apply to this one source of data and

[92] Office of the Information and Privacy Commissioner of BC. *Summary of the Office of the Information and Privacy Commissioner's Investigation of the BC NDP's use of social media and passwords to evaluate candidates*. https://www.oipc.bc.ca/mediation-summaries/1399; Office of the Information and Privacy Commissioner of BC. (August 2013). *Sharing of Personal Information as Part of the Draft Multicultural Strategic Outreach Plan: Government of British Columbia and BC Liberal Party*. https://www.oipc.bc.ca/investigation-reports/1559

[93] Office of the Information and Privacy Commissioner of BC. (February 2019). *Full Disclosure: Political Parties, Campaign Data and Voter Consent*. https://www.oipc.bc.ca/investigation-reports/2278

[94] Office of the Information and Privacy Commissioner of BC. (August 2019). *Coutenay-Alberni Riding Association of the New Democratic Party of Canada*. https://www.oipc.bc.ca/orders/2331

[95] *Canada Elections Act*, SC 2000, c 9, s 275.

not from the wider sources of data that parties may collect from individual voters, or from third parties.[96]

Political parties and other political entities are also exempt from the "Do not Call List" procedures implemented through the Canadian Radio-Telecommunications Commission (CRTC). As provided for in section 41.7 of the *Telecommunications Act*, the National DNCL Rules do not apply in respect of a telecommunication made by a registered party, a party candidate or a nomination or leadership contestant. They are obliged, however, to comply with some of the basic telecommunications rules for unsolicited calling, such as identifying the person on whose behalf the call is made, providing contact information, and displaying the originating phone number. They must also maintain an internal do not call list, but are not obliged to disclose this to callers, or in their privacy policies.[97] Parties are also exempt from the Canadian Anti-Spam legislation (CASL) if the primary purpose of the message is to solicit a contribution, although, as discussed below, some say that they comply voluntarily, by including an unsubscribe option at the end of an email.[98]

This patchwork of incomplete legislative requirements has reached the attention of parliamentary committees, regulatory agencies, civil society organisations and the media. As a result of a scandal involving robocalling during the 2011 federal election, and the ensuing investigation by Elections Canada, questions were raised about the larger role that data analytics plays in Canadian elections.[99] The pressure has mounted as a result of the wider Cambridge Analytica scandal in 2017 and 2018. The House of Commons committee on Access to Information, Privacy and Ethics (ETHI), after a series of hearings into the vulnerabilities of Canada's democratic system arising from the breach of personal data involving Cambridge Analytica and Facebook, recommended "that the Government of Canada take measures to ensure that privacy legislation applies to political activities in Canada, either by amending existing legislation or enacting new legislation."[100] Federal and provincial privacy commissioners have also called for political parties to be brought within Canada's privacy laws.[101] A public campaign has been launched by the Vancouver-based civil society organisation, Open

[96] Bennett and Bayley. (March 2012).

[97] Canadian Radio-television and Telecommunications Commission. Rules for Unsolicited Telecommunications made on behalf of Political entities. *Government of Canada.* https://crtc.gc.ca/eng/phone/telemarketing/politi.htm.

[98] Canadian Radio-television and Telecommunications Commission. (n.d.). Frequently Asked Questions about Canada's Anti-Spam Legislation. *Government of Canada.* https://www.crtc.gc.ca/eng/com500/faq500.htm.

[99] Chief Electoral Officer of Canada. (2013). *Preventing Deceptive Communications with Electors.* http://www.elections.ca/res/rep/off/comm/comm_e.pdf

[100] See page 35 in: House of Commons Standing Committee on Access to Information, Privacy and Ethics. (June 2018). *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*.

[101] Office of the Privacy Commissioner of Canada. (May 30, 2018). *Remarks at presentation before the Senate Open Caucus.* https://www.priv.gc.ca/en/opc-news/speeches/2018/sp-d_20180530/; Ontario Information and Privacy Commissioner. (2017). *Thirty Years of Access and Privacy Service, 2017 Annual Report.*

Media[102] and public opinion surveys demonstrate that the Canadian public supports extending privacy protection law to political parties.[103]

In response, the Government of Canada introduced, as part of the *Elections Modernization Ac*t (Bill c-76), some modest provisions requiring parties to develop privacy codes of practice and to file them with Elections Canada. The law requires political parties to have a publicly available, easily understandable policy describing the collection, protection and sale of personal information, procedures for staff training, and the identity of a designated person to whom privacy concerns can be addressed. The submission of this policy is a part of their application for registration with Elections Canada.[104]

These provisions were greeted with almost universal criticism for their incompleteness, vagueness and lack of any real enforcement mechanism.[105] In consultation with Elections Canada, the Privacy Commissioner has recommended amendments, to ensure that the privacy policies are consistent with the principles found in Schedule 1 of PIPEDA, and that his office be given responsibility for oversight.[106] It is not expected that there will be any further progress on these issues, before the upcoming federal election in October 2019, even though there is likely to be close attention to the parties' campaigning practices, and particularly to the use of Facebook for the delivery of political messaging.[107]

Australia

At a constitutional level, as in Canada, the High Court has ruled that an essential element of parliamentary democracy is the discussion of political and economic issues, during and between election periods.[108] As in other parliamentary democracies, the

---

[102] Open Media. *Privacy Laws Should Apply to Political Parties*. https://act.openmedia.org/C76?utm_source=nom&utm_medium=slideshow&utm_campaign=7144&tdid=1690

[103] Curry, B. (June 13, 2019). Majority of poll respondents express support for extending privacy laws to political parties. *The Globe and Mail.* https://www.theglobeandmail.com/politics/article-majority-of-poll-respondents-express-support-for-extending-privacy/

[104] Bill C-76, *Elections Modernization Act: An Act to amend the Canada Elections Act and consequential amendments*, 1st Sess, 42nd Parliament, 2018 (first reading 30 April 2018).

[105] Bennett, C.J. (May 7, 2018). Election bill does little more than reinforce the status quo. *IPolitics*. https://ipolitics.ca/2018/05/07/election-bill-does-little-more-than-reinforce-the-status-quo/; Scassa, T. (May 2018). *A federal bill to impose privacy obligations on political parties in Canada falls (way) short of the mark*. http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=276:a-federal-bill-to-impose-privacy-obligations-on-political-parties-in-canada-falls-way-short-of-the-mark&Itemid=80.>.

[106] Office of the Privacy Commissioner of Canada. (2018). *Appearance before the Standing Committee on Procedure and House Affairs on the study about Bill C-76, Elections Modernization Act.* https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_20180605/#amendments

[107] Bennett, C.J. (2019). Data-Driven Elections in Canada: What we Might Expect in the 2019 Federal Election Campaign. *Journal of Parliamentary and Political Law 13* JPPL, 301-313.

[108] Reviewed in para. 41 of: Australia Law Reform Commission. *For your information: Australian privacy law and practice.* https://www.alrc.gov.au/publications/41.%20Political%20Exemption/exemption-registered-political-parties-political-acts-and-pract

doctrine of parliamentary privilege, protecting freedom of speech and debate, providing legal immunity for anything they say and do in the course of parliamentary debate, and generally allowing both House of Representatives and Senate to administer their own affairs has also been held to limit the application of statutory privacy rules to the representative function.[109]

As in Canada, the development of privacy protection law has developed incrementally, first covering government agencies, and a limited number of other organisations, under the original Privacy Act of 1988, and then extending in 2000 to cover the private sector, through the application of a general set of 13 Australian Privacy Principles.[110] But the act only applies, controversially, to private sector organisations with an annual turnover of $3 million, as well as some other small business organisations operating in sensitive areas. The Act also does not apply to the activities of state or territory governments, whose agencies are subject to specific privacy legislation. As in Canada, the reach of privacy law across the Australian federation is still not comprehensive.[111] And as in Canada, the privacy laws of Australia also leave political parties unregulated, at Commonwealth and state levels.

The existence of party databases has also been subjected to media scrutiny in Australia. There have been a series of stories in the media about inappropriate communications with voters, about the non–consensual capture of personal data by parties and candidates, and about data breaches going back several years. The global effects of the Cambridge Analytica scandal have led to heightened public and media consciousness about how personal data is being captured and profiled by Australian political parties. In February 2019, reports that Australian political parties had been hacked by "sophisticated state actors" (rumoured to be China) led to renewed calls for parties to be brought under the Privacy Act, and its data breach reporting requirements.[112] There has also been criticism of the matching of email addresses, social media profiles through the company, Nationbuilder[113] and of the parties' use of email tracking tools.[114]

Unlike in Canada, however, political parties are *explicitly* exempted from privacy legislation when carrying out an exempt political activity such as campaigning in an

[109] Ibid.

[110] Australian Privacy Principles. *OAIC*. https://www.oaic.gov.au/privacy/australian-privacy-principles/

[111] Privacy in your state. *OAIC*. https://www.oaic.gov.au/privacy/privacy-in-your-state/

[112] Crowe, D. (February 18, 2019). Political Parties should be stripped of Privacy Act exemptions after hack: experts. *Sydney Morning Herald*. https://www.smh.com.au/politics/federal/political-parties-should-be-stripped-of-privacy-act-exemptions-after-hack-experts-20190218-p50ymh.html

[113] Kaye, B. and Paul, K. (May 4, 2018). After Data Scandals, Australia faces an election under heavy profiling. *Reuters*. https://www.reuters.com/article/us-australia-election-data/after-data-scandals-australia-faces-an-election-under-heavy-profiling-idUSKCN1SB012

[114] Bogle, A. (May 2019). How the Australian federal election invaded your inbox with email tracking tools. *ABC News*. https://www.abc.net.au/news/science/2019-05-02/email-tracking-parties-lobby-groups-australian-federal-election/11056186

election, a referendum or any other aspect of the political process. The Act not only exempts registered political parties and political representatives, but also contractors and subcontractors of registered political parties and their representatives and volunteers of registered political parties.[115] So this raises the obvious question about whether consulting or data analytics companies are exempt from the Privacy Act responsibilities when carrying out work for a party or representative.[116] Non-commercial phone calls, email or text messages are also exempt from the requirements of the Do Not Call Register, and from the commercial spam and telemarketing rules.[117]

The Commonwealth Electoral Act authorises any registered political party or candidate to receive the electoral roll and to send political messaging to any voter. It is illegal under the Act to use the information "for anything other than election purposes." Although the Australian Election Commission (AEC) has from time to time investigated breaches of this provision,[118] it has "no power under the Electoral Act to regulate the content of electoral advertising, or restrict the amount of electoral advertising that candidates and political parties may choose to communicate to electors or the manner in which they communicate with electors."[119]

In 2008, the Australian Law Reform Commission (ALRC) engaged in a thoughtful discussion of the way to balance information privacy rights with the special status of political communication under the Australian constitution. It finally recommended that: "In the interests of promoting public confidence in the political process, those who exercise or seek power in government should adhere to the principles and practices that are required of the wider community. Unless there is a sound policy reason to the contrary, political parties and agencies and organisations engaging in political acts and practices should be required to handle personal information in accordance with the requirements of the *Privacy Act*." Before amending the law, however, the ALRC recommended "the Office of the Privacy Commissioner should develop and publish guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the Act." To date, no such guidance has been issued. It is generally assumed that the major political parties have

[115] Australia Privacy Act, 1988, (Cth) ss 7C.

[116] There seems to be no guidance from the Office of the Australian Information Commissioner on the scope of these exemptions: https://www.oaic.gov.au/privacy/your-privacy-rights/political-parties-and-elections/

[117] Ibid.

