Strasbourg, 26 October 2020

T-PD(2020)02Rev

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Personal Data Processing by and for Political Campaigns: The Application of the Council of Europe's Modernised Convention 108

by

Professor Colin J. Bennett

Directorate General of Human Rights and Rule of Law

The opinions expressed in this work are the responsibility of the authors and do not necessarily reflect the official policy of the Council of Europe

Table of Contents

Executive Summary

Election campaigns in many countries are now driven my complex data analytics, and by a range of new technologies advanced by the "political influence" industry. At the center of efforts to control these practices and combat electoral manipulation and propaganda lies the question of how personal data on individual voters is being processed in political campaigns, and whether or not it is done so legally and ethically. Familiar questions about privacy are now at the center of a heated international debate about democratic integrity, and about the rights to free elections and voter autonomy enshrined in the European Convention on Human Rights.

The modernised Council of Europe Convention 108 has a unique role to play in limiting the surveillance of voters advancing ethical campaigning practices. It is explicitly designed as a global instrument and can travel to different parts of the world, and to established and emerging democratic societies. It is explicitly rooted in human rights and democratic, rather than commercial, terms. It is a technologically neutral instrument which can address new challenges raised by new campaign and voter analytics technologies. It provides a baseline standard for the promotion of best practices for the variety of data controllers and data processors within the global campaigning networks. And it offers a principle-based standard for the coordination of privacy rules across the realms of data protection and election law.

Guidance from the Council of Europe about personal data processing by, and for, political campaigns, would need to address some key issues with reference to recent decisions by data protection authorities, including: the breadth of the meaning of "political opinions" as a form of sensitive data; the identifiability and re-identifiability of personal data on political opinions; rules on consent and political communication; questions of proportionality in the light of the legitimate purposes of political campaigning; the processing of data that has been made "public" through social media platforms; responsibilities for transparency across the campaigning networks; and the appropriate rules for automated decision-making and voter profiling.

The Council of Europe is uniquely suited to address the privacy implications of data-driven elections. A guidance document on Convention 108+ and political campaigning could potentially be very influential. It could assist countries balance privacy protection with the broader duties of political organizations to engage the electorate. It could also be adaptable to different legal environments, constitutional and administrative traditions, party and electoral systems, and political cultures.

Introduction[1]

There is a rich tradition of trying to understand the social value of privacy protection within democratic societies.[2] Privacy bolsters participation and engagement: voting freely, speaking out, engaging in interest groups, signing petitions, participating in civil society activism and protesting. It promotes individual autonomy, and thereby enhances our freedom to make choices under conditions of genuine reflection and equal respect for the preferences, values and interests of others.[3]

However, until recently, virtually nowhere in the 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 democratic process. In a vast literature, we find almost nothing on the monitoring of the electorate by political actors – by political parties, their candidates and the network of consultants and companies that work for them. We know that privacy is important *for* democracy. Until recently, we have known relatively little about how privacy has been compromised *by* democracy - by the agents that seek to mobilise, engage and encourage us to vote – or not to vote.[4]

That situation has obviously changed, rapidly and dramatically. The publicity about the activities of Cambridge Analytica (CA), the Canadian company (Aggregate IQ) and the harvesting of Facebook data through third party applications have achieved extraordinary prominence. These scandals have been investigated in several jurisdictions, and we now have a better grasp of the extent of the political influence industry,[5] and of the risks to democracy associated with the mass profiling of the electorate and the delivery of micro-targeted messages to increasingly narrow categories of voters:[6] "filter bubbles" and an increased willingness to deliver messages on divisive wedge issues; voter discrimination and disenfranchisement; a chilling of political participation; increased partisanship and polarisation; and ambiguous political mandates for elected representatives.[7] The opaqueness of much contemporary political messaging blocks the presumed self-correcting benefits of rights to freedom of speech and erodes the larger democratic conversation about the common good.[8] Data-driven elections and micro-targeting clearly have "macro" effects.[9]

---

[1] I am very grateful to Sophie Kwasny and Bohumila Ottova of the Council of Europe for assisting with the preparation of this report. Graham Greenleaf, Charles Raab and Lee Bygrave provided very helpful comments on earlier drafts. I am also grateful to the members of the delegations who asked questions and provided comments on the earlier versions presented at the panel on Data Protection Views (July 3, 2020) and at the Bureau meeting (September 29, 2020).

[2] A. Lever (2014). *A Democratic Conception of Privacy*. London: Authorhouse. B. Roessler and D. Mokrosinska eds. (2015). *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Cambridge: Cambridge University Press.

[3] C. J. Bennett and S. Oduro Marfo (2019). *Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities* (Paper delivered to 2019 Conference of International Privacy and Data Protection Commissioners) at: https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf

[4] Ibid.

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

[6] C. J. Bennett and D. Lyon eds. (2019). Data-Driven Elections. *Internet Policy Review*, Vol. 8, No. 1 at: https://policyreview.info/data-driven-elections

[7] E. Pariser (2012). *The filter bubble: How the personalised web is changing what we read and think.* New York: Penguin Books; D.S. Hillygus, D.S. & T. Shields (2008). *The persuadable voter: wedge issues in presidential campaigns*. Princeton, NJ: Princeton University Press; S. Barocas (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.

[8] S. Vaidhyanathan (2018). *Anti-Social Media: How Facebook Disconnects us and Undermines Democracy*. Oxford: Oxford University Press. p. 164

[9] S. Hankey, S. J.K. Morrison, and R. Naik (2018). *Data and democracy in the digital age*. The

At the center of efforts to combat electoral manipulation and propaganda lies the question of how personal data on individual voters is being processed in political campaigns, and whether or not it is done so legally and ethically. Familiar data protection questions are now at the center of a heated international debate about democratic integrity, and about the rights to free elections enshrined in the European Convention on Human Rights.[10] International instruments for the protection of data, such as the modernised Council of Europe's Convention 108,[11] assume an increasing importance in the regulation of data-driven elections, and in the support of broad democratic principles of pluralism and individual autonomy.

The basis of the privacy-related work of the Council of Europe is Article 8 of the European Convention on Human Rights. Since the 1970s, the Council of Europe has worked to promote data protection standards which culminated in the original Convention 108 passed in 1981.[12] Based on this long tradition, the modernised Convention 108+ of 2018 is explicitly rooted in a broad aim "to secure the human dignity and protection of the human rights and fundamental freedoms of every individual." It speaks of "personal autonomy based on a person's right to control of his or her personal data and the processing of such data." It recognises that the "right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression."[13]

The processing of personal data in political campaigns requires exactly this kind of reconciliation. Political parties perform unique and essential roles in democratic societies. They educate and mobilise voters. They are the critical mechanisms that link the citizen to his/her government. The processing of personal data by parties and candidates for the purposes of "democratic engagement" should perhaps allow a wide latitude to process personal data to educate and mobilise voters.[14] On the other hand, 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. Parties now "shop for votes" and voters perhaps choose parties in the same way that consumers shop for products.[15]

Given these realities, what is the appropriate balance between privacy rights and the obligations of political parties and candidates to educate and mobilise voters? With respect to data protection principles, is there any justification for treating political organisations differently from governmental agencies or commercial organisations? How can Convention 108+ assist in determining the appropriate balance? This study builds upon prior work by the Council of Europe on digital

Constitution Society, at: https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf

[10] Article 3 of Protocol No. 1 of the ECHR. "Everyone has the right to elect the government of his/her country by secret vote. Without this right there can be no free and fair elections. It guarantees the citizens' free expression, the proper representativeness of elected representatives and the legitimacy of the legislative and executive bodies, and by the same token enhances the people's confidence in the institutions."

