
Faculty of Social Sciences

Faculty Publications

The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies

Colin J. Bennett

August 2013

© 2013 First Monday & Colin Bennett. This paper is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](#).

This article was originally published at:
<https://doi.org/10.5210/fm.v18i8.4789>

Citation for this paper:

Bennett, C.J. (2013). The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies. *First Monday*, 18 (8).
<https://doi.org/10.5210/fm.v18i8.4789>



The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies by Colin Bennett

Abstract

This paper surveys the various voter surveillance practices currently observed in the United States, assesses the extent to which they have been adopted in other democratic countries, and discusses the broad implications for privacy and democracy. Five interrelated techniques are analyzed: the development of voter management databases; the use of personal data from commercial data brokerage firms; micro-targeting; the decentralization of data to local campaigns; and “targeted sharing” through social media. Structural and cultural differences between the United States and other democratic countries prevent the extensive and direct export of many of these practices. Yet issues about inappropriate communication from parties, about the sharing of data across systems, about intrusive uses of the Internet and social media, and about data breaches have surfaced in some countries. Furthermore, trends in Western party systems towards a greater de-alignment of the electorate will surely place further pressures on parties to target voters outside their traditional bases, and to find new, cheaper, and potentially more intrusive, ways to influence their political behavior. Voter surveillance requires further comparative analysis from a variety of disciplinary perspectives. The issues are not confined to the privacy of the individual voter, but relate to broader trends in democratic politics.

Contents

[Introduction](#)
[Voter surveillance trends in the United States](#)
[Importing voter surveillance practices from the United States](#)
[Personal data protection law and political parties](#)
[Privacy, security and political parties: The dominant issues](#)
[The political science of voter surveillance](#)
[Conclusions and implications](#)

Introduction

The remarkable successes of the Obama campaign in 2008 and 2012, and its advanced uses of new technologies to persuade and target voters, have not gone unnoticed in other democratic countries. The winning strategy of that campaign has been attributed, in part, to its unprecedented ability to capture and profile personal data on the American voting public and to target precisely defined constituencies with tailored messaging, in both off-line and online formats. To a considerable extent, these practices have been facilitated by the absence of information privacy laws that apply to political parties and election campaigns, and by the First Amendment to the Constitution that provides robust protections for freedom of speech and association.

While “voter surveillance” is nowhere as extensive or sophisticated in other countries, candidates and political parties elsewhere have reportedly looked with great envy on the activities of their U.S. counterparts and longed for similar abilities to find and target potential supporters and to ensure that they vote. But the conditions are, of course, different. The “micro-targeting” of voters has some dramatically different implications in other democratic cultures which possess different institutions, electioneering traditions, and typically far stronger privacy laws which govern the capture, processing and dissemination of personal data — and especially sensitive personal data such as that related to political opinions and affiliations.

The arguments in favor of processing vast amounts of ‘voter intelligence’ data in order to reach them with relevant political messaging are powerful. Parties and candidates have central responsibilities within democratic societies for voter education and mobilization. The general decline in trust in our democratic institutions, and the extensive trend toward “partisan de-alignment,” should make us pause before being too critical about voter surveillance. These issues call for a delicate balance between two powerful democratic values: on the one hand that of widespread citizen participation in democratic institutions, and on the other the value of personal privacy. This paper explores the ways that these balances are being struck in different democratic states.

While there is a burgeoning literature on the impact of the Internet on democratic practices in different countries (Chadwick, 2006), as well as on new techniques of political marketing (Davies and Newman, 2006; Lees-Marchment, et

al., 2009), very little of this literature focuses on the implications for personal privacy. Moreover, voter surveillance has rarely been addressed by privacy scholars, experts and regulators. And as we shall see, the network of data protection authorities (DPAs), charged with overseeing privacy legislation in different countries, has rarely ventured to regulate what political parties can, and cannot do, with the personal data under their control.

Nevertheless, voter surveillance issues are gradually creeping into the democratic discourse of countries like Canada, Australia, the U.K., and several states in continental Europe [1]. A broad and preliminary overview of the way these issues have been raised and addressed is, therefore, timely. The pressures for the more efficient and extensive uses of “voter intelligence” data are only going to intensify as new practices, and the businesses and consultants that promote them, penetrate the electoral practices of countries outside the U.S.

This article begins with a broad overview of contemporary techniques in the U.S. The next section tries to identify areas where these techniques have been imported into other countries, with particular attention paid to Canada, Australia and the U.K. Privacy and data protection law does cover the activities of candidates and political parties, and the next section analyses how European law, in particular, tries to regulate these activities. A range of privacy-related questions on intrusiveness, the non-consensual capture of personal data, and data breaches, has surfaced and needs proper categorization and analysis. The paper concludes with a broader discussion of the implications of voter surveillance in different democratic regimes, and how the structure of different political systems might affect the adoption of these practices.