[118] There was a case in 2017 where the Electoral Commission successfully brought a prosecution against a the general secretary of the New South Wales Labour Branch for unlawfully using electoral roll information to find name, address and phone number information which he passed along to the union boss. https://www.smh.com.au/national/nsw/former-alp-heavyweight-jamie-clements-guilty-of-unlawfully-using-electoral-data-20170512-gw37jh.html

[119] Australian Electoral Commission. *Privacy and the Election – Frequently Asked Questions.* https://www.aec.gov.au/FAQs/privacy-election.htm

no interest in removing the exemptions for political parties from Australian privacy protection law.[120]

A final dimension of the Australian context is worthy of mention. Voting is mandatory in Australia. All eligible voters over the age of 18 have to register and show up to the polls (even if they just register a "none-of-the-above" vote) in all Commonwealth, state and territory elections, by-elections and referenda. Those who do not vote will receive a "failure to vote" letter from the Australian Election Commission, and if the voter can not provide a "valid and sufficient reason" they are required to pay a A$20 penalty.[121] Compulsory voting is controversial, but it has one obvious implication for this analysis. It renders attempts at voter suppression largely pointless, and by extension the need for data on the individuals whose votes the party might want to suppress. There will be other incentives, of course, to gather data on Australian voters, but encouraging or discouraging them to show up, is not one of them. Australians are required to do so by law.

Regulated personal data capture and consent-based personalised communication in Europe (Case studies: UK and France)

There are a series of relevant regulations and initiatives at the European level. The Commission has taken an active interest in tackling disinformation and misinformation in the light of the Cambridge Analytica/Facebook scandal. In a series of publications in 2018, it has recognised the significance of massive online disinformation and the unlawful processing of personal data for purposes of micro-targeting and has issued relevant guidance.[122] Most notably, a self-regulatory the Code of Practice on Online Disinformation, with regular reporting requirements has been endorsed by online platforms, leading social networks and advertisers.[123] A European approach is perhaps emerging, comprising requirements for ad transparency, international cooperation, and of course the strong assertion of data protection rights to the electoral context.

---

[120] Vaile, D. (March 22, 2018). Australia should strengthen its privacy laws and remove exemptions for politicians. *The Conversation.* http://theconversation.com/australia-should-strengthen-its-privacy-laws-and-remove-exemptions-for-politicians-93717

[121] Australian Election Commission. *Frequently Asked Questions*. https://www.aec.gov.au/FAQs/Voting_Australia.htm

[122] European Commission. (2018). *Tackling online disinformation: a European Approach*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236; European Commission (2018) *Free and fair European elections – Factsheet.* https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_en.pdf; European Commission. (2018). *Action Plan against Disinformation. European Commission contribution to the European Council.* https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf; European Commission. (2018). *Commission guidance on the application of Union data protection law in the electoral context.* https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf; European Commission. (2018). *Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament.* https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf

[123] *EU Code of Practice on Disinformation*. (September 2018). https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

Political parties are regulated under both the 1995 European Data Protection Directive (95/46/EC)[124] and the General Data Protection Regulation (GDPR).[125] The same is true in other countries (such as New Zealand and Hong Kong) with uniform data protection regimes, and which have been influenced by the European model.

Under Article 9 (1) of the GDPR, the "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation shall be prohibited." These categories mirror those mentioned in the revised Council of Europe Convention 108.[126] They are also derived from the principles of non-discrimination on grounds of political opinion enshrined in Article 21 of the Charter of Fundamental Rights of the European Union. According to earlier guidance provided by the Article 29 Working Party, the assumption behind the classification of special categories of personal data is that misuse of these data could have more severe and irreversible consequences for the individual's fundamental rights.[127]

The GDPR lists a number of exemptions, two of which are directly relevant to the political context. Article 9.2 (d) permits processing when "carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects." Article 9.2. (e) permits processing which "relates to personal data which are manifestly made public by the data subject." And Article 9.2 (g) permits processing when necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

Recital 56 of the GDPR attempts to clarify this exemption in the case of political parties:

---

[124] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJEU 1995 L 281)

[125] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on General Data Protection Regulation (OJEU L119 1). http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[126] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (January 1981). *Council of Europe*. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[127] *See* European Union Article 29 Data Protection Working Party. (2011). *Advice Paper on special categories of data ("sensitive data").* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf

> Whereas where, in the course of electoral activities, the operation of the democratic system requires in a Member State requires that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

The Commission guidance on the application of Union data protection law in the electoral context stresses that it "applies to all actors active in the electoral context", including European and national political parties, European and national political foundations, platforms, data analytics companies and public authorities responsible for the electoral process.

In the light of the continuing scandal, and in advance of the European parliamentary elections, the European Data Protection Board (EDPB) issued a statement on the "use of personal data in the course of political campaigns."[128]

1. Personal data revealing political opinions is a special category of data under the GDPR. As a general principle, the processing of such data is prohibited and is subject to a number of narrowly-interpreted conditions, such as the explicit, specific, fully informed, and freely given consent of the individuals.
2. Personal data which have been made public, or otherwise been shared by individual voters, even if they are not data revealing political opinions, are still subject to, and protected by EU data protection law. As an example, using personal data collected through social media cannot be undertaken without complying with the obligations concerning transparency, purpose specification and lawfulness.
3. Even where the processing is lawful, organisations need to observe their other duties pursuant to the GDPR, including the duty to be transparent and provide sufficient information to the individuals who are being analysed and whose personal data are being processed, whether data has been obtained directly or indirectly. Political parties and candidates must stand ready to demonstrate how they have complied with data protection principles, especially the principles of lawfulness, fairness and transparency.
4. Solely automated decision-making, including profiling, where the decision legally or similarly significantly affects the individual subject to the decision, is restricted. Profiling connected to targeted campaign messaging may in certain

[128] European Data Protection Board (EDPB). (March 13, 2019). *Statement 2/19 pm the use of personal data in the course of political campaigns.* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

circumstances cause 'similarly significant effects' and shall in principle only be lawful with the valid explicit consent of the data subject.

5. In case of targeting, adequate information should be provided to voters explaining why they are receiving a particular message, who is responsible for it and how they can exercise their rights as data subjects. In addition, the Board notes that, under the law of some Member States, there is a transparency requirement as to payments for political advertisement.

Despite this guidance, we should not conclude that the law is clear. In prior work, I have raised a number of questions concerning: the breadth of the definition of "political opinions" and whether or not the extent of the sensitive categorisation might extend to the activities from which those opinions might be inferred (e.g. magazine and newspaper readership, group memberships); the definition of "regular contacts"; the meaning of "in the course of electoral activities," when social media facilitates permanent campaigning during and between elections; and the definition of the "reasons of public interest."[129]

The two countries in which these broader issues have been most directly engaged are the UK and France. From rulings by the ICO and the Commission Nationale de l'Informatique et Libertés (CNIL), we are beginning to obtain a clearer picture of the conditions under which data on political opinions might legally be processed in specific contexts, and therefore the extent to which voter analytics might be regulated.[130]

United Kingdom

The UK is the only European country whose parties admit operating voter relation management databases of the kind seen in North America. Using similar proprietary software, UK parties augment the basic address information from the electoral roll with additional personal data on supporters and non-supporters alike from a variety of sources.[131] In 2000, the UK government amended its regulations on the processing of sensitive personal data to permit the processing of personal data on political opinions by registered political parties, provided it "did not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person."[132]

---

[129] Bennett, C.J. (April 2018). Cambridge Analytica and Facebook: A Wake-Up Call. *Privacy Laws and Business International Report,* Issue 152.

[130] Information Commissioner's Office. (2014). *Guidance for political parties for campaigning or promotional purposes.* https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf;
Commission Nationale de l'Informatique et Libertés (CNIL). (January 2012). *Communication Politique: Obligations Legale et Bonnes Pratiques.*
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Politique.pdf

[131] Bennett, C.J. (November 2016). Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?. *International Data Privacy Law*, Volume 6, Issue 4, 261-275.

[132] *The Data Protection (Processing of Sensitive Personal Data) Order 2000.*

Pursuant to Article 6(1) of the GDPR, the UK's 2018 Data Protection Act explicitly references "an activity that supports or promotes democratic engagement" as a legitimate "public interest." The Act goes on to specify the conditions that allow the processing of sensitive forms of data including if the "processing of personal data revealing political opinions, is carried about by registered political party", and is "necessary for the purposes of the person's or organisation's political activities." Political activities include "campaigning, fund-raising, political surveys and case-work."[133]

The first guidance from the Information Commissioner's Office (ICO) dates from 2005 and was issued partially in response to the case against the Scottish National Party for using automated robo-calling for political marketing purposes. There was a similar complaint and ruling against the Labour Party in 2010. The guidance was updated in 2014.[134] It addresses the practical meaning of consent in the electioneering context, by means of post, email, text, fax, phone and automated messages; and the often-tricky relationship between national party headquarters, local campaigns and the third party market research firms that work for parties. The guidance also addresses the rules for "viral-marketing" or "tell a friend" campaigns. The party must always identify itself, and provide contact details and easy procedures for opting out.

This earlier guidance formed important preparation for the series of investigations and reports prompted by the Cambridge Analytica breach. Two Investigation reports detail the enforcement actions associated with the investigations, including:[135] a fine of half a million pounds to Facebook; enforcement actions against SCL Elections Ltd., the parent company of Cambridge Analytica, and against Aggregate IQ, the Victoria-based company that worked for the Vote Leave campaign in the EU referendum; and audits of the main credit reference companies. They also issued a fine against Emma's Diary, a company that provides advice to women and new parents, that allegedly sold information to the data broker, Experian, which was then used by the Labour Party. At the conclusion of their inquiries, the Commissioner was compelled to note "a disturbing disregard for voters' personal privacy by players across the political campaigning ecosystem — from data companies and data brokers to social media platforms, campaign groups and political parties."[136]

(February 17, 2000). http://www.legislation.gov.uk/uksi/2000/417/pdfs/uksi_20000417_en.pdf

[133] *Data Protection Act 2018.* (2018). http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

[134] UK Information Commissioner's Office. (2014). *Guidance for Political Parties for Campaigning for Promotional purposes*. https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf

[135] ICO. (November 2018). *Investigation into the use of data analytics in political campaigns. A Report to Parliament.* https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf; ICO. (July 2018). *Investigation into Data Analytics in Political Campaigns: Investigation Update.* https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.