[11] Council of Europe (2018). Convention for the protection of individuals with regard to the processing of personal data (2018) at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (hereafter Convention 108+)

[12] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 1981, Article 6 at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[13] Convention 108+, Preamble.

[14] Bennett and Oduro Marfo, *Privacy, Voter Surveillance and Democratic Engagement*, p. 4.

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

technologies and elections: the "Study on the use of internet in electoral campaigns;"[16] and particularly the work of the Venice Commission on Digital Technologies and Elections.[17]

The first section of the paper outlines some of the contemporary trends in political campaigning in modern democratic countries, according to recent reports from data protection authorities (DPAs) and academic research. The second section reviews some of the myths and realities about data-driven campaigning, and outlines briefly the broader set of legal, institutional and cultural factors that might determine the surveillance of the electorate in any one society.

The main body of the paper analyses the different, but related, data protection standards that apply directly to the processing of personal data in election campaigns. Of course, all provisions of Convention 108+ might apply to the processing of personal data by political organisations. This paper focusses on those data protection questions which require a more distinctive analysis in the political context, and are more generic across democratic states. It therefore reviews the relevant provisions of Convention 108+ on: identifiability and re-identifiability; the definition of sensitive political opinions; political communications; legitimate interests and proportionality; the processing of public data on social media; the obligation of transparency; and automated processing and profiling. Throughout, reference is made to parallel provisions within the EU General Data Protection Regulation (GDPR)[18] and to recent investigations into political campaign practices by DPAs in the UK, France and Canada.[19]

In conclusion, I argue that Convention 108+ has a unique role to play in the promulgation of good data protection practices for political campaigns, and thereby enhancing democratic rights. The history of the Council of Europe and its experience in promoting democratic rights make the organisation ideally suited to addressing these critical issues in both advanced industrialised societies, as well as within the more fragile and emerging democratic countries.

---

[16] Council of Europe, *Study on the Use of Internet in Election Campaigns*, DGI(2017)11 at: https://rm.coe.int/use-of-internet-in-electoral-campaigns-/16807c0e24

[17] Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies and Elections, adopted by the Council of Democratic Elections at its 65th meeting (Venice, 20 June 2019) and by the Venice Commission at its 119th Plenary Session (Venice, 21-22 June 2019) at: https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2019)016-e

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

[19] UK Office of the Information Commissioner (July 2018). *Democracy Disrupted: Personal Information and Political Influence* at: https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf; UK, ICO, *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 ; Office of the Privacy Commissioner of Canada (OPC) (2019) *Joint Investigation of Aggregate IQ Data Services Ltd. By the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia.* Report of Findings #2019-004 November 26, 2019 at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-004/; Office of the Information and Privacy Commissioner of BC (OIPCBC) (February 2019). *Full Disclosure: Political Parties, Campaign Data and Voter Consent* at: https://www.oipc.bc.ca/investigation-reports/2278; France, Commission Nationale de l'Informatique et des Libertés (CNIL) (November 8, 2016). *Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?* at: https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.

Trends in Digital Political Campaigning

The Facebook/Cambridge Analytica scandal was a reflection and a culmination of a series of trends that go back around twenty years.[20] A 2019 comparative report by the Tactical Tech collective tried to map these trends and portray today's global political "influence industry." It 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 (VRMs), 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). VRMs offer parties a fully integrated campaign management solution for all aspects of their campaigns – voter outreach, door-to-door canvassing, telemarketing, the delivery of signs and posters, event management, social media engagement, issue tracking and get-out-the-vote (GOTV) operations. Aside from the U.S., we know that these systems exist in Canada, the UK and Australia. They have typically been built with the assistance of consultants from the U.S.[21]

An increasing amount of personal data are now captured at the doorstep using new mobile applications, which increasingly place personal data assets in the hands of a multitude of campaign volunteers and allow them to deliver responses on the doorstep to party databases. Some DPAs have expressed concerns about the extent of personal data that might be recorded during canvassing, for instance on gender, ethnicity, or religion.[22] Their inquiries suggest that other information may be recorded without consent about other members of the household, including tenants, or maybe inferred from casual observation of the property – cars in the driveway, children playing in the garden, the general upkeep of the property and so on.[23]

Data operates as *intelligence* when it is accumulated as a result of testing and experimentation. Sasha Issenberg revealed the extent of these practices in *The Victory Lab* – "the secret science of winning campaigns."[24] The systematic comparison of the impact of messaging through "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, radio and social media ads.

Parties in most countries are becoming increasingly adept at using social media to target messages, to recruit volunteers and donors, and to track issue engagement. In contrast to more traditional telemarketing, the capture of data on social media can be used to build a circle of contacts for the purposes of "relational organisation" or "targeted sharing."[25] In Facebook, for instance, the party can upload an encrypted list of phone numbers or e-mails to create customised audiences, based on location, demographics, interests, behaviors and connections. The advertiser will receive real-time feedback, through relevance scores, on the effectiveness of the

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

[21] I review these systems in: C. J. Bennett, "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 (December 2016), pp. 261-275.

[22] OIPCBC, *Full Disclosure* (n 95) p. 15

[23] Ibid p. 16

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

[25] Pierre-Olivier Pielaet, *Report on the Application of the principles of the modernised Convention 108 to the processing of data by political parties* (Strasbourg: Council of Europe, unpublished 2020).

advertising campaign, and then make the necessary adjustments to the ad. A political ad on Facebook is less a discrete message and more a complex machine for producing further messaging through which the Facebook algorithms learn and deliver subtly different messages dependent on a multitude of different variables.[26]

There are a variety of further surreptitious mechanisms through which information on an individual's political beliefs might be harvested to produce data as intelligence. For example, the exercise of the "Like" button in Facebook displays the icon of that party on that individual's social media page, perhaps unintentionally displaying that individual's political beliefs. And "friending" a political party on Facebook without the user implementing the appropriate privacy controls can then result in the user's name and photo being captured by the party and targeted.[27] Privacy International has critiqued the surreptitious use of other unique ad identifiers, pixels and tags. It has also reviewed the various privacy settings of apps that may carry political ads, like TikTok, Snapchat and Pinterest to determine compliance with ad transparency rules.[28]

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 by Tactical Tech: 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 categorization and assignment of personality traits for which Cambridge Analytica became notorious.[29] *WhatsApp* has become a particularly powerful campaigning instrument. Easy to use, end-to-end encrypted and facilitating the sharing of messages to large groups, WhatsApp has been extremely popular in countries like India, Brazil and other countries in the Global South.[30] However, WhatsApp not only allows parties to tailor messages to precise groups, it also offers anonymity, thus making it easy to misrepresent a sender's identity.