Voter surveillance trends in the United States

The study of surveillance now reaches into every corner of contemporary life. It is not just about “visual” monitoring, nor just associated with the security or intelligence apparatus of the state. It has become routine, normal or “everyday.” So one does not have to be a criminal or a suspect to be subjected to surveillance. Surveillance is, according to David Lyon, “any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered” [2]. And surveillance is not simply about large organizations using sophisticated technology; it is also something that individuals increasingly engage in. Surveillance is central to the new forms of disciplinary power and governance within modern and post-modern societies (Haggerty and Ericson, 2006).

Just as the literature speaks of “consumer surveillance” or “employee surveillance,” and analyzes the different practices and issues that arise in these different contexts as we play these different roles, so can one speak of “voter surveillance.” In our capacities as participants, non-participants or potential participants in the democratic electoral process, personal data is collected and processed about us for the purposes of regulating the fair and efficient conduct of elections but also in order to influence our behaviors and decisions. The norms, issues, and practices are, and should be, different in this context, from other contexts (Nissenbaum, 2009). Very little has been written in the broader privacy literature about voter surveillance. This paper is intended to begin to fill that gap and inspire further analysis and research.

We need look no further than the U.S. for an overview of contemporary voter surveillance practices. To the extent that these practices are observed in other societies, they have been imported or copied from the U.S. This overview is an imperfect summary, as these practices are inherently dynamic and shrouded in considerable secrecy as a result of natural jealousies and proprietary instincts between political parties and between the consultants they employ. Nevertheless, the largely journalistic literature that has commented on the recent electoral cycles in the U.S. gives us some important clues as to the most significant trends. Five seem crucial: the development of voter management databases; the integration of personal data from commercial data brokerage firms; micro-targeting; the decentralization of personal data to local campaigns; and, targeted sharing.

Political parties have, for many years and legally, maintained membership lists. Voter management databases, however, are a more recent phenomenon and designed to profile a far broader range of voters, including those who are not, and may never be, supporters. It is difficult to pinpoint the origins of these databases, but they clearly began in the United States and have since spread elsewhere. Voter databases are now considered essential to many aspects of a campaign, including fundraising, get-out-the-vote (GOTV) operations, recruitment of volunteers, and the tracking of issues across key geographic and demographic constituencies.

Over the last 20 years or so, desktop-based and Internet-based software have proliferated and provided “off-the-shelf” solutions for voter management purposes. There are now a number of technology providers whose basic platforms have been adapted by political parties and interest groups. The Voter Activation Network is that preferred by those left-of-center parties, such as the U.S. Democratic Party, as well as by more progressive campaigns. The Democrats launched VoteBuilder, based on the VAN platform back in 2004, and have made steady improvements to it in every campaign since. The Republicans have used a tool called Voter Vault since 2001, which was re-launched as the GOP Data Center for the 2012 elections (Judd, 2013).

The construction of these databases is facilitated by the availability of data from the electoral roll before and during election campaigns. Rules differ from country to country on whether, and for how long, such electoral registration data may be accessed and stored by parties. In the United States, each state under the 2002 Help America Vote Act is required to compile an official state voter database. Because the data fields included in each state are not uniform, companies have merged these data with other publically available sources to create comprehensive voter files which are then sold to a range of users for campaigning purposes [3]. Howard and Kriess [4] suggest that parties might also capture information about voters from a variety of other sources including: publicly stated positions (such as letters to local newspapers or postings on blogs); public petitions; telephone polling; canvassing by phone, writing or on the doorstep; donor databases; and, by the observations of party volunteers who record the addresses at which opposition election signs are posted. Inferences about party preferences and voting intentions can be gleaned from many sources.

We also know that U.S. parties make extensive use of commercial marketing databases. Thus the political data on party affiliation and behavior is combined with other data on activities, interests and purchasing habits available from data brokerage firms such as Acxiom, Dun and Bradstreet, InfoUSA and Aristotle.com. Here is one pitch from Aristotle.com: "In addition to the wealth of demographics Aristotle already provides for high-level micro-targeting, you can now identify your voters based on their interests and hobbies. Aristotle maintains a list of over 5.4 million voters who hold hunting and fishing licenses, as well as individuals who subscribe to a wide array of magazine subscriptions including family, religious, financial, health, culinary and do-it-yourself publications." [5]

Sophisticated algorithms thus allow inferences to be made about political behavior from "non-political" sources — magazines read, sports played, income earned, property owned, and so on — and overlaid with locational information portrayed through a Geographic Information System (GIS). The mining of these data allow tailored messages to increasingly refined portions of the voting public. In place of the crude, single television advertisement broadcast across the entire country, hundreds of variations are possible depending on the target audience and whether the message is conveyed through TV, radio, direct mail, e-mail, Internet banner ads, social media, or traditional signage in public places. This is what has come to be called "micro-targeting" where campaigns have "come to know you better than you know yourself" (Brennan, 2012). It is also deeply controversial; one study found that 86 percent of respondents did not like and did not want personally targeted ads during election campaigns (Turow, *et al.*, 2012).