[136] Information Commissioner's report brings the ICO's investigation into the use of data analytics in political campaigns up to date: https://ico.org.uk/about-the-ico/news-and-events/blog-information-commissioner-s-report-brings-the-ico-s-investigation-into-the-use-of-data-analytics-in-political-campaigns-up-to-date/

The ICO used this opportunity to conduct a broader analysis of the role of voter analytics in contemporary British elections. In *Democracy Disrupted? Personal Information and Political Influence*[137] for the first time, a DPA tried to draw the curtain back on the very complicated world of voter analytics, to paint a picture of the range of organisations involved in contemporary elections, and of the practices they engage in. This report was accompanied by a research report from Demos reviewing the current and future trends in campaigning technologies.[138]

Democracy Disrupted provides a detailed and empirically based description of the various sources of personal data that are used to profile the electorate, and of how micro-targeting works across a variety of media. Around 40 organisations were the focus of the inquiry; many other individuals assisted. The report raises a range of questions about the application of the GDPR to political parties and election campaigns going forward. The ICO reminds political parties that although they have a "special status in the democratic process… allowing them to process political opinion data when carrying out legitimate political activities…. they have responsibilities as data controllers to comply with all the requirements of the law, including the data protection principles."[139]

Most of the findings in the report concern the lack of transparency about "fair processing." The report criticises the parties' privacy policies for shortcomings in accessibility and clarity, in light of the enhanced privacy notices requirements under the GDPR. For any business that supplies data to political parties, and several are mentioned in the report, that business "cannot repurpose that personal data for political campaigning without first explaining this to the individual and obtaining their consent."[140] Vague and expansive statements of purpose are not likely to be good enough. Equally, political parties need to ensure when sourcing personal information from third-party organisations (including data brokers) that appropriate consent has been obtained. This performance of 'due diligence' must be recorded and auditable. Some political parties also use software which assigns a predicted ethnicity and age to individuals, under the contention that this "assumed" or "inferred" data is not necessarily personal information about the data subject. The ICO disagrees.[141] Once this is linked to an individual it does amount to personal data and is subject to the requirements on the processing of special categories of data under the GDPR. There is

[137] Information Commissioner's Office (ICO). (July 2018). *Democracy Disrupted: Personal Information and Political Influence.* https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

[138] Bartlett, J., Smith, J., and Acton, R. (July 2018). *The Future of Political Campaigning*. https://www.demos.co.uk/wp-content/uploads/2018/07/The-Future-of-Political-Campaigning.pdf

[139] See page 19 in ICO (July 2018)

[140] See page 15 in Ibid.

[141] See pages 51 and 52 in Ibid.

a significant risk that assumptions or predictions about ethnicity (based for example on the heritage of the name) could be inaccurate and carry significant risks for the individual.[142]

The investigation also identified a lack of understanding among political parties about the legal basis for uploading contact information to social media platforms, such as through Facebook's Core, Custom and Look-Alike Audiences functions.[143] As in France, the popular company, Nationbuilder, and its Nationbuilder match function, also comes under scrutiny. The ICO is concerned that political parties are using this platform without adequate information being provided to the people affected.[144] Even where a party got the personal information from publicly available sources such as the Electoral Register, they must still provide a clear privacy notice to individuals. The report also discusses the legality of micro-targeting under the GDPR's provisions on automated decision-making and profiling.[145] Political micro-targeting may be a type of automated decision-making that does have sufficiently significant effects on individuals, triggering the requirements under Article 22.

The ICO made a series of ten recommendations, issued eleven political parties with warning letters detailing areas of concern and non-compliance. These letters were in advance of Assessment Notices providing for compulsory audits of a selection of the parties. The ICO has also asked the government to legislate a statutory code of practice on the use of personal data in political campaigns.[146] Until then, the Commissioner called for an 'ethical pause' to allow the key players to reflect on their responsibilities.[147] That draft framework code of practice was circulated in August 2019, and is currently subject to consultation.[148]

France

There is plenty of evidence that digital campaigning techniques have begun to enter French politics, as well. Various start-ups now offer a suite of services to parties and candidates, for the analysis of constituencies, allowing parties and candidates to prioritise their canvassing activities.[149] But there is no evidence of the kinds of comprehensive Voter Relationship Management systems observable in the U.S. and in

[142] Ibid.
[143] See page 32 in Ibid.
[144] Ibid.
[145] See page 16 in Ibid.
[146] See page 44 in Ibid.
[147] See page 45 in ICO (July 2018)
[148] Information Commissioner's Office (ICO). (August 2019). *Guidance on Political Campaigning: Draft Framework Code for Consultation*. https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf
[149] An example is Cinquante-Plus-Un. See https://www.youtube.com/watch?v=N2KuHpxkN6M

parliamentary systems like Canada and the UK.[150] Any voter analytics company has to be scrupulous about compliance with some strong interpretations of French data protection law as it applies to political campaigning.

The CNIL has probably offered the most regular, and consistent, rulings on digital political marketing practices of all the European DPAs. Its interest in the subject goes back to the so-called 'Sarkospam' scandal of September 2005, when hundreds of thousands of unsolicited emails were sent on behalf of presidential candidate Nicolas Sarkozy.[151] The case prompted a series of recommendations about the use of files by political parties, groups, candidates and elected officials. Political canvassing by e-mail should not use any databases other than those who had explicitly opted in. And the CNIL ruled that those who had opted in to commercial databases who were not explicitly told at the time that their information may be used for political marketing (as occurred in the Sarkospam case), must be contacted again and offered the opportunity to opt out.[152] The guidance also recommended that political parties declare to the CNIL when they are processing data on people who are occasionally in contact (for instance, those who have signed a petition, requested documentation, or visited the blog), but not those who are regularly in contact, such as donors or regular members.

The CNIL issued further guidance in 2012[153] and placed the rules about political communication in the context of the broader application of French data protection law to the entire processing activities of parties in France, and the information they collect. The guidance addressed: the types of internal files of the elected official, the candidate or the political party, and distinguishes how each might use files of members, regular contacts and occasional contacts; the use of the electoral register, of directories and files from the private sector; and the rules for communication by telephone, SMS, email and Internet. The CNIL also provided examples of best practice for obtaining informed consent.

Particular data protection issues were also raised as a result of the institution of U.S. style open primary elections for the Socialist Party in the 2012 presidential election. In this election, not only would registered Socialist voters be able to participate, so would

---

[150] Bennett, C.J. (December 2016). Voter databases, micro-targeting and data protection law: can political parties campaign in Europe as they do in North America?. *International Data Privacy Law*, *Vol. 6*, No. 4, 261-75.

[151] Lebegue, T. (September 27, 2005). Françaises, Français, Nicolas Sarkozy vous spamme. *Libération.* http://www.liberation.fr/france/2005/09/27/francaises-francais-nicolas-sarkozy-vous-spamme_533767

[152] Commission nationale de l'informatique et des libertés. (November 2006). *Délibération n. 2006-228 du 5 octobre 2006 portant recommandation relative à la mise en oeuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques.* https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000459927

[153] CNIL. (January 2012). *Communication Politique: Obligations Legale et Bonnes Pratiques.* https://www.cnil.fr/sites/default/files/typo/document/CNIL_Politique.pdf

all voters who donated one euro to the party and agreed to sign a commitment attesting to the values of the left (freedom, equality, fraternity, secularism, justice, solidarity and progress). The party organised one national vote in two stages on 9 and 16 October 2011 and elected Francois Hollande. Some 2.6 million voters participated in the first round, and three million in the second. The CNIL struggled with the question of whether the party might continue to process data on those who had voted in the primaries, as if they were members or "regular contacts." They concluded eventually that they could not, because the purpose of collection was different,[154] unless the voter separately consented to be contacted.

The community organising system, Nationbuilder, has been popular across the world for candidates and parties across the ideological spectrum, including in France. The company offers a fully integrated suite of tools for the organisation of a campaign, and outreach through email, telephone, social media and traditional door-to-door campaigning. The CNIL was particularly interested in a functionality called "NationBuilder Match." When a supporter is added to a user's "nation" and provides his/her email address, the software will immediately add any public LinkedIn, Facebook and Twitter profiles associated with that email address, including any profile pictures.[155] It was also reported that in some cases Nationbuilder Match was uploading locational information, and information on all the users who "liked" the candidates' publications on Facebook, or followed a candidate on Twitter.[156]

For the CNIL, "those who voluntarily provided their email address for the purpose of receiving a newsletter from a candidate cannot be considered as having been informed or having consented to enter into relations with that candidate through a social network"[157] Moreover, with regard to the tracking of users across multiple platforms, the CNIL stated that "being a regular contact via the Facebook network is not a sufficient condition to collect and use the contact information as shown on a Twitter profile"[158] NationBuilder deactivated this functionality in France, and subsequently across all EU member states.[159]

---

[154] Délibération no. 2012-020 du Janvier 2012 portant recommandation relative à la mise en oeuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques, available at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025344843

[155] Escobedo, A. NationBuilder match. *Nationbuilder*. https://nationbuilder.com/nationbuilder_social_match

[156] Untersinger, M. (April 3, 2017). Logiciels électoraux : les politiques français ont dû mettre fin à la récolte de certaines données personnelles. *Le Monde.* http://www.lemonde.fr/pixels/article/2017/04/03/logiciels-electoraux-les-politiques-francais-ont-du-mettre-fin-a-la-recolte-de-donnees-personnelles_5105296_4408996.html; See also Filippone, D. (April 4, 2017). NationBuilder met fin à la collecte de données issues des réseaux sociaux. *Le Monde Informatique*. http://www.lemondeinformatique.fr/actualites/lire-nationbuilder-met-fin-a-la-collecte-de-donnees-issues-des-reseaux-sociaux-67842.html.

[157] Commission Nationale de l'Informatique et Libertés. *"Elections 2016 / 2017 : quelles règles doivent respecter les candidats et partis?*" https://www.cnil.fr/fr/elections-2016-2017-quelles-regles-doivent-respecter-les-candidats-et-partis

[158] Ibid.

[159] Telephone conversation with Toni Cowan-Brown, Vice President, Strategic Partnerships at NationBuilder (June 21st, 2019).

This case raises the question of the legal distinction under the GDPR between "regular contacts" and "occasional contacts."[160] The CNIL defines regular contacts as those who "engage with a political party in a positive way in order to maintain regular exchanges in relation to the party's political action." This notion is therefore distinct from that of "member." Regular contacts must be informed about the conditions under which their data will be processed through the mandatory privacy notices on the candidates' or parties' profiles on social networks. The policies should state (a) the nature of the data collected, (b) the purpose of the treatment of the data, and (c) the procedures to oppose such processing. If such requirements are met, then the CNIL says that it is possible for the candidates or parties to use all the features offered by the different social networks to communicate with their regular contacts—for instance, they can publish content that will be brought to their attention, send private messages to them via these networks, and so on. However, "persons must be able to oppose this communication at all times."

When it comes to occasional contacts, for example those who have "liked", commented or retweeted content, the systematic collection of their additional data (email address, Facebook or Twitter accounts, etc.) is unfair ("*n'est pas loyale*"). However, the CNIL specifies the conditions under which parties or candidates can process the "additional" data collected from occasional contacts. Indeed, it is possible to send a message to occasional contacts "via the usual method" ("*par le biais du vecteur habituel*") (that is to say, via email if the person has one, via Facebook if the person "liked" a post, via private message if the person "retweeted", etc.) in order to obtain the person's consent to the collection of additional data that concerns him or her. But the CNIL is clear that in the total absence of contact between a candidate or party and an internet user, it is unfair ("*déloyal*") to capture data on those individuals. The enrichment of contact databases must not therefore lead to the collection and processing of personal data relating to third-party internet users. Further, it is illegal to use someone's "friends list" for the purpose of communication, whether the person in question is a regular or an occasional contact.

The combined effects of these rulings constrain the abilities of parties and candidates to harvest data from social media networks. They begin to establish some clearer rules about the processing of these forms of sensitive data, at least in France. However, the pressures in France (as elsewhere) to harness the power of digital technologies are enormous. And these same restrictions have not yet been articulated at the European level as a general interpretation of the GDPR.

[160] Commission Nationale de l'Informatique et Libertés. (November 8, 2016). *Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?*. https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.

Prohibited personal data capture and personalised political communication (Case study: Japan)

The Japanese constitution (Article 15) states that: "The people have the inalienable right to choose their public officials and to dismiss them. All public officials are servants of the whole community and not of any group thereof. Universal adult suffrage is guaranteed with regard to the election of public officials. In all elections, secrecy of the ballot shall not be violated. A voter shall not be answerable, publicly or privately, for the choice he has made."[161] These provisions, as well as long-standing Japanese traditions, produce an election campaigning culture unlike anywhere else.