In the U.S. Jeff Chester and Kathryn Montgomery trace the ongoing "marriage of politics and commerce" and the ongoing growth of data-driven political marketing.[31] They reviewed seven key techniques employed during the 2016 campaigns in the U.S., all of which point to the massive consolidation of data 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 now virtually indistinguishable from contemporary programmatic

[26] Bogost, I. and A.C. Madrigal (2020). How Facebook works for Trump. *The Atlantic* (April 17) at: https://www.theatlantic.com/technology/archive/2020/04/how-facebooks-ad-technology-helps-trump-win/606403/

[27] A thorough analysis of the use of Facebook in the electoral arena is provided in U.K. Information Commissioner's Office report *Democracy Disrupted? Personal information and political influence.*

[28] Apart from Facebook and Google, what are other platforms doing about political ads? At: https://privacyinternational.org/long-read/3703/apart-google-facebook-and-twitter-what-are-other-platforms-doing-about-political-ads#TikTok-ad-targeting

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

[30] E. Hickok (2018). *The Influence Industry: Digital Platforms, Technologies and Data in the General Elections in India* at: https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-india.pdf; R. Evangelista and F. Bruno, "WhatsApp and Political instability in Brazil: targeted messages and political radicalisation," Internet Policy Review, Volume 8, Issue 4 at: https://policyreview.info/articles/analysis/whatsapp-and-political-instability-brazil-targeted-messages-and-political

[31] J. Chester J., & K.C. Montgomery (2017). The role of digital marketing in political campaigns. *Internet Policy Review*, *6*(4), at: https://doi.org/10.14763/2017.4.773

advertising practices of the ad-tech sector, including the highly controversial process of "real-time bidding" (RTB), which has come under recent scrutiny from DPAs.[32]

In a 2019 update previewing the practices likely to be pursued in the 2020 election cycle, the same authors predict: an increasing sophistication in "identity resolution technologies"; a "rapidly maturing commercial geo-spatial intelligence complex enhancing mobile and other geotargeting strategies; the expansion into unregulated streaming and digital video platforms; and further developments in personalisation techniques and testing.[33]

A 2018 report from Demos, commissioned by the ICO has monitored digital marketing techniques in the UK and is perhaps a more reliable guide to digital campaigning in parliamentary systems. Demos previewed the kinds of practices likely to be observed in British political campaigning in the years ahead.[34]

- More detailed audience segmentation
- Cross-device targeting
- A growth in the use of psychographic techniques
- The use of AI to target, measure and improve campaigns
- The use of AI to automatically generate content
- The use of personal data to predict election results
- Delivery via new platforms (e.g. digital video and wearable tech)

The development of these techniques also have organizational consequences for political campaigns. Whereas it was once possible to distinguish the different kinds of organisations associated with political campaigning, the current network of institutions is now complex and opaque. We now see in several countries close alliances between political data brokers, digital advertising firms, social media platforms, data management and analytical companies, and political parties in a broad "campaigning ecosystem." Increasingly the modern political campaign 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; digital advertising; TV advertising; email and text messaging; social media outreach; event management; volunteer coordination; and get-out-the-vote (GOTV) operations. Each of these roles requires careful coordination.[35]

In general, therefore, more data on voters are being captured than in the past, and those data are increasingly shared through a complicated network of organisations, involving some quite obscure companies that are beginning to play important roles as intermediaries within the democratic process. These trends are global even though their impacts in different societies are highly variable.

---

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

[33] J. Chester and K. Montgomery (2019). The digital commercialisation of US politics – 2020 and beyond. Internet Policy Review. Volume 8, Issue 4 at: https://policyreview.info/articles/analysis/digital-commercialisation-us-politics-2020-and-beyond

[34] J. Bartlett, J. Smith & R. Acton (2018). *The Future of Digital Campaigning*. Demos, 2018 at: http://www.demos.co.uk/wp-content/uploads/2018/07/The-Future-of-Political-Campaigning.pdf

[35] R.K. Nielsen (2012). *Ground Wars: Personalised Communication in Political Campaigns*. Princeton: Princeton University Press; D. Kreiss (2016). *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy.* Oxford: Oxford University Press.

Data-Driven Elections: Myths and Realities

The current narrative about digitalised data-driven elections is often rooted in a technological imperative; if data are available on the electorate, then there should be a natural tendency to use it to influence voters and persuade them to turn up at the polls. This imperative permeates the sales pitches from the voter analytics industry and produces a competitive desire to claim higher and more precise levels of personal data on the electorate. Thus, CA claimed (at one point) that it collected up to 5000 data points on over 220 million Americans and used more than 100 data variables to model target audience groups and predict the behaviour of like-minded people.[36] Although these claims should be read with scepticism, there is a logic underlying them. The "political influence industry" assumes that there is nothing inherently distinctive about persuading the average American, German, Canadian, Swede, French or British voter with the correct personalised messages, at the correct time, using the correct medium – provided the candidate or party has enough data.[37] For competitive political parties and candidates in many democracies, political micro-targeting is now widely seen as a critical way to gain an edge over opponents.

There is an ongoing debate about the efficacy of political micro-targeting in political and academic circles. Popular writing about these technologies, as well as the corporate hype, typically oversells the impact of these techniques. There is plenty of mythology surrounding data-driven campaigns, and evidence that these techniques are far more effective at mobilising supporters than in persuading voters to change their attitudes and behavior.[38] That said, there is also evidence that targeted ads can appeal to biases and vulnerabilities and have the effect of suppressing turnout among specific voting groups. A Channel Four news report on the use of micro-targeting techniques in the 2016 U.S. election found clear evidence that African-Americans were disproportionately categorised in the Republicans' voter database as amenable to "deterrence." Voter turnout was significantly lower among this group in key midwestern cities compared with that in 2012.[39]

The companies that market these products for digitalised campaigning are overwhelmingly American, and the strategies employed in the U.S. confront some basic constraints in other democracies. Privacy and data protection law in most other democracies does limit the potential for data mining of personal data, and therefore the reach and extent of the personal information economy. Stricter campaign finance laws in most democracies also constrain the purchase of commercial sources of data, and the amount spent nationally and in individual constituencies. The sophisticated voter analytics observed in the U.S. is not easily deployed elsewhere.

In considering the application of Convention 108+ to political campaigning, therefore, it is important to remember some abiding realities about the contemporary electoral environment in

[36] "Cambridge Analytica parent firm SCL Elections fined over data refusal," BBC news, January 10, 2019 at: https://www.bbc.com/news/technology-46822439

[37] 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.

