PRIVACY, ELECTIONS AND POLITICAL PARTIES: EMERGING ISSUES FOR DATA PROTECTION AUTHORITIES

Colin J. Bennett, Department of Political Science, University of Victoria, BC. Canada

www.colinbennett.ca

The 2012 presidential election in the United States has raised to public attention the general question of how political parties and candidates process and analyze personal data on individual voters. An incomplete summary of these techniques incudes: extensive "voter management" databases; widespread use of personal data purchased from data brokerage firms; extensive use of robo-calling and robo-texting; smart-phone apps that allow door-to-door canvassers instant access to voter histories; extensive uses of social media that allows for peer pressure or "targeted sharing"; and integrated campaign "toolkits" for website development, social media strategies, and political messaging.[1] These techniques permitted the "micro-targeting" of online and offline messages to more precisely defined categories of voters, especially in marginal states and districts.[2]

The range and sophistication of techniques in the US are staggering, and obviously facilitated by the absence of any general data protection law that applies to such data, as well as to a First Amendment that provides robust protections for freedom of communication and association. And of course, these techniques are facilitated by a permissive campaign financing system that generally places no restrictions on how much money individual candidates may spend on their election campaigns, or how much they may raise from individuals, groups or corporations.

We might find micro-targeting practices a little "creepy" – but the arguments on the other side of the debate are important and worthy of serious consideration. After all, political parties do have a democratic responsibility to educate voters about their positions and policies, and to mobilize voters. In an era of declining voter turnout, and membership in political parties in most Western democracies, perhaps micro-targeting should be embraced as a more effective and efficient way for parties to target their messages to those who are interested in hearing them. These issues raise a set of fascinating questions about the appropriate balance between privacy and the values of democratic education and participation.[3]

To what extent are the "micro-targeting" techniques entering the election campaigns of other democratic countries? And what are the implications for privacy laws and for the data protection authorities (DPAs)? Very little has been written about these issues in the privacy literature. And with few exceptions, DPAs have been reluctant to provide

---

[1] The best contemporary overview of these practices is: Sasha Issenberg, *The Victory Lab: The Secret Science of Winning Campaigns* (Crown Publishing, 2012).

[2] Charles DuHigg, "Campaigns Mine Personal Lives to Get out the Vote," *New York Times*, October 13, 2012.

[3] Colin J. Bennett, "What Political Parties Know about You," *Policy Options (February 2013) at: http://www.irpp.org/po/archive/feb13/bennett.pdf?utm_source=Thinking+Ahead+February&utm_campaign=Thinking+Ahead+July+EN&utm_medium=email*

guidance to parties and candidates, and less still to regulate their activities. Furthermore, there are huge differences in electoral laws, financing provisions, voting systems and political cultures between the United States and parliamentary systems.

On the other hand, there is evidence that parties in other countries are drawing lessons from the American experience, and that similar techniques are gradually entering the politics of other countries. Back in 2005, the DPAs were sufficiently concerned about the use of new technologies to "establish direct and personalized contacts with vast categories of data subjects," about "invasive profiling" and about the unlawful collection of "sensitive data related to real or supposed moral and political convictions and activities" to issue a joint Resolution at their international conference in Montreux.[4] So how have voter surveillance issues arisen in countries outside the U.S.

I begin with Canada. Neither the Canadian Privacy Act of 1982, nor the Protection of Personal Information and Electronic Documents Act (PIPEDA) of 2000 cover political parties because they are neither government agencies nor commercial entities; like some other non-profit entities, they fall between the cracks of the Canadian privacy regime. Nevertheless, the Canadian Privacy Commissioner has received a number of complaints about invasion of privacy by candidates and politicians going back several years. Partly in response, the office commissioned me to conduct a study on the subject, which concluded that the federal parties process an increasing amount of data on supporters, non-supporters, volunteers, candidates and employees.[5]

The issue has also achieved a prominence in the media as a result of a scandal involving the practice of "robo-calling" at the 2011 federal election. Voters in key marginal constituencies received automatic calls from an individual purporting to represent Elections Canada, and informing them (falsely) that their place of voting had changed. The "robo-call" scandal hit the front pages, and prompted investigations from the Royal Canadian Mounted Police and from Elections Canada.[6] The most interesting aspect of this affair is that only non-Conservative supporters were targeted, meaning that the individual must have had access to the voter management database operated by the Conservatives – the Conservative Information Management System (CIMs). The Chief Electoral Officer recommended that it was about time for the basic privacy principles within PIPEDA to be applied to political parties.[7]

Like Canada, the privacy laws of Australia also leave political parties unregulated. And like Canada, 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. In 2008, the Australian Law Reform

---

[4] International Conference of Data Protection and Privacy Commissioners, *Resolution on the Use of Personal Data for Political Communication*, Montreux, Switzerland, 16th September 2005.

[5] Colin J. Bennett and Robin M. Bayley, *Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis* (Report to the Office of the Privacy Commissioner of Canada, March 2012) at: http://www.priv.gc.ca/information/research-recherche/2012/pp_201203_e.asp

[6] Elections Canada, *Preventing Deceptive Communications with Electors* Chief Electoral Officer of Canada, 2013 at: http://www.elections.ca/res/rep/off/comm/comm_e.pdf

[7] Ibid, p. 32

Commission (ALRC) 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."[8] To date, no such guidance has been issued.