Much of this "voter intelligence data" can now be integrated into other software for Web site development, social media strategies, and political messaging. Google's "Political Campaign Toolkit" is an example, and allows campaigns to: "drive your campaign message to the right people at the right time"; "reach engaged voters everywhere in one account"; "respond rapidly": and, "target your ads geographically or by demographic, and craft unique messages to voters, donors, or volunteers." [6] Another example is NationBuilder, promoted as a new tool for campaign management because "people aren't paying attention to ads anymore; they're paying attention to real people." [7] Nationbuilder claims to provide management tools for identifying supporters, volunteers, donors, and recruiters, which can then be matched with voter files relevant for the location and campaign.

Much of these data are then decentralized through mobile applications that allow canvassers to access these data in real time and generate relevant lists for telephone marketing, e-mail marketing and door-to-door canvassing. Nationbuilder promotes a tool called "Electionear" that "lets you have high-impact conversations with voters and constituents without wasting precious time and money in the process." [8] Other examples are the Footwork and Moonshadow "Ground Game" applications [9]. These applications can place a significant amount of information about voter histories, profiles, and basic contact details in the hands of thousands of campaign workers who may not have any privacy and security training. And when those "high-impact conversations" occur over the phone or on the doorstep, are voters told that the results of these conversations might be communicated instantaneously to campaign and party headquarters for permanent storage?

There is another and larger shift in campaign logic at work. Polling evidence suggests emphatically that voters, and particularly young voters, do not trust parties or media organizations, but are more likely to be influenced by the attitudes and behavior of their friends. In the era of social media, this has come to be known as "targeted sharing" and the Obama campaign made particularly effective use of this strategy in 2012 (Sherer, 2012). In the final weeks of the campaign, over 600,000 Facebook friends of the Obama campaign signed up for an Obama for America application that allowed the sharing of specific content about the Obama campaign with their friends. In an instant, the campaign had access to more than five million new contacts who potentially saw each other registering to vote, giving money, sharing videos on the campaign, and voting on or before Election Day. Scientific studies indicated that this kind of "targeted sharing" through Facebook can have a small but significant impact on voting, especially among the 18-29 age group (Bond, *et al.*, 2012).

The range and sophistication of voter surveillance techniques in the U.S. are staggering, unprecedented and unparalleled elsewhere. They are 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. They are also made possible by a permissive campaign financing system that generally places no restrictions on how much money individual candidates may spend on their election campaigns, nor how much (in total) they may raise from individuals, groups or corporations. The current polarization of the U.S. political system will continue to place enormous pressure on both main parties to continue to use these, and other tools.

The direct targeting of potential voters by political parties is still not a widespread practice in countries outside North America, where parties still tend to communicate through mass messaging, rather than through the micro-targeting of individual voters or specific neighborhoods. Structural differences between presidential and parliamentary systems, between unitary and federal states, between first-past-the-post (simple plurality) and proportional representation (PR) electoral systems, also influence the spread of these practices. Furthermore, the system of primary elections in the U.S., which places central responsibility with political parties for registering voters, has no equivalent elsewhere. It is therefore tempting to conclude that this level of voter surveillance could never be emulated elsewhere.

Nevertheless, despite clear differences, certain American voter management practices have found their way into other political systems, through the active efforts of American political consultants and their counterparts elsewhere. So, what do we know about the export of U.S. voter surveillance techniques to other democratic states?



Importing voter surveillance practices from the United States

An indication that similar campaigning techniques have gradually been entering the politics of other countries is reflected in concerns expressed by the international DPAs back in 2005. In a joint resolution at their annual conference in Montreux, the DPAs expressed a collective concern 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” (International Conference of Data Protection and Privacy Commissioners, 2005).