[38] J. Baldwin-Philippi, J. (2017). The myths of Data-Driven Campaigning. *Journal of Political Communication, 34* (4); J. Baldwin-Philippi (2019). Data Analytics: Between empirics and assumptions. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1437

[39] Channel 4 News (2020). Revealed: Trump Campaign strategy to deter millions of Black Americans from voting in 2016, September 28, 2020 at: https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016

different countries, and that the nature and level of voter targeting in different jurisdictions will be determined by a complex interplay of legal, political, and cultural factors.[40]

Aside from international and domestic data protection law, other relevant *legal factors* include:

- Constitutional provisions and case law on freedom of communication, information and association, particularly with respect to public and political affairs
- 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 and regulations
- Election advertising transparency regulations
- Anti-spam rules — the related rules about unsolicited communication by email or text

The overall balance is also going to be profoundly affected by relevant *institutional* features of the political system that shape the nature of political competition, and the role that personal data plays in that competition. For instance, is the electoral system based on proportional representation or "first-past-the-post"? Is voting compulsory, as in Australia and Belgium? Do parties run internal "primary elections" as some did recently in France? What is the frequency of referendums?

The party system is also critical. How many parties are competitive for legislative seats? Are party organisations centralised or decentralised? Do local campaigns have autonomy to decide their own messaging? What are the sources for campaign funds for local candidates and parties?

There are also wider *cultural* variables, associated with historical experience. What is the general acceptability of direct candidate-to-voter campaigning practices, such as door-to-door canvassing, or telephone polling? Do voters trust political elites? Are they generally willing to participate openly in political affairs, and believe that their participation will "make a difference"? Some political cultures, especially those with recent memories of authoritarian rule, are simply not accepting of the level of intrusiveness that is common in North American political campaigns.[41]

In addressing the privacy risks and the application of national and international data protection regulations, therefore, it is important to ground the analysis in actual practices, and to be sensitive to the many other constraints (beyond the law) that will limit the importation of voter analytics and digital campaigning techniques from the U.S. With these assumptions, how might the application of the modernised Convention 108 be usefully applied to the political campaigning environment in countries that have acceded, or might in the future accede, to the Convention?

Political Campaigns, Political Parties and Convention 108+

Political campaigns have been regulated under data protection law for many years in Europe. Political organisations were covered by the original Convention 108, as well as by the 1995 EU Data protection directive. Of course, the entire range of principles and requirements apply.

[40] Bennett and Oduro Marfo, *Privacy, Voter Surveillance and Democratic Engagement*, pp. 53-54.
[41] C.J Bennett (August 2013). "The politics of privacy and the privacy of politics."

However, there are a number that have special significance and require more detailed analysis, in relation to the Convention 108+ and its Explanatory Report, the requirements of the GDPR, and also the findings of certain DPAs from investigations into uses of personal data in the political environment. It also draws upon a recent draft code of practice from the ICO on the application of data protection standards to UK political organizations.[42] The main data protection issues on the use of personal data in the course of political campaigning have also been addressed by the European Data Protection Board (EDPB).[43]

This section of the paper analyses the critical questions under the modernised Convention 108+ which influence the conduct of contemporary political campaigns. It is important to note that political campaigns are not only election campaigns; many societies conduct referendums. Thus, campaigns are not only run by formal political parties; more temporary and informal campaigning organisations (of the kind observed in the 2016 Brexit referendum) capture and process personal data on individual voters. The political campaign can now involve several actors, beyond political parties and candidates (the central data controllers): social media platforms, data brokers, ad networks, analytics companies, polling firms and consultants.

1) The identifiability and re-identifiability of data on political opinions

The main threshold question for the application of data protection law is the definition of personal data. The breadth of that concept has enormous consequences for the processing of data within political campaigns.

Convention 108+ applies to personal data relating to an "identified or identifiable individual." If an individual could be identified only by using "excessively complex, long and costly operations" then the individual may not be considered identifiable. Technological and other considerations will influence what might be considered unreasonable time and effort in different contexts.[44]

As in the GDPR, the individual's identifiability refers not only to his/her name or other legal identifier. The critical variable is the ability to individualise or "single-out." That process can occur through device identifiers, such as IP addresses or pseudonymised identities. Thus, if the individual can be "addressed" as an individual, even if not by name, then those personal data are identifiable. Furthermore, if an individual can be identified through the combination of different sources of data, on for instance, age, sex, geo-location, family status etc. then the data may not be considered anonymous. There is a continuum of identifiability, and organisations should presume that if those data may be used to identify, or re-identify, a data subject then data protection law applies, and the individual has rights over those data.[45]

---

[42] UK, Information Commissioners Office (2019). Guidance on Political Campaigning: Draft Framework code for consultation at: https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf;

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

[44] *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Strasbourg: Council of Europe, 2018), p. 4. (Explanatory Report).

[45] J. Polonetsky, O. Tene, K. Finch (2016). Shades of Grey: Seeing the full spectrum of Practical Data De-Identification 56 Santa Clara Law Review 593.

In principle, the kind of voter analytics pursued in North America should not be possible in Europe, or other countries, on account of the strict prohibition against processing data on political opinions. Companies have, therefore, promoted a variety of products using aggregated and/or anonymised geo-demographic data to profile the political complexion of specific electoral districts. An example in the European context is the company established by Thomas Liegy and his colleagues, now called eXplain. This company has many political clients in Europe and beyond. Among other things it markets a product called Pivot, which "allows us to pinpoint the zones in which constituents are most likely to "swing", and vote for you. Our technology then makes it possible to run impactful and engaging door-to-door campaigning — empirically proven to be the most effective way to win over voters".[46] They apply their analytics to a specialised database of socio-electoral information – structured to "identify those zones most densely populated with voters who might change their voting habits in your favour." These applications were used extensively by the Macron "Grande Marche" campaign in 2016. The software arguably allowed for campaign workers to canvass French voters who may not have been contacted before.[47]

These, and similar, products are pitched as privacy-friendly and data protection compliant. And yet there will always be questions about whether the data being inputted is effectively anonymised according to contemporary standards, as well as whether the subsequent inference about the voter means effectively that personal data are being processed about the political opinions of that voter.