Japan's Public Offices Election Law (POEL) comprises 275 clauses that regulate campaigning during the period from announcing one's candidacy to election day, and daily political activities. Door-to-door campaigning and telephone solicitation are banned. And politicians are not allowed to buy time on radio or TV, or space in newspapers for advertising. Candidates are bound by rules regarding the number of speeches they can make, the type of canvassing they can do, which written materials can be distributed and displayed, and the number of fliers that might be distributed during a campaign (70,000). Japanese law also prohibits "pre-campaign" campaigning. The solicitation of votes should only occur during the official period of the campaign — not before, and not on election day.

Given these limitations, candidates have to resort to campaigning in public, giving speeches wherever crowds might congregate — train stations, shopping malls, farmers' fields. And by law, their speeches have to be concluded within 45 minutes.[162] Japanese campaigns are therefore very noisy affairs, as competing soundtracks, festooned with posters and slogans, bellow campaign messages around the streets of Japanese cities. There is a tradition that the candidate distinguishes herself, or himself, by wearing white gloves, supposedly to distinguish the candidate from others and to symbolise a clean and untarnished image.[163]

Many of these stipulations date from election reforms instituted in 1925, the time when universal suffrage was extended to all males over 25 years. These rules were intended to operate as a deterrence against bribery, pork-barrel politics and corruption. They also are designed to produce a level-playing field, equalizing the opportunities between candidates of large and small political parties. They have become integrated within Japanese political culture, even though they are widely

[161] The Constitution of Japan. https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html

[162] Sim, W. (October 2017). Election Campaigns, the Japanese Way. *The Straits Times*. https://www.straitstimes.com/asia/east-asia/election-fever-hits-japan

[163] Mealey, R. (October 2017). Japan Elections a little bit old-fashioned with strict laws and billboard bans. *ABC News*. https://www.abc.net.au/news/2017-10-14/election-campaigns-in-japan-an-old-fashioned-affair/9040624

criticised for their complexity and precision.[164] They also operate within a context of near one-party rule — the Liberal Democratic Party has governed Japan for all but three years since 1955.

For a society so immersed in digital culture and social media, these rules were bound to come under some pressure. The government therefore made changes to the POEL in 2013 which allowed for some forms of internet campaigning. Under these rules, candidates and parties were legally allowed to run websites, but they cannot contain a "vote for me" message, and they cannot refer to an opponent. They can be used to sign up members of the party and to solicit donations, but this is not common in a society that relies so heavily on personalised and localised networks. Nor can the website be updated after the campaign has begun. The assumption is that the information provided to the electorate at the beginning of the campaign serves as a kind of "contract" with the electorate. The statement of intentions is supposed to remain stable, and not altered by the kinds of last-minute promises that are a common feature in North America. In the Japanese context, therefore, "micro-targeting" (as defined above) would essentially be illegal.[165]

The most popular social media platform in Japan is LINE, an app that functions primarily as a communications tool, similar to WhatsApp.[166] Twitter, Instagram and Facebook are essentially viewed under Japanese law as "websites." In a similar stretch of legal terminology, Youtube is regulated as a "broadcaster" and may not be used for personalised political communication. That said, the use of social media platforms as broadcast media for political candidates are becoming increasingly popular. It was reported, for example, that Instagram had become the platform of choice for Prime Minister Abe in the 2019 elections for the upper house, signalling an attempt to reach younger voters.[167] But there is little evidence of the sophisticated digital campaign strategies seen elsewhere. There is also no evidence that they are used for more personalised messaging, and no evidence that they are used to harvest information on followers and friends.

The conditions under which Japanese parties and candidates campaign, therefore, is almost entirely regulated under the POEL and the associated regulations, and overseen by the Elections Division of the Ministry of Internal Affairs and Communications. "Political bodies" (*seiji dantai*) therefore, are exempted from the

[164] Nikkei Asian Review. (January 2017). *Japan's Election System Choking on Rules.* https://asia.nikkei.com/Politics/Japan-s-election-system-choking-on-rules

[165] Interview with officials from Elections Division of Japanese Ministry of Communications (May 8, 2018).

[166] Wasabi Communications. *An Overview of Social Media in Japan.* https://www.wasabi-communications.com/en/blog/an-overview-of-social-media-in-japan/

[167] Oda, S. (July 2019). Targeting Young Voters, Japan's Abne Takes to Instagram. *Bloomberg News.* https://www.bloomberg.com/news/articles/2019-07-17/targeting-young-voters-japan-s-abe-takes-to-instagram

2017 Act on the Protection of Personal Information.[168] This category embraces registered political parties (*seito*) which have at least 5 members of the Diet and receive the public subsidy, as well as smaller, and generally more radical, political groupings that may also be active at national, prefectural and municipal levels. Furthermore, the Act states that the Personal Information Protection Commission "shall not hinder the freedom of expression, freedom of academia, freedom of religion, and freedom of political activity" in the course of its activities.[169]

A further interesting dimension of Japanese law concerns the definition of sensitive categories of data.[170] "Political opinions" (as specified in the GDPR) are not explicitly defined as such. Instead, the law uses the broader, and more amorphous, concept of "creed" (*shinjo*) which embraces political ideology and other belief systems, including religion. These data "require special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal."[171] These rules essentially prohibit the capture of such data without express consent. However, given the strict rules about personalised political communication, the capture of such data for purposes of political campaigning would be pointless. Traditional public opinion polling is conducted, and public relations companies give plenty of advice about image and message construction. But there is no evidence of the entrance of voter analytics companies into Japanese politics, and no evidence that they are likely to emerge. Japanese law, and more importantly its political traditions, would stand as strict barriers.[172]

Emerging personalised Information Capture from Mass Messaging Applications in the Global South (Case Studies: Kenya and Brazil)

In many countries of the Global South, digital technology is playing an increasing role in election campaigns.[173] The growth in access to mobile phones and the Internet as well as the pervasive use of associated platforms like WhatsApp and Facebook have meant that the average voter in the Global South can now somehow be reached 'online'.[174] Aware of this trend, many political parties in these countries have been designing and deploying campaign publicity systems to take advantage of these new

[168] See Article 76 (1)(v) in: Amended Act on the Protection of Personal Information. (December 2016). Find English translation here: https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf
[169] Ibid., Article 43 (1)
[170] Interviews, Japan Personal Information Commission, May 7, 2018.
[171] Ibid, Article 2 (3)
[172] Interviews, Elections Division of Japanese Ministry of Communications (May 8, 2018).
[173] Chan, S. (2017). Africa leads the way in election technology, but there's a long way to go. *The Conversation.* https://theconversation.com/africa-leads-the-way-in-election-technology-but-theres-a-long-way-to-go-84925
[174] Murgia, M., Findlay, S., & Schipani, A. (2019). India: the WhatsApp election. *FT*. https://www.ft.com/content/9fe88fba-6c0d-11e9-a9a5-351eeaef6d84

campaigning opportunities.[175] One common approach that is increasingly being fine-tuned is mass-messaging through applications like WhatsApp.[176]

While micro-targeting techniques may still be less prevalent or effective in Global South countries, it is critical to pay attention to how the mass-messaging techniques and the associated industry, are quickly laying foundations for more effective micro-targeting in many Global South countries. These foundations include building and testing channels to access personal data[177], normalising voter targeting, and fostering dubious partnerships[178] between political actors and the companies within the political "influence industry." Tactical Tech's research projects on 'Personal Data and Political Persuasion' provide many substantive insights on the growing use of voter profiling and targeting techniques in Global South countries such as Malaysia, Argentina, India, Chile, Kenya and Colombia. These case studies show both the abuse and circumvention of laws, as well as the exploitation of legal gaps.

In Malaysia, for instance, it is reported that political parties resort to "location and language-based micro-targeted Facebook advertisements" to influence voters.[179] In Chile political parties are using tools to help them "discover the geolocation of voters" as well as "their socioeconomic status and political preferences".[180] Chilean parties are working with companies like InstaGIS that access user comments, likes and locations on social media for profiling and segmentation purposes. Additionally, while Chile's national laws prohibit the use of the national electoral roll for commercial purposes, it has been found that commercial data-driven campaigns are gaining roots.[181] In India, political parties have used cookies to harvest data for targeting voters with ads.[182] In addition to major investments in social media analytics, political parties in India have

[175] VOA. (February 2016). Executive: Indian Political Parties Abuse WhatsApp Service ahead of Election. *VOA News.* https://www.voanews.com/south-central-asia/executive-indian-political-parties-abuse-whatsapp-service-ahead-election; Mohammed, O. (2015). WhatsApp is now the primary platform for political trash talk in Tanzania's election campaign. *Quartz Africa*. https://qz.com/africa/510899/whatsapp-is-now-the-primary-platform-for-political-trash-talk-in-tanzanias-election-campaign/

[176] Tactical Tech. (November 2018). *WhatsApp: The Widespread Use of WhatsApp in Political Campaigning in the Global South*. https://ourdataourselves.tacticaltech.org/posts/whatsapp/.

[177] Freeze, C. and MacKinnon, M. (March 2018). Records reveal AggregateIQ and SCL Group's plan to influence politics in Trinidad and Tobago. *The Globe and Mail.* https://www.theglobeandmail.com/canada/article-consulting-firms-in-data-scandal-first-partnered-on-project-in/

[178] Myjoyonline. (October 2018). Part of $175m loan to build hospitals spent on NDC re-election research. *Ghanaweb.* https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Part-of-175m-loan-to-build-hospitals-spent-on-NDC-re-election-research-692606; Oduro-Marfo, S. (April 2018). Cambridge Analytica, Africa and talk of Colonialism. *Ipolitics.* https://ipolitics.ca/article/cambridge-analytica-africa-and-talk-of-colonialism/

[179] Tactical Tech. (June 2018). *Malaysia: Voter Data in the 2018 Elections*. https://ourdataourselves.tacticaltech.org/posts/overview-malaysia

[180] Tactical Tech (September 2018). *Chile: Voter Rolls and Geo-targeting.* https://ourdataourselves.tacticaltech.org/posts/overview-chile

[181] Ibid.

[182] Tactical Tech. (August 2018). *India: Digital Platforms, Technologies and Data in the 2014 and 2019 Elections.* https://ourdataourselves.tacticaltech.org/posts/overview-india

utilised other tools such as voice assistants — popularly called 'political siri'— in targeting voters with campaign messages.[183]

Notwithstanding the growing incidence of such political targeting in Global South countries, it was Cambridge Analytica's involvement in elections in countries like Ghana, Nigeria, Kenya, India and Trinidad and Tobago that raised awareness on how political advertising could undermine democracies — especially young or budding ones. In Nigeria, Cambridge Analytica and its partner, Aggregate IQ are said to have utilised hacked information on the leading opposition candidate and (ethnic and religion-based) disinformation and voter suppression techniques.[184] In Ghana, Cambridge Analytica's parent company, SCL flouted the country's constitution by using state funds to gather data on public sentiments for the incumbent political party.[185] In this case, the Ghanaian legislature was presented with a budget for funding a national survey on healthcare facilities while the actual project also gathered opinions to inform the campaign of the political party in government. In Trinidad and Tobago, SCL and AIQ were reportedly looking into buying raw data on internet use, including billing details, from internet service providers.[186] In many of these cases, we find political parties doing whatever they can to win votes including breaking laws, undermining fragile democratic institutions and whipping up polarising ethnic and religious sentiments. Thus it is important to note the place of local agency in the proliferation of voter targeting technologies and practices in Global South countries.[187]

Ultimately, while Cambridge Analytica's voter targeting scandal may have dominated international headlines, it is important to pay similar attention to the more widespread phenomenon of voter mass-messaging in many Global South countries. In the cases below, we show the increasing capacities of political parties in the Global South to harvest as much personal data as possible to deliver bulk campaign messages to targeted populations, with a common profile, and derived from distinct sources, such as lists of university students or professionals.