We certainly know that the voter management software used by U.S. parties has been adopted elsewhere. In Canada, for instance, there has been close collaboration between Republican consultants and the Canadian Conservative party, whose Constituent Information Management System (CIMS) was developed using the Voter Vault software pioneered by the Republicans. In Canada, voter lists are legally provided to political parties under the authority of the Canada Elections Act (Bennett and Bayley, 2012). The Conservatives then use this framework to populate the database with a range of other data on voter behavior and preferences. As a result of a recent scandal in Canada over the practice of robo-calling, the operation of CIMS has been subjected to public scrutiny and provides some insights into how these databases actually work (Curry, 2012). The Party, we understand, populates CIMS “with information including *but not limited to*: the Canadian Electors List; Phone numbers; mailing addresses; issue relationships; membership information; donor information and history.” [10] The published training materials on CIMS reveal that each voter is assigned a score of -15 to +15 on the basis of these data. Walk lists, phone lists, e-mail lists, lawn sign allocations and other campaigning tools are then generated, to allow the party to more efficiently target voters, and thus use its limited human and financial resources to best effect [11]. The Canadian Liberal Party has a similar “voter identification and relationship management system” called Liberalist, originally based on the Democrats’ Voter Activation Network platform [12].

It is reported that the main political parties in the U.K. have operated similar databases for several years, based on the proprietary software used by their counterparts in the United States. They too augment the basic address information legally acquired from the full electoral register with additional personal data on supporters and non-supporters alike (Amberhawk Training, 2013). The Conservative Party originally used the “Voter Vault” software and now uses MERLIN (Managing Elector Relations through Local Information Networks) (Crabtree, 2010). The Labour Party now operates a system called Contact Creator [13].

The legal requirement that data controllers register their holdings of personal data with the U.K. Information Commissioner’s Office (ICO) provides some further insights into the categories of data processed by political parties. The Labour Party processes personal information about: staff, members and supporters, suppliers, the electorate, complainants, correspondents and enquirers. And this may contain sensitive categories of data such as physical or mental health details, racial or ethnic origin, religious or other beliefs, and political opinions. The longer register entry for the Conservative Party breaks down data categories according to five different purposes: staff administration; advertising, marketing and public relations; administration of membership records; canvassing political support amongst the electorate; consultancy and advisory services; and, fundraising. A broad range of sensitive and non-sensitive data categories is listed under each purpose. Neither register entry has been updated since 2001 [14].

The existence of party databases has also been subjected to media scrutiny in Australia. Most notably, in advance of the 2010 state election in Victoria, the *Melbourne Age* published details of the voter management database operated by the Australian Labour Party, which reportedly used software called “Electrac.” The Liberal Party used a system entitled “Feedback” (Millar and McKenzie, 2010). These systems have a far longer history, and are probably targeted more at voter persuasion and issue tracking than GOTV operations, seeing that it is mandatory to vote in Australia (van Onselen and Errington, 2004).

Evidence of similar voter management tools in other countries is spotty. In most other democracies, as we shall see below, it would generally be regarded as illegal under personal data protection law to process data on political opinions and affiliations on people other than those who had explicitly signed up as members or who had regular contact with the party. But there are also important constraints imposed by wider electoral traditions. In many societies, the practice of individual communication and targeting is simply not regarded as culturally acceptable. An extreme case is that of Japan, where long-standing Japanese election law prohibits Japanese politicians from making use of any electronic media for campaigning in the 12 days prior to an election. Political candidates are allowed to have Web sites during this time, but they are not allowed to update them or post material via social media (Masters, 2009). And in every country, campaign finance regulation severely limits the funds available to political parties through which they might build, and of course continually update, voter management systems.

Thus, the relevant privacy questions are simply not encountered and addressed in other countries in the same way that they have been in North America. But that does not mean that privacy questions have not arisen, and that they will not continue to challenge the DPAs.

Personal data protection law and political parties

Over the last 40 years or so, jurisdictions the world over have passed laws designed to protect the personal data processed by both public and private organizations. European jurisdictions favor the term “data protection” whereas countries elsewhere tend to prefer “privacy” or “information privacy” as the best way to frame the issues. All these laws, and reports suggest that there are now over 90 (Greenleaf, 2013), have essentially the same purpose: to grant individuals rights over the information that circulates about them, and to impose obligations on organizations to process that data responsibly and securely (Bennett and Raab, 2006). To what extent, and in what ways, do data protection or information privacy laws apply to the activities of political parties?

Members of the European Union (EU) have been obliged to pass data protection legislation consistent with the provisions of the 1995 European Union Data Protection Directive (EU, 1995). The current intent is to replace this Directive, and also the national laws, with one harmonized Regulation on Data Protection (EU, 2012). Under both regimes, political parties are clearly regulated. There are a number of relevant provisions that can be cited from the new Draft Regulation.