2) The definition of "political opinions" as a form of sensitive data

There is a substantial body of jurisprudence on the importance of free political debate and pluralism under Article 10 of the ECHR. The European Court of Human Rights has repeatedly held that the expression of political opinions has privileged status, as a basis for free expression and free elections.[48] Further, the right to free elections enshrined in Article 3 of the ECHR entails a positive obligation on member states to establish the conditions under which individuals can freely form and express their opinions and choose their representatives without discrimination. Article 14 prohibits discrimination on grounds of "political or other opinions", although the Court has rarely considered cases of discrimination on these grounds.[49] Political opinions have also been defined as a sensitive category of data in both the original Convention 108 of 1981,[50] and in the 1995 EU Data Protection Directive.[51]

Similarly, under Convention 108+, "personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of the Convention." It goes on: "Such safeguards shall guard against the

[46] https://explain-technology.com/our-products/pivot/
[47] J. Duportail, (2018). The 2017 Presidential Election: The arrival of targeted political speech in French Politics. Tactical tech. At: https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-france.pdf
[48] Venice Commission, Digital Technologies and Elections, p. 13.
[49] European Court of Human Rights, Guide on Article 14 of the European Convention of Human Rights and on Article 1 of Protocol No. 12 to the Convention (August 31, 2020), p. 30 at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf
[50] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 1981, Article 6 at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37
[51] EU Data Protection Directive, Article 8.

risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination."[52] The accompanying explanatory report highlights the dangers of discrimination from the inappropriate processing of sensitive personal data. But there is no further guidance on the meaning of "political opinions" nor any further mention of exemptions for the processing of personal data for electoral activities, as appears in the GDPR.

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."[53] These principles 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. The processing of such data may entail special risks of "varying likelihood and severity" to the rights and freedoms of individuals.[54]

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) also permits processing which "relates to personal data which are manifestly made public by the data subject." With respect to political parties, Recital 56 of the GDPR states: "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."[55] None of these provisions is substantially different from those in the 1995 Data Protection Directive.

We have been seeing member states take advantage of these provisions to allow for a greater leeway in the processing of personal data by political parties and candidates. In the UK's Data Protection Act, for example, the processing of political opinion data is permitted by a registered political party, "in the course of its legitimate political activities" provided that it does not cause "substantial damage or substantial distress to any individual" – a relatively high standard and one that presumably needs to be proven by the individual. And Schedule 1, para 22, provides a special public interest condition for the processing of sensitive data on political opinions by political parties engaged in "political activities."[56] There are similar expansive provisions introduced in other countries, which have motivated complaints by civil society organisations.[57] In Spain, for instance, the Constitutional Court has struck down the public interest exception in

[52] Convention 108+, Article 6
[53] EU General Data Protection Regulation, Article 9 (1)
[54] EU General Data Protection Regulation, Recital 75.
[55] EU *General Data Protection Regulation*, Recital 56
[56] UK, Data Protection Act (2018) c.12. Schedule 1 (para 22) at: http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted
[57] Privacy International April 30th, 2019. "GDPR loopholes facilitate data exploitation by political parties" at: https://privacyinternational.org/news-analysis/2836/gdpr-loopholes-facilitate-data-exploitation-political-parties

the Spanish data protection law implementing the GDPR, which would have allowed political parties to capture data on political opinions without consent and to profile voters.[58]

Neither has there been any significant analysis of the meaning of "political opinions" as a category of sensitive data under data protection law. The term is not self-defining, although there are helpful examples provided in the ICO guidance on political campaigning.[59] In prior work, I have raised a number of questions concerning the breadth of the definition of "political opinions." There is also vagueness surrounding the meaning of "in the course of electoral activities," and the definition of the "reasons of public interest."[60]

The concept of political opinions could be interpreted on a number of different levels. First, it could mean a *political ideology* or creed – liberal, conservative, socialist, communist and so on. Interestingly, this is the meaning that is expressed in the now "adequate" Japanese data protection law. "Political opinions" are not explicitly defined as such. Instead, the law (Art. 2(3)) 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."[61]

Another interpretation would be political *affiliation*, or perhaps partisan affiliation. That might refer to actual party membership, lists of which parties can legally process. It might also refer to financial donors, which parties in many countries have to record and report as a result of campaign financing transparency rules. It might also refer to a broader notion of *partisan identification*, perhaps inferred from membership information, but also from the profiling conducted through voter relationship management systems. Many political parties will know their consistent supporters and campaign to get them to go to the polls. A tradition of analysis within political science studies how partisanship is correlated with different socio-demographic variables over time and space: gender, class, race, location and so on. Patterns vary, but those factors give very important cues to political behavior, and indeed political "opinions."

Then, of course, there are opinions about *policy* – economic, social, environmental, labour, immigration, rights of minorities and so on. These opinions will also be correlated with ideology and partisan affiliation. They may also, of course, be sensitive, especially in countries with current, or recent tendencies to authoritarianism who wish to isolate and persecute those with anti-government views. Thus, a political opinion about gay rights, for instance, in a country with homophobic laws, is no doubt highly sensitive as a possible revelation of sexual preferences and might lead to the kind of discrimination about which Convention 108+ warns.

The Convention and the GDPR are also, of course, explicit that the sensitive data is that which *reveals* political opinions,[62] and political opinions can be inferred from a whole range of other activities (e.g. magazines or newspapers reads), conditions (such as neighborhood or postal code) or policy beliefs and preferences.

---

[58] "Spanish Constitutional Court strikes down political profiling," *GDPR Today*, Vol. 4. No 11 (June 2019) at: https://www.gdprtoday.org/spanish-constitutional-court-strikes-down-political-profiling/

[59] ICO, Guidance on Political Campaigning, pp. 43-44.

[60] C.J. Bennett (April 2018). Cambridge Analytica and Facebook: A Wake-Up Call. *Privacy Laws and Business International Report,* Issue 152. C. J. Bennett, "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 (December 2016), pp. 261-275.

[61] Interviews, Japan Personal Information Commission, May 7, 2018.

[62] EU General Data Protection Regulation, Article 9(1)

These issues about the collection of personal data for political campaigning were investigated by the ICO in the UK context in their 2018 report, *Democracy Disrupted*. 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."[63] 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.

Furthermore, some political parties, it was reported, use software which assigns a predicted ethnicity and age to the names of individuals, under the contention that this "assumed" or "inferred" data is not necessarily personal information about the data subject. The ICO disagreed. Once those data are linked to an individual it does amount to personal data and is subject to the requirements on the processing of special categories of data. There is 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.[64] This interpretation is consistent with earlier guidance from the Article 29 Working Party on Automated Individual Decision-Making and Profiling which noted that "profiling can create special category data from inference from data which is not special category data in its own right but becomes so when combined with other data."[65]

Thus, "political opinions" may be a very broad category: ideology, affiliation, identification or policy beliefs. Those "opinions" might be derived or inferred from a wide range of activities or conditions. The breadth of the definition of political opinions has enormous consequences for the rules governing the capture of personal data within political campaigns.