So, what of the application of privacy law in Europe to political parties? Under the 1995 European Data Protection Directive, and under the new Draft Regulation, political parties are clearly covered by data protection rules. There are a number of relevant provisions. I will cite the new wording in the new Draft Regulation, as the rules are essentially the same.[9]

First data on political opinions is unequivocally defined as a "sensitive" form of personal data, which is generally prohibited unless: "processing is 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 data are not disclosed outside that body without the consent of the data subjects" (Article 9(d)). Recital 36 reinforces this exemption in the case of political parties: "Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established."

A plain reading of the law would indicate, therefore, that parties may only process political data on members, former members of on persons "who have regular contact." But what does this mean? Someone who attends meetings? Some who has friended the party on Facebook? And what of political communication that might be in the public domain – signs in windows, letters in newspapers, blog postings and so on? We convey explicitly and implicitly our political affiliations and preferences in an increasing number of contexts, and in a range of manners.

Does European law outlaw the kind of "voter management databases" common in North America? It is reported that the main political parties in the UK have operated such

---

[8] Australia Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, para. 41 at: http://www.austlii.edu.au/au/other/alrc/publications/reports/108/41.html#Heading25

[9] European Union (EU). Proposal for a Regulation of the European Union and the Council on the *Protection of Individuals with respect to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Published January 25, 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

databases for several years, using similar proprietary software to their counterparts in the United States, and essentially augmenting the basic address information from the electoral roll with additional personal data on voters.[10] The Conservative Party has used the "Voter Vault" software now uses MERLIN (Managing Elector Relations through Local Information Networks).[11] The Labour Party now operates a system called Contact Creator.[12]

The Information Commissioner's Office has not ruled on the legality of such databases, but it did issue some guidance on the general question of political communication in 2005, as a result of a series of complaints about inappropriate telemarketing and particularly by individuals who objected to receiving calls from canvassers from parties they would never support.[13]

The French Commission Nationale de L'Informatique et Libertés (CNIL) provided similar guidance on political campaigning in 2012.[14] The CNIL also issued a more general set of decisions on the application of the data protection law to the range of party activities, including the construction of databases. Of particular interest in France was the recent innovation of a primary election for the presidential candidates for the French socialist party. "Open" primary elections pose particular problems for the application of data protection law to political parties. Voters from the general public may participate in the "internal" affairs of the party by selecting its candidate for the general election. Are such voters "regular contacts"? The CNIL struggled with this question and tried to balance the data protection law with the legitimate rights of association that parties claim.[15] Similar issues arose for the Italian Garante after primary elections for the center left coalition, Common Good, in 2012.[16]

Isolated examples of the inappropriate capture, use and disclosure of personal data by political parties and their candidates surface from time to time in other European countries. An initial survey suggests the following questions have required resolution:

- Questions of intrusion – inappropriate communication by phone, e-mail, or text to people who have not given their consent, and who may be listed in respective "do-not-call" lists

---

[10] Amberhawk Training Ltd. "Could the Conservative Party's Electoral Database breach the Data Protection Act?" at: http://amberhawk.typepad.com/amberhawk/2013/03/could-the-conservative-partys-electoral-database-breach-the-data-protection-act.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HawkTalk+%28Hawk+Talk%29

[11] James Crabtree, "David Cameron's Battle to Connect" Wired Magazine, March 24, 2010 at: http://www.wired.co.uk/magazine/archive/2010/04/features/david-camerons-battle-to-connect

[12] http://www.cfl.labour.co.uk/images/uploads/166988/9b6fc688-c195-be24-2db3-b7f130f35c08.pdf

[13] UK Information Commissioners Office, *Guidance for political parties for campaigning or promotional purposes* (UK: ICO, 2005)

[14] Commission Nationale de l'Informatique et Libertes (CNIL), *Communication Politique: Obligations Legale et Bonnes Pratiques (Paris: CNIL, January 2012)*

[15] Commission Nationale de l"Informatique et Libertes (CNIL), *Deliberation no. 2012-020 du Janvier 2012 portant recommendation relative à la mise en oeuvre par les partis ou groupements à caractère politique, eélus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques.*

[16] Garante per la protezione dei dati personali, *Elezioni primarie 2012 e trattamento di dati personali* – 31 October 2012.

- The non-consensual capture of personal data by elected officials who come into contact with constituents in their capacities as electoral officials and communicate data on electors to their party headquarters
- The logging of support or non-support by canvassers who may communicate data on political preferences in the course of election campaigning at the door, or over the telephone
- The capture of data on political preferences through Facebook, Twitter and other social networking services
- The capture of personal data through the inappropriate logging of cookies when the party website is visited.[17]
- The use of membership lists for other organizations (churches, unions, clubs, schools etc.) used by candidates for political canvassing
- Data breaches, especially when address information from the respective electoral roll is shared with party organizations at election time

I predict that these, and other privacy issues, will become more prominent in the years ahead. The pressures for political parties to find more efficient methods to reach voters with their messages will increase as a result of social networking and other technologies, the influence of political consultants, the break down of traditional bases of support and the inherent competitiveness between parties within any political system. This brief survey suggests that the lessons from the United States have not been lost on their counterparts in many European countries, despite obvious and fundamental differences in data protection law, election rules, and political cultures.

[17] This became an issue in the Netherlands when some parties were found to be in breach of the Dutch law on cookies.