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 gives the following guidance about the processing of personal data by 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 strict reading of the law would indicate, therefore, that parties may only process political data on members, former members or 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. No European DPA has ruled on the legality of the databases held by political parties. But a recent analysis from a British law firm suggests that, even if voter-related data is in the public domain, it would still not be considered “fair processing” under the U.K. Data Protection Act (Amberhawk Training, 2013).

In countries that have not passed comprehensive privacy protection rules for both public and private sectors, political parties have tended to fall between the cracks of two legal regimes; one tailored to government agencies, and the other for commercial enterprises. In Canada, for instance, neither the Canadian Privacy Act of 1982, nor the Protection of Personal Information and Electronic Documents Act (PIPEDA) of 2000 cover political parties. At the same time, the Office of the Canadian Privacy Commissioner (OPC) has received a number of complaints about invasion of privacy by candidates and politicians going back several years. Partly in response, the OPC commissioned 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, and clearly need to be brought into the system of privacy regulation in some way (Bennett and Bayley, 2012).

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 (RCMP) and from Elections Canada. The most interesting aspect of this affair is that only non-Conservative supporters were targeted, meaning that the individual must have had either authorized or unauthorized access to the CIMS voter management database. The Chief Electoral Officer recommended that it was timely and appropriate for the basic privacy principles within PIPEDA to be applied to political parties (Elections Canada, 2013).

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 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 organizations 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” (Australian Law Reform Commission, 2008). To date, no such guidance has been issued. Furthermore, recent proposals to amend the Australian Privacy Act to create a comprehensive set of rules for all organizations still leave political parties out of the picture.

In the vast majority of other states (in Asia, Latin America and elsewhere), political parties are generally assumed to be covered by data protection law. That does not mean to say that there is any expectation that they will be actively regulated, nor that they necessarily realized the various implications when the laws were enacted. The questions raised here are largely new, and have generally gone unrecognized during the public and parliamentary debates that have attended the enactment of national data protection statutes.



Privacy, security and political parties: The dominant issues

The importance of including political parties within the overall data protection regime is highlighted by the range of issues that have already arisen, and required guidance and regulation. 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 democratic countries. Four sets of interrelated questions have so far arisen.

The first, and most common, relates to in questions of *inappropriate communication* during campaigns. The U.K. ICO issued 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 (ICO, 2005). This followed a case involving the Scottish National Party that was found to have breached the Privacy of Electronic Communications Regulations (PECR) by using automated dialing and calling devices without the data subject's consent. The French Commission Nationale de l'Informatique et des Libertés (CNIL, <http://www.cnil.fr/english/>) provided similar guidance on political campaigning in 2012 (CNIL, 2012). Practices do tend to differ around Europe, depending on whether the DPA considers political marketing equivalent to commercial marketing, and also whether parties are obliged under law to observe the restrictions imposed by national “Do-Not-Call” lists. In many countries, individually addressed mail requires an explicit opt-out provision. The rules for e-mail

tend to be somewhat stricter.

A second set of issues relate to the inappropriate use of lists from other sources for the purposes of political campaigning and communication. These questions often involve elected members of the legislature who have access to personal data in that capacity, and who then use that information, deliberately or unwittingly, for electoral advantage. One set of problems relates to the use of membership lists gleaned from other organizations (unions, churches, sports and recreational clubs, etc.) for campaigning and electioneering purposes. These cases are typically quite straightforward in countries where strong data protection laws exist, although it should be noted that in some European countries, such as Belgium and the Netherlands, historically based on a “pillarized” or vertically integrated organization of society, the close ties between various associations and political parties have also historically meant the sharing of membership lists (Post, 1989).

Problems have particularly occurred in countries where parties are not covered by privacy protection legislation. There are several examples from Canada. In 2006, Conservative Party MP Cheryl Gallant sent birthday cards to her constituents using data from passport applications, an incident later investigated by the Office of the Ethics Commissioner under the Conflict of Interest Code for Members of the House of Commons. In October 2007, Rosh Hashanah cards were sent by the Prime Minister’s Office to supporters with “Jewish-sounding” names, many of who were unsettled and left wondering how such a list could be compiled. In 2011, about 10,000 people signed a petition addressed to Jason Kenney and his ministry, Citizenship and Immigration, demanding that a young Nicaraguan gay artist who was facing deportation, be allowed to stay in Canada. Kenney later sent out an e-mail message to those who had signed the petition, extolling what the government of Canada has been doing to promote “gay and lesbian refugee protection” and startling many in the gay community that a federal minister had their contact information at his disposal (Bennett, 2013). A leak of the details of the database of the Australian Labour Party showed how campaign workers had access to many details on the private lives of voters originally shared confidentially with the offices of local MPs (Millar and McKenzie, 2010).