3) Rules on consented political communications

Issues about inappropriate political communications raise questions about the application of rules for opting-in and opting-out of tele-communications across a variety of traditional, and more contemporary, media and platforms. These issues have taxed the DPAs in the past and will continue to do so as the means of delivering political ads to more precise segments of the electorate gets more sophisticated. Most DPAs in Europe, have received complaints about unsolicited communications by political parties. Some of these complaints stem from solicitations from parties that the data subject would never support, triggering irate questions about how that party got their contact details. In this respect, political communication sometimes carries sensitivities not encountered in the commercial world.[66]

At root lies the question of whether the communication of political content should be treated in a fundamentally different way to the delivery of commercial messages. Historically, rules about "direct-marketing" or "tele-marketing" have tended to make no distinction. The Explanatory Memorandum accompanying Recommendation No. R (95) 4 on the "protection of personal data

[63] ICO, *Democracy Disrupted*, p. 15.
[64] ICO, *Democracy Disrupted*, p. 31.
[65] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, February 6, 2018, p. 15 at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
[66] Bennett, Voter databases, micro-targeting and data protection law, p. 270.

in the area of telecommunication services" is explicit that the original Convention 108 applied not only to commercial marketing, but also to political marketing.[67] The recommendation has its origins in an earlier 1985 Recommendation on the *Protection of Personal Data Used for the Purposes of Direct Marketing*, which posited a very broad definition of direct marketing and drew no distinction between commercial or political messaging.[68]

In terms of Convention 108+, the right to control intrusive communications from political parties or candidates is rooted in: Article 5 on the legitimacy of processing and quality of data; Article 8 on transparency; and Article 9 on the rights of data subjects, and particularly on the right to object to processing. Critical in this area is the appropriate balance between data protection rights and interests and the rights to freedom of expression stated in Article 11(b).

Some European DPAs have issued guidance on inappropriate political marketing, under both the 1995 Data Protection Directive and the 2002 E-Privacy Directive.[69] Examples include a series of guidance from both ICO[70] and the CNIL.[71] The CNIL also issued regulations on spamming in response to the so-called 'Sarkospam' scandal occurred in September 2005, when hundreds of thousands of unsolicited e-mails were sent on behalf of presidential candidate Nicolas Sarkozy. The case prompted a series of recommendations from the CNIL about the use of files by political parties, groups, candidates and elected officials.[72]

Domestic rules generally stipulate that a political campaign will need the individual's consent before sending marketing emails or texts, or making automated marketing calls. The caller is required to state explicitly the party that he/she represents, display clearly the number, and record and respect any request by the individual not to be called again. If the party is relying on marketing lists, they must keep records to demonstrate what the individual has consented to, and how they consented. Where there is a "do-not-call" list, the campaigner must screen its list against these names.[73]

Political campaigns are also affected by the rules concerning the receipt of "cookies." Article 5(3) of the E-Privacy Directive requires prior informed consent for storage or access to information stored on a user's terminal equipment. Data controllers must ask users if they agree to most cookies and similar technologies before the site starts to use them. For consent to be valid, it must be informed, specific, freely given and must constitute a real indication of the individual's

[67] Council of Europe, 1995. Explanatory Memorandum Recommendation No.R (95) 4 of the Committee of Ministers to Member States on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, para 85. at: https://rm.coe.int/16806846cc

[68] Council of Europe, 1985. Recommendation No. R (85) 20 On the Protection of Personal Data Used for the Purposes of Direct Marketing. Strasbourg: Council of Europe, October 1985. at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804bd336

[69] Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector ("E-Privacy Directive"), (OJEU L 201) at: http://ec.europa.eu/justice/dataprotection/law/files/recast_20091219_en.pdf

[70] U.K. Information Commissioner's Office (ICO) (2018). *Guidance on Political Campaigning* at: https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf

[71] France, CNIL. Communication Politique: Obligations Legale et Bonnes Pratiques édicion Janvier 2012, Les guides de la CNIL at: http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Politique.pdf

[72] Délibération n. 2006-228 du 5 octobre 2006 portant recommandation relative à la mise en œuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000459927

[73] ICO, *Guidance on Political Campaigning.*

wishes. There is nothing in the Directive to suggest that this provision does not apply to political party websites. Indeed, some political parties have been found to run afoul of these rules.[74]

Under the GDPR, processing is permitted for members, former members or those who have "regular contact." The general presumption, as expressed in the guidance from the CNIL for example, is that if the individual has taken positive action to initiate a membership, to donate or to connect on a regular basis, then implied consent for further communication is given. Beyond those narrow categories, then express consent must be obtained. However, there will be ongoing dispute over the meaning of "regular contacts" in the context of different social media environments. It is quite obvious that the rules have to be more nuanced to reflect the different media through which political campaigning now occurs.

4) Questions of proportionality in the light of the legitimate purposes

Convention 108+ stipulates that "data processing shall be proportionate in relation to the legitimate purpose and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake." [75] Data processing shall either be carried out on the basis of "free, specific, informed and unambiguous consent of the data subject" or of some other legitimate basis laid down by law. Examples of such legitimate interests are offered in the accompanying explanatory report, and there is no mention of data processing by political campaigns or organisations. Further, the data controller "is not permitted to process data for undefined, imprecise or vague purposes."[76]

That said, the Convention does specify "freedom of expression" as a legitimate interest that needs to be balanced against the rights of the data subject. The explanatory report mentions "journalistic, academic, artistic or literary expression" in this context. There is no mention of political expression. What therefore are the "legitimate purposes" of a political campaign, and how should they be defined and delimited?

There can be no argument that political parties and candidates need to communicate effectively with the electorate. They need to introduce policy positions and candidates. They need to understand voters' needs and beliefs. They need to encourage engagement with the democratic process and mobilise their supporters on election day. The more interesting 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, and thus to allow them to exercise their democratic rights?

On this question, cultural traditions shape campaigning practices as much as legal provisions. In some societies, such as the U.S, there is a general presumption in favor of open communication between individual voters and political actors. In others, Japan being a prime example, individualized campaigning as well as micro-targeting, is not only frowned upon but highly illegal, and associated with historic problems of political corruption. In some societies, door-to-door canvassing is common, even expected. In others, and particularly those with recent memories of authoritarian rule, the prospect of a politician knocking on one's front door could be greeted with

[74] Bennett, Voter databases, micro-targeting and data protection law, p. 270.
[75] Convention 108+ Article 5.
[76] Explanatory Report, p. 8.

fear and suspicion. The "legitimate interests" of political campaigns, therefore, will vary enormously dependent on the reasonable expectations of the electorate and the historical and political contexts.[77] The ICO has already addressed the various activities that do, and do not, promote democratic engagement and can therefore be used as a "legitimate interest" under UK law.[78]

Under the vast majority of conditions for direct party or candidate contact with the voter, the provision of "freely given, specific, informed and unambiguous" consent should be possible, whether the personal data is being captured on the doorstep, on the phone or online. There is a "specific context" to election campaigning which should be clearly delineated from other commercial or governmental purposes and situations.[79] Whether or not there is a "legitimate basis for the processing laid down by law" will also vary from society to society. The fact that complete voters' lists are shared in some countries legally with parties and candidates at the beginning of each election cycle legitimates the process of communicating with voters and serves as public interest grounds for democratic engagement. Practices differ on how those lists are transferred, whether they are done so digitally and for how long they may be retained.