While personal data is being dubiously accessed in many countries in Global South countries, data privacy regimes have not yet been firmly institutionalised. Some of the resulting challenges are discussed below in two cases: Kenya, which has yet to

---

[183] Ibid.

[184] Cadwalladr, C. (March 2018). Cambridge Analytica's ruthless bid to sway the vote in Nigeria. *The Guardian.* https://www.theguardian.com/uk-news/2018/mar/21/cambridge-analyticas-ruthless-bid-to-sway-the-vote-in-nigeria

[185] Myjoyonline. (October 2018). *Part of $175m loan to build hospitals spent on NDC re-election research*. https://www.myjoyonline.com/politics/2018/October-15th/part-of-175m-loan-to-build-hospitals-spent-on-research-into-mahamas-2016-chances.php

[186] Loop. (March 2018). *T&T's link to Cambridge Analytica scandal*. http://www.looptt.com/content/tts-link-cambridge-analytica-scandal

[187] Oduro-Marfo, S. (April 2018). Cambridge Analytica, Africa and talk of Colonialism. *Ipolitics.* https://ipolitics.ca/article/cambridge-analytica-africa-and-talk-of-colonialism/

develop a data protection law; and Brazil, whose data protection law has just been promulgated. While these cases do not represent all the prevailing conditions in Global South countries, they do provide effective illustrations of environments with lax data protection regimes, and which have attempted to address the concerns through the regulation of political advertising. These two countries illustrate the growing use of mass messaging techniques for political marketing in Global South countries and how the phenomenon could set foundations for effective micro-targeting practices.

Kenya

Section 38b of the Kenyan constitution provides that citizens are free to "recruit members for a political party" or "to campaign for a political party or cause". This right is elaborated in the country's Electoral Code of Conduct in which citizens are warned to "do nothing to impede the right of any party, through its candidates, canvassers, and representatives, to have reasonable access to voters…"[188] To this end, the Access to Information law in Kenya permits the acquisition of a redacted version of the voters' register by citizens including political actors.[189] Also, as evidenced by the prevalence of door-to-door campaigns, the political canvassing rules in Kenya do not prevent personal contact between a political candidate and the voter.

However, the right to freely engage in political canvassing does not come without limitations. Kenya's Electoral Code of Conduct proscribes the distribution of offensive campaign messages. While the Electoral Code of Conduct forbids "campaigning in places of worship or during burial ceremonies", it is conspicuously silent about access to persons and private residences. Following from this, the Electoral Code of Conduct does not emphasise issues such as data privacy nor personalised messaging.

Kenya's legislative landscape already has some laws that could serve as foundations for constructing a regulatory framework to better guide the access to, and use of, citizen data for political campaigning. In addition to the Guidelines on bulk messaging (described below), privacy rights are supported in Article 31 of the Constitution. Also in Kenya's Information and Communication Act, articles 31, 83 and 93b limit the interception and disclosure of data without consent. Kenya's Consumer Protection Regulations similarly regulates data monitoring and disclosure.

---

[188] Electoral Code of Conduct. *Kenya's Elections Act.* (2015). https://www.iebc.or.ke/uploads/resources/stsPzf9498.pdf

[189] "... one could present an Access to Information request for the voter register via a letter to the CEO giving justification for the register. This acknowledges that the voter register is a public document… the version of the register … in this instance would be redacted to the name, electoral area, and truncated ID number showing the first two and last two digits." See page 15 in Muthuri, R., Karanja, M., Monyango, F. and Karanja, W. (2018).
Investigating Privacy Implications Of Biometric Voter Registration In Kenya's 2017 Election Process.
https://privacyinternational.org/sites/default/files/2018-06/Biometric%20Technology-Elections-Privacy.pdf

Although Kenya has no dedicated data protection law, there is a data protection bill that has been under consideration from 2018. The bill mirrors the provisions in the GDPR.[190] Article 2 of the bill defines personal political opinion as sensitive data and as such, regulates its access, processing and use.[191] While the passing of the bill could go some way to promote data privacy and democracy in Kenya, there are other legislations that could neutralise the positives of the potential data protection law. An example is the Registration of Persons Act which "would allow the government to collect people's personal information – including DNA samples, biometric data like fingerprints and retinal scans and GPS information" in the name of national security.[192]

In the absence of general legislation, the Guidelines for Prevention of Dissemination of Undesirable Bulk Political SMS and Social Media Content via Electronic Communications Networks (hereafter referred to as the Guidelines) assume a huge significance. They were passed in July 2017 to help regulate the content and transmission of political messages.[193] As reflected in its title, the Guidelines mainly focus on undesirable bulk messages, and attempt to deter political messages that "contain offensive, abusive, insulting, misleading, confusing, obscene or profane language" or "contain inciting, threatening or discriminatory language that may or is intended to expose an individual or group of individuals to violence, hatred, hostility, discrimination or ridicule on the basis of ethnicity, tribe, race, color, religion, gender, disability or otherwise."

The Guidelines also require that "political Messages will only be delivered through licensed Content Service Providers (CSPs) who have direct interoperability agreements with a Mobile Network Operator (MNO) or Mobile Virtual Network Operator (MVNO)". Procedurally, the Guidelines provide that political messages be first sent to CSPs, who then send it to the MNO or MVNO for vetting. Publication is based on the approval of the latter. Thus, two external accountability agents sit between a political actor and the voter when it comes to bulk political messaging in Kenya. The Guidelines also call for messages to be sent only to users who have consented via opt-in subscription and that, it should be possible for subscribers to opt-out whenever they wish. Importantly also, the Guidelines warn against the "unauthorised use, sharing or sale of existing customer databases for purposes of sending out Political Messages, Poll Tracking and lobby activities."

---

[190] Muendo, M. (February 2018). Kenya plans to place public security above data privacy. That's a bad idea. *The Conversation*. https://theconversation.com/kenya-plans-to-place-public-security-above-data-privacy-thats-a-bad-idea-111099

[191] Kenya Data Protection Bill, 2018. http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf

[192] Muendo, M. (February 2018).

[193] *Guidelines for Prevention of Dissemination of Undesirable Bulk Political SMS and Social Media Content via Electronic Communications Networks.* (2017). https://ca.go.ke/wp-content/uploads/2018/02/Guidelines-on-Prevention-of-Dissemination-of-Undesirable-Bulk-and-Premium-Rate-Political-Messages-and-Political-Social-Media-Content-Via-Electronic-Networks-1.pdf

When viewed in tandem, both the Guidelines and the Electoral Code try to ensure that political campaigning does not breach public cohesion or offend sensitivities. This approach is neither problematic nor surprising, given the violence surrounding the elections in 2007. In fact, inciteful political rhetoric "disseminated by mobile phones, especially via text messages" has been viewed as one of the key factors that promoted the electoral violence in 2007.[194]

Despite the utility of a regulatory environment focused on promoting public cohesiveness, the Guidelines and Kenya's Electoral Code of Conduct are clearly challenged by new campaigning practices. Firstly, micro-targeting messages could eventually be so specific that they may not be sent in bulk. Second, messages may be harmful without being 'undesirable' as defined in the Guidelines. A campaign message crafted with a voter's specific profile in mind could be nominally benign but could cumulatively threaten democratic practices.

These gaps were exploited by Cambridge Analytica in Kenya's 2013 and 2017 elections. In the context of less-integrated digital databases, Cambridge Analytica resorted to a survey of 50000 participants to get a sense of "key national and local political issues, levels of trust in key politicians, voting behaviours/intentions, and preferred information channels".[195] According to Cambridge Analytica, they used the accrued information to rebrand their client, write manifestos, create an online presence and also frame political messages.[196] At the core of its work, Cambridge Analytica is believed to have utilised campaign rhetoric highlighting citizens' fears and exploiting ethnic tensions. As one commentator put it, in Kenya, Cambridge Analytica was riling "up dangerous ethnonationalist rhetoric purely for profit".[197]

Beyond Cambridge Analytica, there will still be political interests and corporate collaborators — both local and international - exploiting citizen data for targeting purposes. For example, political parties in Kenya are increasingly investing in digital membership registration systems, gathering personal data with and without the needed consent. As Grace Mutung'u notes, the Jubilee Party has deployed electronic smart-cards to register members and the leading opposition party the Orange Democratic Movement (ODM) uses a mobile app for the same purpose.[198] Jubilee's smart card collects the name, identity card number and the phone number of

[194] Barkan, J.D. (2013). Electoral Violence in Kenya. *Council on Foreign Relations*. https://www.cfr.org/report/electoral-violence-kenya

[195] BBC. (March 2018). *Cambridge Analytica's Kenya election role 'must be investigated'*. https://www.bbc.com/news/world-africa-43471707

[196] Ibid.

[197] Nyabola, N. (March 2018). Politics in the digital age: Cambridge Analytica in Kenya. *Al Jazeera.* https://www.aljazeera.com/indepth/opinion/politics-digital-age-cambridge-analytica-kenya-180322123648852.html

[198] Mutung'u, G. (2018). The Influence Industry Data and Digital Election Campaigning. *Tactical Tech*. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf

registrants. Upon receiving the card, registrants are to send an SMS to 30553 to activate the card. The ODM via its mobile app is then able to collect information such as name, date of birth, phone number, and polling station details.[199] While the said registration platforms stipulate member-consent, it is on record that many Kenyans have been registered as party members without their knowledge.[200]

In the context of the 2017 Kenyan election, Muthuri et. al. found that unsolicited political messages were sent via Content Service Providers.[201] Most recipients had been enrolled by CSPs on an opt-out basis. In a survey of 228 respondents, Muthuri et al. found that 99% of the respondents, while not subscribing to any political content service, had still received political messages. The messages also contained the alphanumeric data of voters as they appeared in the electoral register. While political operatives could purchase a redacted version of the electoral roll from the Independent Electoral and Boundaries Commission, the fact that the alphanumeric data of voters was not redacted could deepen voter tracking and occasion abuses. The researchers also found that the enforcement of the bulk messaging Guidelines was focused more on "preventing hate speech than protecting Kenyans' biometric and voter data".

Indeed, the targeting of voters in Kenya could worsen as the state invests more in the Integrated Population Register System (IPRS). The IPRS is described as the "one stop shop for all the population data" and as "the single source of truth for the population of all Kenya and foreign residents in Kenya."[202] At the centre of IPRS is the Huduma Numba project, a biometric-based citizens card, currently being deployed. The existence of IPRS and the Huduma Numba in the absence of a comprehensive data protection law could facilitate the exploitation of citizens' data for political targeting.

Brazil

Brazil's General Data Protection Law will only come into effect in 2020.[203] It is based on the GDPR framework, and contains similar provisions for the processing of sensitive data on political opinions or "political organisation membership." As in the GDPR, sensitive data may only be processed under limited and specified conditions. There is

---

[199] Ibid.

[200] A victim of this practice complained on social media: "I've never registered as a member of any political party yet I'm a registered member of Jubilee! Just like I was in TNA in 2012. Outrageous".This person's gender, date of birth and identity/passport number had been correctly captured by the political party responsible for his non-consensual registration. Another victim commenting on the same thread indicated that his name and age had been guessed wrongly. Clearly, both instances could have dangerous implications for citizens' privacy and democracy in general.
See Wamathai, J. (2017). Registered as a political party member without your consent? Here's how to deregister. *Hapa Kenya.* https://hapakenya.com/2017/03/05/registered-as-a-political-party-member-without-your-consent-heres-how-to-deregister/

[201] See Muthuri, R., Karanja, M., Monyango, F. and Karanja, W. (2018).