One countervailing principle in parliamentary systems based on the “Westminster model” is that of “parliamentary privilege.” Among other things, this doctrine has been invoked to exclude from the purview of access to information and privacy law, information that is collected and processed in the course of an elected representative’s democratic duties. In New Zealand, for instance, there is an important exception in the application of the data protection law for parliamentary privilege. However, the former Commissioner, Bruce Slane, as early as 1997 expressed some considerable concerns about the use of the New Zealand electoral roll for “non-electoral purposes” (New Zealand, Privacy Commissioner, 1997). In other jurisdictions, the Australian state of Victoria for instance, codes of conduct have been developed to provide guidance to elected members about appropriate uses of personal information (Victoria Parliament, 2001).

A third set of issues relates to the capture of data on political preferences through various online activities. One widespread issue is the logging of “cookies” when an individual visits the party’s Web site. The non-consensual capture of information about browsing habits through the logging of cookies is governed in Europe by the laws passed pursuant to the E-Privacy Directive of 2009 (EU, 2009). The Netherlands has a particularly strict interpretation of the level of consent required for the installation of cookies, leading to stories that the leading political parties and indeed the Cabinet were breaking their own rules (Oord and Kampschreur, 2012).

Beyond the interpretation of the e-privacy rules, all political parties now have the ability to capture a variety of personal data online through a variety of transparent and less transparent means. In this respect, the issues they confront are no different from those in any other commercial or non-commercial organization. Best practices dictate that they should communicate a clear privacy policy indicating the extent to which identifiable personal information might be captured by any visitor to the Web site, and how it might be used and disclosed. Ideally, such a policy should not be framed in complex and lengthy legalese. A recent analysis of the privacy policies of Canadian political parties found, however, that “the commitments are often vague, and the remedies incomplete. In terms of personal-information handling information and processes, none discloses or hints at the presence of a privacy management framework, or a designated individual with responsibility for privacy issues” [15]. In 2011, the Irish Data Protection Commissioner was notified that the Web site of the Fine Gael party did not have a privacy statement, in contravention of Irish law. A further issue arose because the Web host provider was based in the United States, meaning that personal data was being transferred outside the EU, requiring that the provider be certified under the EU-US Safe Harbor agreement, which it was (Kelly, 2011).

Parties in many countries are becoming increasingly adept at using social media to target messages, to recruit volunteers and donors and to track issue engagement. Social media can also provide a far cheaper way to communicate to a larger audience than more traditional broadcast methods. All the Web sites of the major parties in most democratic states have links to a variety of social media platforms. In the social networking environment, the online privacy practices of political parties are also deeply dependent upon the corporate policies and technical standards and defaults of the social media companies. Those practices are varied and fluctuating and to differing extents, encourage the liberal sharing of personal information [16]. For instance, 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. “Friending” a political party on Facebook without the user implementing the appropriate privacy controls can then result in the users’ name and photo being listed on the parties’ social media page. Thus, the practices of political parties, and the privacy rights of their members, are closely related to the privacy policies and mechanisms embedded within these social media platforms, as well as to the privacy choices that individuals make according to varying degrees of knowledge about privacy and sophistication about the technology.

The final issue concerns data breaches. Many provincial and national legislatures around the world have enacted legislation mandating notice to data subjects about the loss or unauthorized acquisition by an unauthorized person of an information resource containing personal information. The scope and standards of these laws vary, and some of them limit liability when the data are suitably encrypted. However, many organizations that suffered a breach learned that the cost of providing notice to data subjects can be large, and the damage to reputation significant. No type of organization has been immune from such losses, including political parties.

Thus far, there has not been a significant breach of electoral data from political parties during an election campaign, that we know of; one can only speculate on the political consequences of a major loss of personal data at such a time. Nevertheless, there have been some troubling instances. In 2012, there was a leak of over two million voter files from Elections Ontario. Two USB keys went missing containing names, addresses, genders, birth dates and whether a person voted in the last election for residents in as many as 25 ridings. An investigation by the Ontario Information and Privacy Commissioner found systemic failures in privacy management within Elections Ontario (Ontario, Information & Privacy Commissioner, 2012). Other breaches occur through the malicious activity of hackers, such as the breach of information on online donors to the Canadian Conservative Party, caused by a hacker who exploited a vulnerability within the Conservative Party Web site (Canadian Broadcasting Corporation, 2011). In Ireland in 2011, Fine Gael's Web site was the subject of a sustained denial of service attack during which the personal details (including IP addresses, mobile phone numbers, location and e-mail addresses) of up to 2,000 users of the site were compromised (Kelly, 2011).