What is less clear, however, is the processing of further data on the electorate within voter relationship management databases. The only European example is the UK, but other illustrations exist in Canada, Australia and, of course, in the U.S. In these societies, the parties take the general voters list, or electoral register, and populate those basic household data with information from a variety of other sources – doorstep canvassing, telephone polling, petitions, third party data sources, census information and so on.[80]

DPAs have, from time to time, ruled against parties or candidates using lists from related organisations (churches, clubs, associations etc.) for purposes of political communication.[81] There are also issues when elected members of the legislature who have access to personal data in that capacity, use that information, deliberately or unwittingly, for electoral advantage. In parliamentary systems, there is supposed to be a "firewall" between the personal data captured as a result of constituency or legislative responsibilities, and that used for political campaigning. But often that distinction is eroded. The distinction between official, institutional communication, and electoral campaigning is not always clear.[82]

And then there may be lists purchased from *data brokers*. In August 2018, the ICO fined Emma's Diary for selling data on new mothers to the Labour Party. This company, which provides advice on pregnancy and childcare, sold the information to Experian Marketing Services, a branch of the credit reference agency, specifically for use by the Labour Party. Experian then created a database which the party used to profile new mothers and market those living in areas of marginal seats about its policies on children care during the 2017 General Election.[83]

---

[77] Bennett and Oduro Marfo, *Privacy, Voter Surveillance and Democratic Engagement*, pp. ii.
[78] ICO, Guidance on Political Campaigning, p. 39.
[79] Explanatory Report, p. 7.
[80] Bennett and Oduro Marfo, *Privacy, Voter Surveillance and Democratic Engagement*, pp. 21-27
[81] Bennett, "Voter databases, micro-targeting and data protection law", p. 267
[82] Ibid.
[83] ICO News Release (09 August, 2018). "Emma's Diary fined 140,000 pounds for selling personal information for political campaigning" at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/

5) The processing of personal data that has been made "public"

Nothing in Convention 108+ excuses controllers of data protection responsibilities just because those data are allegedly "out there." It is silent on any distinction between "publicly available" and other forms of personal data. The European Data Protection Board (EPDB) has also insisted that "personal data '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. Thus, data collected through social media for the purposes of voter contact cannot be undertaken without complying with the obligations concerning transparency, purpose specification and lawfulness.[84]

The CNIL has issued several rulings on the uses of social media data by political campaigns and has distinguished between regular and occasional contacts. The former are those contacts who "engage with a political party in a positive way in order to maintain regular exchanges in relation to the party's political action." In social media terminology, this translates to following someone on Twitter, becoming friends with someone on Facebook, or, more generally speaking, demonstrating a willingness to maintain regular contact with the political party or candidate. On the other hand, an "occasional contact" refers to those who "occasionally solicit a political party or a candidate, without holding regular exchanges with them in the course of their political activity," for instance, liking or sharing on Facebook, or retweeting. Occasional contacts may be contacted once to offer them the possibility of opting in to communications. In the event of a positive response, the persons contacted become regular contacts. But in the event of a negative response, or lack of response, their data cannot be legally processed and must be deleted.[85]

Similar rules apply to the processing of data from social media platforms to match contact information such as email addresses to customise voter outreach. The "scraping" of personal data from social media sites is generally not legal under European data protection law without explicit consent. Under those standards, such individuals would not be classified as "regular contacts." A program run by the popular company, Nationbuilder ("Nationbuilder Match") was ruled illegal by the CNIL. The company has discontinued the service globally.[86]

Similar standards have been applied to political parties in Canada. Political parties would not have consent to add to their database any personal information collected through social media merely because the individual has interacted with the party by "liking" a post or a tweet.[87] The UK ICO has noted that data protection law does not stop political parties from obtaining and using personal data from publicly available sources. However, they must still comply with data protection law, and provide appropriate notice to voters: "The ICO is concerned about political parties using this functionality without adequate information being provided to the people affected. The parties must

[84] European Data Protection Board, Statement 2/2019 on the use of personal data in the course of political campaigns. March 13, 2019 at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf
[85] Commission Nationale de l'Informatique et des Libertés, "Elections 2016 / 2017 : quelles règles doivent respecter les candidats et partis?" At: https://www.cnil.fr/fr/elections-2016-2017-quelles-regles-doivent-respecter-les-candidats-et-partis; Commission Nationale de l'Informatique et des Libertés, "Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?" (November 8, 2016). at: https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.
[86] Nationalbuilder Match désactivée en France (March 31, 2017) at: https://nationbuilder.com/nbmatch_france
[87] OIPCBC*, Full Disclosure*, p. 21

therefore include deployment of these platforms as part of future data protection impact assessments."[88]

6) Transparency

Even where the processing is lawful, organisations need to be transparent about the legal basis for processing, the categories of data processed, the recipients of those data, and the means of exercising data protection rights.[89] Certain essential information about the processing should be provided in a proactive manner. This should include identity of the controller, the legal basis for processing, the categories of data processed and the means of exercising rights. Information may also include the preservation period, the reasoning underlying the data processing, and information on data transfers.[90]

It is presumed that the political party (or in the case of a referendum, the campaign) are the data controllers and assume all these obligations. There are many different contexts, however, through which parties and campaigns might communicate with voters: on the doorstep; over the phone; through their websites; on social media; in public meetings; and others. Often, the collection of data will occur within the frenzy of a short election campaign, when pressures to knock on doors, phone so many numbers, sign up workers and volunteers, and collect donations, are extensive. Initial investigations have found that political parties often circumvent these requirements in the context of highly competitive campaigns.

Many of the findings in the 2018 ICO report, for instance, relate to 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. Parties also need to apply due diligence when sourcing information from third party organisations to ensure that appropriate consent has been obtained and the transparency requirements of the GDPR are adhered to.[91] In the aftermath of the Cambridge Analytica/Facebook scandal, there is a pressing need to enhance trust in the democratic process. The adherence to the transparency standards in data protection law is a crucial way to build that trust.

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.[92]

7) Rules on automated decision-making and voter profiling

Convention 108+ states that every individual has the right "not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having

[88] UK, ICO, *Democracy Disrupted*, p. 32.
[89] Convention 108+ Article 8.
[90] Explanatory Report, p. 12.
[91] ICO, Democracy Disrupted, p. 6.
[92] Bennett and Oduro Marfo, p. 57.

his or her views taken into consideration." [93] According to the Explanatory Report, the "data subject should have the opportunity to substantiate the possible inaccuracy of the personal data before it is used, the irrelevance of the profile to be applied to his or her particular situation, or other factors that might have an impact on the result of the automated decision."[94]

Automated decision-making through deep machine learning, artificial intelligence[95] and secret algorithmic processing can stigmatise and discriminate. The Convention requires that this should not occur without the individual having his/her rights taken into consideration. Article 22 (1) of the GDPR is arguably worded more strongly: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Typical areas of discrimination mentioned in this context are the receipt of credit, or social benefits.