[202] http://www.immigration.go.ke/integrated-population-registration-systemiprs/

[203] https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf

nothing in the legislation to suggest that it will not apply to political parties.[204] There are some 40 additional legal provisions relating to data protection. [205] Many of these frameworks are sectoral. Some deal with various public and private relationships; and others relate to "the treatment and access to documents and information handled by governmental entities and bodies".[206]

In the case of political advertising, there are possibly only a few countries that could compare with Brazil in terms of the breadth and detail of state regulations. Substantive legal provisions that have guided political advertising in Brazil can be found in the Electoral Code[207] and the electoral standards.[208] The Political Reform Law[209], as well as a Superior Electoral Court's (TSE) Resolution[210] both passed in 2017 also have major implications for political advertising — or as they call it in Brazil, electoral propaganda. These laws regulate provide instructions on many specific aspects of political campaigning: when parties can campaign, when parties should be on television and radio and even the size of campaign pamphlets that can be left in private properties. Overall, there is a clear commitment in these laws to control the electioneering process to reduce social, political and financial cost as well as prevent corporate capture of the political process.

Article 57 in the electoral standards is dedicated to regulating electoral publicity on the Internet. It provides that political campaigns should be conducted on websites owned by candidates or political parties or coalitions, and registered with Brazil's electoral authority.[211] The website (as well as blogs, social networks, instant messaging sites and similar internet applications) must be hosted directly or indirectly by locally-established internet service providers.[212]

Candidates, parties and coalitions are not allowed to pay for adverts on third party websites but they can pay to boost social media ads and prioritise their content in search engine results. All content must be posted by natural persons and not robots or fake accounts. Also, campaign messages on the internet must come with unambiguous information as to the party, candidate or coalition that is responsible for the content. Additionally 57-b/iii instructs that while electronic messages can be sent by political parties, coalitions and candidates to voters, the addresses should have

[204] Law No. 13,709 of August 14, 2018 on the protection of personal data. English translation at: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf
[205] Monteiro, R.L. (2018). The new Brazilian General Data Protection Law — a detailed analysis. *IAPP*. https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/
[206] Privacy International. (2019). *State of Privacy in Brazil.* https://privacyinternational.org/state-privacy/42/state-privacy-brazil
[207] See part 5/Title II of Law 4.735/1965. http://www.planalto.gov.br/ccivil_03/leis/L4737.htm#art240
[208] See Articles 36-57 in Law 9504/1997. http://www.planalto.gov.br/ccivil_03/leis/l9504.htm#art36a
[209] Law 13.488/2017
[210] See Resolution 23.551. http://www.tse.jus.br/legislacao-tse/res/2017/RES235512017.html
[211] See 57b(i) and 57b(ii) in Law 9504/1997.
[212] See 57b(iv) in Law 9504/1997

been "collected without payment." Article 57-e adds that particular entities "may not use, donate or transfer the electronic records of their customers in favor of candidates, parties or coalitions". A number of different bodies are listed including; "body under direct or indirect public administration or foundation maintained with government resources"; "public utility type of entity"; "professional association or union"; "entities devoted to charity and religious affairs"; "civil society organisations of public interest". The law also bans the sale of email address lists. Article 57-g instructs that recipients of messages should be able to unsubscribe from the messaging service.

Brazil's broader Internet Law (Marco Civil da Internet) protects civil rights in the specific context of internet use.[213] The law provides more explicitly for the inviolability of privacy and confidentiality of internet communications and upholds the general need for express consent "on the collection, use, storage and processing of personal data."[214] However, like the Article 57 of the electoral standards discussed above, the Marco Civil da Internet is specific to internet-based activities. To curb this challenge, Brazil's Superior Electoral Court via Resolution 23.551 expanded the scope of the campaign advertising laws to cover the instant messaging and voice calling applications of smartphones.[215]

While all these legal provisions could help regulate the micro-targeting of voters in Brazil, the dystopian realities of political marketing as seen in Brazil's last general elections prove that more efforts are needed to curb the micro-targeting of voters by political actors. There are two major challenges when it comes to regulating the micro-targeting of voters. The first is that despite the provisions of Article 57 and the Marco Civil da Internet, the non-consensual collection, sharing and use of personal data were still prevalent. Second, non-website messaging platforms especially WhatsApp became central to targeting of voters.

Even before Brazil's general elections in October 2018, the Tactical Technology Collective, cautioned:

> With the debut of sponsored ads in the 2018 Brazilian elections, the country will perhaps experience the biggest push toward the use of personal voter data. Whereas voters were once primarily influenced by television and web ads, the introduction of content promotion in social networks, ad-targeting practices and the use of personal data for enhancing and directing propaganda

[213] Marco Civil Law of the Internet in Brazil. (April 2014). *CGI.* https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180

[214] See Article 7 (ix) in the Marco Civil da Internet

[215] See Article 32(xv) in Resolution 23.551

> online may subject voters to much more targeting and segmentation, yet potentially much less access to information.[216]

Tactical Tech's prediction was based on the key findings from a study by Coding Rights on the digital campaigning industry in Brazil. The study found that the ease of access to voters online, the severe legal constraints on running political messages on radio and television, as well as the legal reform permitting contestants to pay for adverts on social media would mean that more political parties would concentrate on social media and mobile platforms to win votes.[217] Paid political advertising on social media platforms like Facebook was bound to be based on user-profiling and targeted messages. The researchers also noted that a thriving data brokering industry existed in Brazil. Data brokers were already collecting data such as those from social networking sites, credit rating bureaus and census bodies for purposes of micro-targeting. The researchers also indicated that as WhatsApp was the most popular digital platform in Brazil (an estimated 125 million users) and is typically available for free, it would become a major battleground for targeting voters.

These predictions by Tactical Tech and Coding Rights were manifested during Brazil's October 2018 elections. It is reported that political campaigners deployed software that searched Facebook for the phone numbers of potential voters. Such software could choose a "target audience by searching for keywords, pages or public groups on Facebook" and could also send around "300,000 messages at a time".[218] After scraping for personal data, the software automatically sent WhatsApp messages to phone numbers and also added the owners of these phone numbers to WhatsApp groups for political campaign purposes. The software reportedly could sort data according to city, gender and interests. As Rafael Evangelista and Femanda Bruno explain in a working paper, the use of WhatsApp for political messaging in Brazil was not necessarily random.[219] The authors show how political campaigners "built and took advantage of new or already established discussion groups of specific issues to target messages and to hiddenly manage these groups." In addition, many of these messages incited racial tensions and homophobia for political advantage.[220]

---

[216] Tactical Tech. (October 2018). *Brazilian Elections and the Public-Private Data Trade.* https://ourdataourselves.tacticaltech.org/posts/overview-brazil/

[217] Coding Rights & Tactical Tech. (2018). *Analysis of the playing field for the influence industry in preparation for the Brazilian general elections.* https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-data-and-politics-brazil.pdf

[218] Magenta, M., Gragnani, J. & Souza, F. (2018). How WhatsApp is being abused in Brazil's elections. *BBC.* https://www.bbc.com/news/technology-45956557

[219] Evangelista, R. and Bruno, F. (2019). *WhatsApp and political instability in Brazil: targeted messages and political radicalization.* This paper was presented at the conference on "Data-driven elections: Implications for and Challenges for Democratic Societies" held in Victoria, BC, Canada in April 2019.

[220] Ibid.

The flurry of 'fake news' was so intense that the matter was eventually investigated by Brazil's electoral court after the first round of elections. This was despite the fact that in May 2018, the head of Brazil's Supreme Electoral Court had signed an agreement with a number of political parties indicating symbolic commitment to fighting the spread of fake news.[221] Despite its moves to curb the spread of fake news, the court admits that "there is no specific electoral legislation for WhatsApp" beyond laws on internet-based electoral advertising.[222]

The abuse of existing laws as well as the increasing centrality of encrypted messaging platforms like WhatsApp in political campaigns have left the Brazilian state in a position of playing catch-up. While recent legal reforms that permit political parties, candidates and coalitions to pay for political advertisements on social media and prioritisation on search engines allow politicians to better reach voters, the reforms have also made voter profiling and micro-targeting more acute.

Positively, Brazil's General Data Protection Law will come into effect in 2020. In the specific context of politics, the law classifies political opinion and political organisation membership as sensitive data and protects them. As political parties and political campaigning are not explicitly mentioned in the law, it remains to be seen how the operationalisation of the law will shape the activities of political parties as they campaign in the future.

Critical Questions about Voter Surveillance and Democratic Engagement

Modern digital technologies are obviously shaping and "curating" the information we consume online. The curation of *political* information through secret algorithms gives the social media platforms enormous power over our worldviews, and extraordinary abilities to modify our political beliefs and behaviours.[223] That said, we should be cautious about technological determinism; just because the technology is available does not mean that it will be used, nor that it will have similar impacts. Data-driven elections are clearly technologically intensive affairs. As Nick Anstead has remarked, "the reality is that discussions about data in politics sit at the confluence of the social, institutional, and the cultural. Debates on the subject is inevitably reflect our deepest hopes and fears about the health of our democracy."[224]

---

[221] Superior Electoral Court. (June 2018). *2018 Elections: TSE and political parties sign an agreement for not spreading fake news.* http://english.tse.jus.br/noticias-tse-en/2018/Julho/2018-elections-tse-and-political-parties-sign-an-agreement-for-not-spreading-fake-news

[222] Magenta, M., Gragnani, J. & Souza, F. (2018).

[223] See page 9 in Hankey et. al (2018)

[224] Anstead, N. (2018). Data and Election Campaigning. *Political Insight*, *9*(2), 32-35.

There is nothing inevitable about these trends. Democracy does not require detailed knowledge of the beliefs and intentions of voters. Voter surveillance is an attribute of a particular type of "engagement" — one that is measured in the superficial and ephemeral metrics of social media. On the contrary, privacy protection is a necessary condition for more genuine forms of political participation, especially in countries that have recent memories of authoritarian rule.

The cases analysed above demonstrate that the nature and level of voter surveillance in different jurisdictions will be determined by a complex interplay of legal, political, and cultural factors.

Relevant *legal* provisions include:

- Constitutional provisions relating to freedom of communication, information and association, particularly with respect to public and political affairs
- Data protection (information privacy) law, which applies the broad range of information privacy principles on the capture, processing and dissemination of personally identifiable information, and more specifically to sensitive data on political opinions
- Election law — which often regulates the distribution of voter lists and registers and imposes sanctions for the illegitimate use and disclosure of those lists
- Campaign financing law — which regulates the amount spent by political parties and individual candidates, and often requires the capture of data on donors, and the amounts donated
- Telemarketing rules — which establish the conditions under which direct personalised communication can occur by marketers, pollsters and others
- Online Advertising Codes
- Election advertising codes
- Anti-spam rules — the related rules about unsolicited communication by email or text

The overall balance is also going to be profoundly affected by *structural* features of the political system that shape the nature of political competition, and the role that personal data plays in that competition: [225]

- The electoral system: proportional representation or "first-past-the-post"; compulsory or non-compulsory voting; the existence of "primary elections;" the frequency of referendums
- The party system: how many parties are competitive for legislative seats; centralisation vs. decentralisation of party organisations; whether the party system is the same at national and local levels

There are also wider *cultural*[226] variables, associated with historical experience:

- The general acceptability of direct candidate-to-voter campaigning practices, such as door-to-door canvassing, or telephone polling
- The legacies of authoritarian rule which create wider fears of political persecution
- The overall degree of trust in political elites
- The overall willingness to participate in political affairs, and to believe that participation will "make a difference."