These isolated cases give an indication that data protection and other relevant legal provisions have influenced party activities in countries outside the United States. But the extent and nature of voter surveillance by political parties is probably influenced less by the content of data protection law, and the activities of DPAs, than by broader institutional and cultural features of individual political systems. The final section discusses those characteristics, and therefore brings this issue under a wider lens of emerging trends in democratic and electoral politics.



The political science of voter surveillance

It is tempting to conclude that the practices now observed in the United States are the direct result of a digital revolution that enables the mining and analysis of "Big Data" and then places the results of that analysis into the hands of individual political parties and thousands of campaign workers and volunteers. Technology certainly is a critical part of the story of the "secret science" behind winning elections. So too are the many professional political consultants, often with impressive technical credentials, who aggressively market their predictive models and algorithms to partisan professionals desperate for any political advantage within highly competitive electoral and political environments. That is the story told by Issenberg (2012).

There is, however, another set of socio-political factors that are driving many of the contemporary trends in political marketing and voter surveillance. We need to examine this larger context in order to begin to ask the really critical questions about the implications of these trends for democratic politics. This final section is suggestive of the deeper causes and implications, and of the further research that is required.

Voter surveillance has arisen during an era when political analysts have noted, and lamented, a general process of *partisan de-alignment*. In simple terms, fewer people have fixed attachments to political parties; fewer are now members of political parties; and, fewer regard them as the main vehicle of political participation and engagement. The trend is a general one across Western democracies and rooted in a general decline in trust in political institutions (Dalton, 2004). The decline is normally dated to the 1960s with the advent of television, the rise of alternative "social movements" and the weakening of the class attachments to parties that had characterized the industrial era.

One of the implications of "parties without partisans" (Dalton and Wattenberg, 2000) is that political parties have needed to find newer methods to engage with the electorate to find donors, volunteers, members and supporters. They cannot rely on huge proportions of the voting public based on conventional class or religious affiliations. Voter surveillance techniques have arisen, therefore, partly to address this fundamental shift in partisan allegiances. Voters have become more distrustful of politics, but also more demanding. In rational choice terms, a greater proportion can be regarded as clients of the political system, whose allegiances float depending on the personalities and programs on offer. Unlike earlier generations, where family partisan attachments typically predicted voting behavior, for the last thirty years higher proportions of voters in Western democracies can be susceptible to the correct marketing pitch. And that method of persuasion, it is contended, is likely to be more effective when the party knows more about the individual preferences and attitudes of the voting public.

The nature of political parties has therefore changed. The conventional distinctions were provided by Maurice Duverger (1954) who distinguished between cadre, mass and devotee parties. The cadre party was the model that existed before the large-scale franchise. They were essentially elite and centralized parliamentary groupings, which then sought support from the wider electorate when voting was extended throughout the late nineteenth and twentieth centuries; a good example would be the British Conservative Party. Mass parties, like the Labour and Social Democratic Parties of Western Europe, grew out of working class and trade union movements. The legislative wing was a part, and not necessarily the most important part, of that broader movement. The concept of membership, therefore, was fundamentally different. According to Duverger, the third category of political parties are devotee parties, built strictly around a charismatic leader, and which also tended to rise and fall according to the popularity of that leader.

These classic distinctions have broken down with the advent of "catch-all" parties (Kirchheimer, 1966). These parties emerged in response to the changing social conditions after World War II and are typically identified by their size as larger and more mainstream parties, by their pursuit of votes at the expense of doctrine, by their centrist and often inconsistent party platforms designed to appeal to ever wider audiences, and by an organizational style that is elite driven, and dependent on outside consultants. Catch-all parties attempt to win votes from anywhere they can, regardless of prior attachments and allegiances. Again the thesis is complex and there is disagreement over the extent to which this is, in fact, one category. If the main governing parties in Western democracies are now characterized by the "catch-all" characteristics, then the need to appeal and market beyond a narrow base is crucial, requiring a concomitant need for more information on a dynamic and shifting electorate.

Another trend that is also perhaps driven by partisan de-alignment is the search in many countries for more open and participatory procedures for selecting party candidates and leaders. "Primary elections" are the principal vehicle, and

have been a feature of U.S. democratic politics since the early twentieth century. Voters from the general public may participate in the “internal” affairs of the party by selecting candidates (congressional and presidential, state and federal) for the general election. Primary elections have become more frequent and widespread in recent years. They have essentially elevated the Democratic and Republican parties to the status of quasi-public institutions legitimized in state law, and responsible for the recruitment of candidates and the registration of electors.