It is almost impossible to separate issues of automated processing from those of automated profiling, defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location of movements." According to a recent report on profiling and Convention 108+, profiling can be "high-risk" when it has a significant impact on the person or group of persons, when it involves a risk of manipulation, when it involves special categories of data, or when it is performed by largely online information services.[96] In the electoral context, there are concerns that voter profiling can have a "chilling effect" on freedom of speech and participation. It is widely recognised that the feelings of being under surveillance can impair the exercise of fundamental freedoms, including participation in elections.[97] The EDPB has already ruled that: "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 circumstances cause 'similarly significant effects' and shall in principle only be lawful with the valid explicit consent of the data subject." [98]

That said, voter profiling can take many different forms, and is often invisible to individuals.[99] Most simply, many political parties have adopted some very basic personalised scoring systems to predict a voter's likely support or opposition.[100] These ranking systems allow parties to focus their efforts on the voters who are most likely to support them, and to improve a party's ability to recruit new volunteers and donors. Attempts to render these scoring systems transparent have been

---

[93] Convention 108+, Article 9.1

[94] Explanatory Report, p. 13.

[95] *Guidelines on Artificial Intelligence and Data Protection*, adopted by the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal data on 25 January 2019. at https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

[96] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal data. *Profiling and Convention 108+: Suggestions for an update*. Strasbourg: November 7, 2019.

[97] Joint Report of Venice Commission, June 2019, p. 20.

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

[99] ICO, Guidance on Political Campaigning, p. 65.

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

resisted in some countries, on the grounds that the revelation of proprietary scoring and profiling systems would damage the competitive position of the party concerned.[101]

More sophisticated voter profiling occurs through the generation of look-alike audience generation on Facebook. The 2017-18 ICO investigation into UK political parties generally 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. According to investigations in Canada, the disclosure of supporter email addresses for data analysis and profiling to reach similar audiences through Facebook's "Lookalike" tool is entirely different from the political parties' stated or inferred reason for collecting the email address in the first place.[102]

According to a recent report on profiling and Convention 108+, the enforcement of principles on the fair and proportionate processing is difficult given that profiling relies on categories of data that are difficult to predict in advance of processing. The report suggests that profiling should be limited to those categories that the data subject can reasonably be expected to consider in view of the legitimate purposes.[103] Profiling must contribute "both to the well-being of individuals and to the development of an inclusive, democratic and sustainable society." Profiling must not result in discrimination against individuals, groups or communities. It must "neither undermine the dignity of persons, nor democracy."[104]

Conclusions

The illegal and/or unethical processing of personal data in political campaigns raises profound questions about democratic practice, the quality of democratic debate, the openness of democratic competition and the nature of political participation. Practices vary widely, and they are developing rapidly and organically, as different political actors and organisations assess the advantages of digital campaigning given their resources, legal frameworks, institutional environment and political culture.

Given this complexity and dynamism, how can Convention 108+ contribute to the resolution of these broader questions of democratic engagement? How can Convention 108+ be applied to political campaigns and campaigning organisations without jeopardizing the rights of political actors to communicate with the electorate, and mobilise them to vote?

This analysis points to the following broad conclusions:

- Convention 108+ was explicitly conceived as a global instrument. It is framed in terms of general principles and designed to be applied in different parts of the world, and various political systems. It was conceived with recognition of its potential global impact, as a treaty-based process rather than a market-powered process.[105] It is the only realistic prospect for a global data protection agreement.[106]

[101] This argument was rejected by the OIPCBC, *Full Disclosure*, p. 37.
[102] Ibid, p. 26
[103] *Profiling and Convention 108*, 7 November 2019, p. 4.
[104] Ibid, p. 3.
[105] L. Bygrave. 2020. "The Strasbourg Effect in Data Protection: Its Logic, Mechanics and Prospects in Light of the 'Brussels Effect'. At: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3617871
[106] G. Greenleaf. 2018. Convention 108+ and the Data Protection Framework of the EU. at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3202606

- Convention 108+ is explicitly framed in human rights and democratic, rather than commercial, terms. Its roots in human rights and democracy make it a more suitable international instrument for the harmonization of practices in the electoral arena.

- The Council of Europe has played an historical role in the advancement of democratic practices and rights, through the Venice Commission and other bodies. Questions about electoral manipulation, propaganda and misinformation are inseparable from issues of data protection. The Council of Europe is perfectly suited to understand these relationships, and how legal and ethical personal data processing can improve the integrity of the democracy, and the functioning of democratic institutions.

- The Council of Europe has an impressive track record of identifying technological challenges and developing clearly framed regulatory solutions. In an era when digital campaigning practices are advancing rapidly and globally, it is ideally suited to addressing these problems. The modernisation of Convention 108 was intended to address new challenges raised by new technologies and its principles are particularly appropriate to face the online manipulation and misuse of data in the campaign arena. The issues addressed in this paper also relate closely to former recommendations on digital and social media.

- The Council of Europe also has a breadth of experience across related regulatory and policy sectors. A diverse array of constitutional, statutory and self-regulatory rules can affect the processing of personal data in election campaigns. The Council of Europe has a long tradition of providing the guidance and coordination for different national regulators in different sectors. Convention 108+ stands as a valuable set of principle-based standards for the understanding and integration of various rules across countries.

- Beyond DPAs, elections and telecommunications regulators have statutory responsibilities over election financing, advertising and administration in many countries. Convention 108+ can serve as a valuable framework for the coordination of the work of different regulatory bodies, domestically and internationally.

- The "legitimate interests" of political campaigns and organisations are different from those of government agencies and corporations. The public interests in democratic engagement require careful reconciliation with rights to voter privacy. The Council of Europe is uniquely suited to addressing the privacy implications of data-driven elections in this broader context, and to understanding the relationship between privacy protection and the promotion of democratic practices.

- "Political opinions" are defined as sensitive forms of data in Convention 108+. This classification is motivated by historical concerns about voter suppression and manipulation. Any guidance or recommendations about privacy and election campaigns need to be sensitive to different candidate-to-voter campaigning practices. In countries with recent memories of authoritarian rule, the sensitivity of data on political affiliation is particularly acute. The Council of Europe has a valuable experience in promoting democratic practice in established, as well as newer and more fragile, democratic states.

- Contemporary political campaigning is complex, opaque and involves a shifting ecosystem of actors and organisations, which can vary considerably from society to society. The political "influence industry" operates across cultures with very little to no sensitivity for

campaigning traditions, institutional realities or political practices. A baseline standard, provided by Convention 108+, for the processing of personal data within different democratic elections can serve as an important guide to best practices for the variety of data controllers and data processors within the global campaigning networks. It can also serve as a possible basis for codes of practice, of the sort currently being developed in the UK.

- These are clearly global questions requiring the highest level of international collaboration between DPAs, in Europe and beyond. 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. Convention 108+ provides a valuable principles-based instrument upon which to base that coordination.