There is a complex array of legal, institutional, historical and cultural variables which determine the extent to which elections are, and can be, "data-driven." We obviously need far more empirical research on how these factors play out in individual jurisdictions.

More broadly, there are a series of more critical questions about the effects of these trends on democratic engagement. What are the broader effects of the "consumerization of the political space" in which we are assumed to have preferences and tastes that only need to be unearthed using the most sophisticated technology to determine what public policies and goods voters "want"? What are the broader political implications of treating voters like consumers, of "shopping for votes"? [227]

A first set of concerns relate to *divisiveness.* Does micro-targeting lead to an increased tendency to deliver messages on "wedge issues"? Does it contribute to a fragmentation of the political system and increased partisanship? Does it produce

[225] Bennett, C.J. (August 2013). The politics of privacy and the privacy of politics: parties, elections and voter surveillance in Western democracies. *First Monday*, *Vol. 18*, No. 8.
[226] Aronoff, M. J. (2001). Political culture. *International Encyclopedia of the Social & Behavioral Sciences*, pp. 11640-11644.
[227] Delacourt (2017).

"filter bubbles" when individuals only see an algorithmically curated subset of information?

Secondly, there are concerns about the effect on the *"marketplace of ideas"* when false advertising cannot be countered in real time? In the open, false claims might be challenged. In secret, they can stand unchallenged.[228]

Thirdly, there are concerns about political *participation*. Does micro-targeting contribute to lower rates of political participation, as voters perceive that their interests are being manipulated by political and technical elites? Does this precise segmentation reduce the portion of the electorate that politicians need to campaign to and for, and ultimately care about after the election? Does this mean that the interests of others are ignored, or marginalised? In larger terms, does it encourage patron-client forms of politics?[229]

Fourthly, there are concerns about the effects on *campaigning* itself. Do data-driven campaigns mean "permanent campaigns"? Does the perceived need for data on voters' interests and beliefs mean that parties have the capacity to make voter contact a more enduring enterprise, before, during and after official election campaigns?[230] Do data-driven elections discourage volunteering for political parties? Do data-driven elections erode the face-to-face contact with the voter which are common in those countries used to door-to-door canvassing?

Fifth, there are concerns about its effects on *governance*. When one message is given to one group of voters, and another to a different group of voters, does micro-targeting lead to more ambiguous political mandates for elected representatives?[231]

Sixth, there are concerns about the *party system and electoral competition*. Do data-driven elections favour larger and more established political parties, which have the resources to employ the technical consultants to manage the data and coordinate the messaging?

Finally, and in those countries whose electoral politics are more fragile, is there a danger that data-driven elections will strengthen the *surveillance* state? Is knowledge

[228] Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *Information Polity*, *23 (4)*, 429-434.
[229] See page 209 in Hersh (2015).
[230] See page 258 in Delacourt (2016); Patton, S. (2017). Data, Parties and the Permanent Campaign. In *Permanent Campaigns in Canada.* Alex Marland et al. (eds). Vancouver: University of British Columbia Press. pp. 47-66.
[231] Barocas, S. (2012). The price of precision: Voter microtargeting and its potential harms to the democratic process. In *Proceedings of the first edition workshop on Politics, elections and data*, pp. 31-36.

of voting beliefs and intentions a valuable resource for agents of national security and intelligence?

Questions about the legitimate processing of personal data on the electorate is at the heart of the answer to each of these larger questions. What then are the lessons for the world's DPAs, as well as the larger community of privacy advocates and experts?

Conclusion: Challenges for Data Protection Authorities

Familiar data protection questions on transparency, fair processing, consent, security, and accountability, are now at the center of an international debate about democratic practice. DPAs now find themselves at the center of this global conversation.

Although most of the practices surveyed above have been pioneered in the pro-typical elections in the U.S., this is not just an American problem. Elections in many other countries are increasingly "data-driven" and methods of personalised political messaging increasingly sophisticated. The inherent competitiveness of the party political struggle in different countries has prompted elites to try to gain any edge over their rivals. The domestic demand for voter analytics is eagerly met by the political influence industry, and by an increasingly close collaboration between political parties and the major social media platforms.

To the extent that contemporary elections are "data-driven", their worst effects have been apparent in countries whose privacy/data protection laws do not cover political parties and other political actors. Data protection has not impeded political parties' ability to perform their basic democratic functions: political mobilisation, recruitment and policy development.

In countries where political parties and candidates are not covered by a uniform data protection law, one set of rules applies to the parties, and another to the wider network of data analytics, polling and consulting companies that operate within the "permanent campaigns" of modern democracy. In countries like Canada and Australia, this is a situation that cannot be defended or sustained.

The human and financial resources open to DPAs are, of course, limited. Attention to the use of data in elections competes with equally compelling national and global data protection issues in government and the private sector. That said, this analysis suggests the following lessons and challenges for DPAs.

- *The importance of understanding the political campaigning network*: Contemporary political campaigning is complex, opaque and involves a shifting ecosystem of actors and organisations, which can vary considerably from society to society. An important lesson from the investigations of political campaign practices in the UK and elsewhere, is that DPAs should acquire a broader understanding of that network in their respective societies.
- *The importance of understanding the entire regulatory environment for elections:* A diverse array of constitutional, statutory and self-regulatory rules can affect the processing of personal data in the electoral context. It is important for national DPAs to have a comprehensive grasp of the regulatory conditions that permit, or prohibit, the processing of personal data for purposes of democratic engagement, including the rules for campaign financing.
- *The importance of cooperation with other national regulators*: It is equally important to cooperate with other relevant regulators including elections and telecommunications regulators. Elections regulators, in particular, have the long-standing expertise in elections law and the experience in administering the many facets of elections administration, including the distribution of voters lists. However, the regulation of personal data processing in the electoral context cannot be left to elections regulators alone. The larger context of "data-driven" elections is not something the typical elections regulator has the resources, or competence, to regulate.
- *The importance of the relationship between data protection law and election financing:* Recent proposals for ad transparency, including digital archiving, offer opportunities for DPAs better to understand the nature of political micro-targeting in their respective societies, the level of granularity, and the source(s) of payment. In the world of political campaigning, data protection infractions can also be elections financing infractions, and vice versa. Ad transparency requirements can provide an important source of leverage for regulators and advocates.
- *The importance of proactive guidance on best campaigning practices*: The risks outlined above cannot simply be understood in response to individual complaints to particular candidates and parties at the time of elections. DPAs can assist political parties. They have valuable experience in the detailed and practical work of data protection implementation and privacy management, and can assist in the tailoring of rules to the elections context.
- *The importance of international collaboration:* These are clearly global questions requiring the highest level of international collaboration between DPAs, in Europe and beyond. The political "influence industry" knows no geographic boundaries. Its impact nationally and internationally will require the most vigilant and constant cross-national attention from DPAs through their

international and regional associations, as well as from the wider network of international privacy advocates and experts.

Key Works Cited

Anstead, N. (2018). Data and Election Campaigning. *Political Insight*, *9*(2), 32-35.

Aronoff, M. J. (2001). Political culture. *International Encyclopedia of the Social & Behavioral Sciences*, pp. 11640-11644.

Bachtiger, A., John S. Dryzek, Jane Mansbridge and Mark E. Warren. (2018). *The Oxford Handbook of Deliberative Democracy*. Oxford: Oxford University Press.

Baldwin-Philippi, J. (2017). The myths of Data-Driven Campaigning. *Journal of Political Communication. Vol 34,* No. 4.

Barocas, S. (2012). The price of precision: Voter microtargeting and its potential harms to the democratic process. In *Proceedings of the first edition workshop on Politics, elections and data*, pp. 31-36.

Bartlett, J., Smith, J., and Acton, R. (July 2018). The Future of Political Campaigning. *Demos*. https://www.demos.co.uk/wp-content/uploads/2018/07/The-Future-of-Political-Campaigning.pdf

Bennett, C.J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Ithaca: Cornell University Press.

(2013). The politics of privacy and the privacy of politics: parties, elections and voter surveillance in Western democracies. *First Monday*, *Vol. 18*, No. 8.

(June 2013). Privacy, elections and political parties: emerging issues for data protection authorities. *Privacy Laws and Business International*, Issue 123.

(2015). Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications. *Surveillance and Society*, *Vol. 13*, No. 3-4. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/voter_surv

(December 2016). Voter databases, micro-targeting and data protection law: can political parties campaign in Europe as they do in North America?. *International Data Privacy Law*, *Vol. 6*, No. 4, 261-75.

(2018). Cambridge Analytica and Facebook: A Wake-Up Call. *Privacy Laws and Business International Report,* Issue 152.

(2019). Data-Driven Elections in Canada: What we Might Expect in the 2019 Federal Election Campaign. *Journal of Parliamentary and Political Law 13* JPPL, 301-313.

Bennett, C.J. and Bayley, R.M. (March 2012). Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis. *Office of the Privacy Commissioner of Canada*. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/#toc3a

Bennett, C. J., Haggerty, K. D., Lyon, D., & Steeves, V. (Eds.). (2014). *Transparent lives: surveillance in Canada*. Athabasca University Press.

Chester, J. and Montgomery, K, (December 2017). The role of digital marketing in political campaigns. *Internet Policy Review: Journal of Internet Regulation*, *Volume 6,* No. 4.

Chief Electoral Officer of Canada. (2013). *Preventing Deceptive Communications with Electors.* http://www.elections.ca/res/rep/off/comm/comm_e.pdf

CNIL. (January 2012). *Communication Politique: Obligations Legale et Bonnes Pratiques.* https://www.cnil.fr/sites/default/files/typo/document/CNIL_Politique.pdf

(November 8, 2016). *Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?*. https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.

(November 2016). *Elections 2016 / 2017: quelles règles doivent respecter les candidats et partis?*. https://www.cnil.fr/fr/elections-2016-2017-quelles-regles-doivent-respecter-les-candidats-et-partis

Coding Rights & Tactical Tech. (2018). *Analysis of the playing field for the influence industry in preparation for the Brazilian general elections.* https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-data-and-politics-brazil.pdf

Cohen, J.E. (2012). *Configuring the Networked Self: Law, Code and the Play of Everyday Practice*. New Haven: Yale University Press.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (January 1981). *Council of Europe*. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

Dalton, R. J., Shin, D. C., & Jou, W. (2007). Popular conceptions of the meaning of democracy: Democratic understanding in unlikely places. *CSD*. https://escholarship.org/content/qt2j74b860/qt2j74b860.pdf

Delacourt, S. (2015). *Shopping for Votes: How Politicians Choose Us and We Choose them*, 2nd ed. Madeira Park, BC: Douglas and McIntyre.

'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data'. (1995). *Official Journal L 281, P. 0031 - 0050.* *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046*

EDPS. (March 2019). *EDPS Opinion on online manipulation and personal data.* *https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf*

Endres, K., & Kelly, K. J. (2018). Does microtargeting matter? Campaign contact strategies and young voters. *Journal of Elections, Public Opinion and Parties*, *28*(1), 1-18.

'EU Code of Practice on Disinformation'. (September 2018). https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

European Commission. (2018). *Free and fair European elections – Factsheet.* https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_en.pdf;

(2018). *Action Plan against Disinformation. European Commission contribution to the European Council.* https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf;

(2018). *Commission guidance on the application of Union data protection law in the electoral context.* https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf

(2018). *Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament.* https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf

(2018). *Tackling online disinformation: a European Approach*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

(September 2018). *Code of Practice on Disinformation*. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

European Data Protection Board (EDPB). (March 13, 2019). *Statement 2/2019 on the use of personal data in the course of political campaigns.* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

European Union Article 29 Data Protection Working Party. (2011). *Advice Paper on special categories of data ("sensitive data")*. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-

document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf

Garante per la protezione dei dati personali. (March 6, 2014). Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale. *Official Gazette of the Italian Data Protection Authority 71*. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267

Gavison, R. (January 1980). Privacy and the Limits of the Law. *The Yale Law Journal*. vol. 89, no 3, 455.

Gellman, R. M. (1993). Fragmented, Incomplete and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions. *Software Law Journal* VI: 199-238

Gorton, W. (2016). Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy, *New Political Science*, *no. 1*. pp. 61-80. https://doi.org/10.1080/07393148.2015.1125119

'Guidelines for Prevention of Dissemination of Undesirable Bulk Political SMS and Social Media Content via Electronic Communications Networks'. (2017). https://ca.go.ke/wp-content/uploads/2018/02/Guidelines-on-Prevention-of-Dissemination-of-Undesirable-Bulk-and-Premium-Rate-Political-Messages-and-Political-Social-Media-Content-Via-Electronic-Networks-1.pdf

Haggerty, K. and Samatas, M. (eds). (2010). *Surveillance and Democracy*. New York: Routledge.

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

Harris, L., & Harrigan, P. (2015). Social media in politics: The ultimate voter engagement tool or simply an echo chamber? *Journal of Political Marketing, 14*(3), 251–283.

Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *Information Polity*, *23 (4)*, 429-434.

Hersh, E. (2015). Hacking the Electorate: How Campaigns Perceive Voters. Cambridge: Cambridge University Press.

House of Commons Standing Committee on Access to Information, Privacy and Ethics. (June 2018). *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*.

Information Commissioner's Office (ICO). (2014). *Guidance for Political Parties for Campaigning for Promotional purposes*. https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf

(July 2018). *Democracy Disrupted: Personal Information and Political Influence*. https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

(July 2018). *Investigation into Data Analytics in Political Campaigns: Investigation Update*. https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf

(November 2018). *Investigation into the use of data analytics in political campaigns. A Report to Parliament*. https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

(June 2019). *Update report into adtech and real time bidding*. https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

(August 2019). *Guidance on Political Campaigning: Draft Framework Code for Consultation*. https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf

Issenberg, S. (2013). *The victory lab: The secret science of winning campaigns*. Portland: Broadway Books.

James, F. (2009). *When the People Speak: Deliberative Democracy and Public Consultation*. New York: Oxford University Press.

Judge, E. and Pal, M. (2014). Privacy and the Electorate: Big Data and the personalization of Politics. *University of Ottawa Center for Law, Technology and Society*. http://techlaw.uottawa.ca/sites/techlaw.uottawa.ca/files/judge_pal_privacyandtheelectorate_ksg_report_oct_14_final.pdf.

Kim, Y. M., Hsu, J., Neiman, D., Kou, C., Bankston, L., Kim, S. Y., ... & Raskutti, G. (2018). The stealth media? Groups and targets behind divisive issue campaigns on Facebook. *Political Communication*, *35*(4), 515-541.

Kreiss, D. (2011). Yes we can (profile you): A brief primer on campaigns and political data. *Stan. L. Rev. Online*, *64*, 70.

Kreiss, D. (2016). *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy*. Oxford: Oxford University Press.

Lever, A. (2015). Privacy and democracy: What the secret ballot reveals. *Law, Culture and the Humanities*, *11*(2), 164-183.

Lijphart, A. (ed.). (1992). Parliamentary versus presidential government. Oxford: Oxford University Press; Schmitter, P. C., & Karl, T. L. (1991). What democracy is... and is not. *Journal of democracy*, *2*(3), 75-88.

Lyon, D. (2018). *The Culture of Surveillance*. Cambridge: Polity Press.

McEnvoy, M. (February 2019). *Full Disclosure: Political Parties, Campaign Data and Voter Consent*. Investigation Report P19-01. https://www.oipc.bc.ca/investigation-reports/2278

Mill, J.S. (1869, 1991). *On Liberty and Other Essays.* John Gray (ed). Oxford: Oxford University Press.

Muthuri, R., Karanja, M., Monyango, F., and Karanja, W. (2018). *Investigating Privacy Implications Of Biometric Voter Registration In Kenya's 2017 Election Process*. https://privacyinternational.org/sites/default/files/2018-06/Biometric%20Technology-Elections-Privacy.pdf

Mutung'u, G. (2018). The Influence Industry Data and Digital Election Campaigning. *Tactical Tech*. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf

Nickerson D.W. and Rogers T. (2014). Political Campaigns and Big Data. *The Journal of Economic Perspectives, 28* (2).

Nielsen, R.K. (2012). *Ground Wars: Personalised Communication in Political Campaigns*. Princeton: Princeton University Press.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy and the Integrity of Social Life.* Stanford: Stanford University Press.

O'Connor, N. (January 2018). Reforming the U.S. Approach to Data Protection and Privacy. *CFR*. https://www.cfr.org/report/reforming-us-approach-data-protection

Office of the Information and Privacy Commissioner of BC. *Summary of the Office of the Information and Privacy Commissioner's Investigation of the BC NDP's use of social media and passwords to evaluate candidates*. https://www.oipc.bc.ca/mediation-summaries/1399

(August 2013). *Sharing of Personal Information as Part of the Draft Multicultural Strategic Outreach Plan: Government of British Columbia and BC Liberal Party.* https://www.oipc.bc.ca/investigation-reports/1559

(February 2019). *Full Disclosure: Political Parties, Campaign Data and Voter Consent*. https://www.oipc.bc.ca/investigation-reports/2278

Office of the Privacy Commissioner of Canada. (2018). *Appearance before the Standing Committee on Procedure and House Affairs on the study about Bill C-76, Elections Modernization Act.* https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_20180605/#amendments

(January 2018). Overview of Privacy Legislation in Canada. *Office of the Privacy Commissioner of Canada*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.

(May 30, 2018). *Remarks at presentation before the Senate Open Caucus.* https://www.priv.gc.ca/en/opc-news/speeches/2018/sp-d_20180530/

Ontario Information and Privacy Commissioner. (2017). *Thirty Years of Access and Privacy Service, 2017 Annual Report.*

Packard, V., & Payne, R. (1957). *The hidden persuaders*. New York: D. McKay Company.

Parsons, C., Colin J. Bennett and Adam Molnar. (2015). Privacy, Surveillance and the Social Web. In B. Roessler and D. Mokrosinska (eds.). *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Cambridge: Cambridge University Press.

Pateman, C. (1975). *Participation and Democratic Theory*. Cambridge: Cambridge University Press.

Patton, S. (2017). Data, Parties and the Permanent Campaign. In *Permanent Campaigns in Canada.* Alex Marland et al. (eds). Vancouver: University of British Columbia Press. pp. 47-66.

Privacy International. (2019). *State of Privacy in Brazil.* https://privacyinternational.org/state-privacy/42/state-privacy-brazil

Regan, P. (1995). *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill: University of North Carolina Press.

'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on General Data Protection Regulation' (OJEU L119 1). http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

'Resolution on the Use of Personal Data for Political Communication'. (16 September 2005). https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf

Richards, N. (2015). *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age.* Oxford: Oxford University Press.

Rubinstein, I. S. (2014). Voter privacy in the age of big data. *Wis. L. Rev.*, 861.

Schwartz, P. M. (1999). Privacy and democracy in cyberspace. *Vand. L. Rev.*, *52*, 1607.

Shils, E. (1956). *The Torment of Secrecy*. Glencoe, Ill: Free Press.

Solove, D. (2008). *Understanding Privacy.* Cambridge: Harvard University Press.

Spicer, M. W. (2019). What do we mean by democracy? Reflections on an essentially contested concept and its relationship to politics and public administration. *Administration & Society, 51*(5), 724-748

Steeves, V. (2009). Reclaiming the Social Value of Privacy. In Kerr, I. Steeves, V and Lucock, C. (eds). *Lessons from the Identity Frail: Anonymity, Privacy and Identity in a Networked Society.* New York: Oxford University Press, pp. 191-288.

Tactical Tech. (March 2019). *Personal Data: Political Persuasion – Inside the Influence Industry. How it works.* Berlin: Tactical Tech. https://tacticaltech.org/#/projects/data-politics/

(June 2018). *Malaysia: Voter Data in the 2018 Elections.* https://ourdataourselves.tacticaltech.org/posts/overview-malaysia

(August 2018). *India: Digital Platforms, Technologies and Data in the 2014 and 2019 Elections.* https://ourdataourselves.tacticaltech.org/posts/overview-india

(September 2018). *Chile: Voter Rolls and Geo-targeting.* https://ourdataourselves.tacticaltech.org/posts/overview-chile

(October 2018). *Brazilian Elections and the Public-Private Data Trade.* https://ourdataourselves.tacticaltech.org/posts/overview-brazil/

(November 2018). *WhatsApp: The Widespread Use of WhatsApp in Political Campaigning in the Global South*. https://ourdataourselves.tacticaltech.org/posts/whatsapp/

Volokh, E. (2000). Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You. *52 STAN. L. REV. 1049,* 1050–51.

Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. *Harv. L. Rev., 4*, 193.

Westin, A.F. (1967). *Privacy and Freedom.* New York: Atheneum.

COLIN J. BENNETT

Colin Bennett received his Bachelor's and Master's degrees from the University of Wales, and his PhD from the University of Illinois at Urbana-Champaign. Since 1986 he has taught in the Department of Political Science at the University of Victoria. He has enjoyed Visiting Professorships at: Harvard's Kennedy School of Government; the Center for the Study of Law and Society at the University of California, Berkeley; the School of Law, University of New South Wales; the Law, Science, Technology and Society Centre at the Vrije Universiteit in Brussels; and at the Faculty of Information, University of Toronto. His research has focused on the comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels. In addition to numerous scholarly and newspaper articles, he has written or edited seven books, including *The Governance of Privacy* (MIT Press, 2006 with Charles Raab); and *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press, 2008). He has completed policy reports on privacy and data protection for many national and international agencies. He was co-investigator of a large Social Sciences and Humanities Research Council (SSHRC) Major Collaborative Research Initiative grant entitled "The New Transparency: Surveillance and Social Sorting" which culminated in the 2016 report: *Transparent Lives: Surveillance in Canada*. Through a SSHRC Partnership Grant on "Big Data Surveillance", and a new SSHRC Insight Grant, he is currently researching the comparative politics of data-driven elections, and the capture and use of personal information by political parties and candidates in Western democracies.

SMITH ODURO-MARFO

Smith Oduro-Marfo received his Bachelor's and Master's degrees from the University of Ghana and is currently a PhD candidate with the Political Science Department, University of Victoria. He researches issues relating to surveillance, privacy, and identification systems in Africa. He is particularly interested in how these issues intersect (or not) with the concept, conditions and practice of Development. His ongoing dissertation project, supervised by Dr. Colin Bennett, is a study on how citizen identification systems in Ghana interact with Development and ideas of progress. Smith is currently a research fellow with the "Big Data Surveillance project" (hosted at Queens University), the International Development Research Centre (Canada), and the Centre for Global Studies (University of Victoria). He runs the www.privacyinafrica.com website which collates news articles on surveillance, identification and privacy issues in Africa.