In parliamentary systems, primary elections are far less common and far more recent, and raise a number of different questions. The most extensive participation in a primary occurred in France in 2011. Based on the Italian experience of 2005 and 2007, the French Socialist party decided that its candidate for the 2012 presidential election would be decided on the basis of an open primary. Not only would registered Socialist voters be able to participate; so would all voters who agreed to sign a commitment attesting to the values of the left and willing to donate a nominal sum of one euro to the party. The party organized one national vote, but in two stages on 9 and 16 October 2011 and elected Francois Hollande. Some 2.6 million voters participated in the first round, and three million in the second.

Protests were raised regarding the primary’s constitutionality, the legitimacy of using public facilities for a “private” election, as well as the legality of using electoral lists for an internal party process. Primary elections pose some peculiar and novel challenges for privacy principles, and data protection authorities. The CNIL struggled with the question of whether the party might continue to process data on those who had voted in the primaries, as if they were members or “regular contacts.” They concluded eventually that they could not, because the purpose of collection was different (CNIL, 2012). Similar issues arose for the Italian DPA after primary elections for the center left coalition, Common Good, in 2012 (Italy Garante, 2012). To the extent that primary elections will continue to be a feature of democratic politics in Europe, they will continue to raise interesting issues about the appropriate balance between parties’ rights to association, and the privacy rights of voters.


Conclusions and implications

This survey would predict, therefore, that we will see a “ratcheting up” of voter surveillance techniques, including “micro-targeting” in more countries outside the United States, albeit tempered by local traditions, rules, and procedures. What would be the broader implications for our democratic politics?

Howard and Kriess (2010) contend that excessive surveillance of voters can have negative consequences for associational freedom, democratic debate and democratic competitiveness. Constant surveillance of political activity, attitudes and behavior has a demonstrable chilling effect of democratic discourse and participation, they argue. They also contend:

Asymmetries in information between political actors and voters, in turn, facilitate the ability of elites to manipulate the electorate. For example, candidates and their agents — paid operatives or citizen-supporters enlisted to spread their message and generate data on their friends and neighbors — know a lot more about those they are seeking to represent than citizens do about them. This makes these forms of “personalized political communication” fundamentally transactional and manipulative, as campaigns and their supporters strive to tailor their political speech in terms of what individual voters want to hear.

In parliamentary systems, we might hypothesize that voter surveillance would have some additional effects and implications. In a system like the United States, with two huge and very well financed parties, incremental differences in voter management techniques might affect the outcome of individual elections, but it will not seriously influence the structure of the party system itself. The effects in multi-party parliamentary systems might be different, and may very well consolidate power in the larger, and more well-financed, parties and make it more difficult for smaller parties to be nationally competitive. Micro-targeting can also have a disproportionate impact in parliamentary systems where small shifts in the voting behavior of relatively small, and precisely defined, slithers of the electorate in key competitive electoral districts, can indeed affect the distribution of seats in the legislature and even the composition of governments. The effect might be especially pronounced in those parliamentary systems, such as the U.K. and Canada, whose elections are based on the simple-plurality electoral system, and where minor shifts in the popular vote can produce exaggerated swings in seats won.

Questions about voter surveillance are rooted, therefore, in these and other basic characteristics of particular democratic systems: the electoral process; the number and fragmentation of political parties; the rules for campaign financing; leadership selection processes; the autonomy of local candidates; as well as historical campaigning traditions. The relationship between these structures and processes and the development of different voter surveillance techniques require far more research in a comparative context. The broad conclusion here is that one should not assume that the techniques currently apparent in the United States will somehow stay there, because of American “exceptionalism.” The early evidence is that the “secret science of winning campaigns” (Issenberg, 2012) is a subject that parties elsewhere are eagerly interested in learning, with profound, but unknown, implications for personal privacy, civil liberties and democratic values. 

About the author

Colin Bennett received his Bachelor’s and Master’s degrees from the University of Wales, and his Ph.D. from the University of Illinois at Urbana-Champaign. Since 1986 he has taught in the Department of Political Science at the University of Victoria, where he is now Professor. He has held Visiting Professorships at: Harvard’s Kennedy School of

Government; the Center for the Study of Law and Society at University of California, Berkeley; the School of Law, University of New South Wales; and, at the Law, Science, Technology and Society Centre at the Vrije Universiteit in Brussels.

His research has focused on the comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels. In addition to numerous scholarly and newspaper articles, he has published six books: *Regulating privacy: Data protection and public policy in Europe and the United States* (Cornell University Press, 1992); *Visions of privacy: Policy choices for the digital age* (University of Toronto Press, 1999, co-edited with Rebecca Grant); *The governance of privacy: Policy instruments in global perspective* (MIT Press, 2006 with Charles Raab); *The privacy advocates: Resisting the spread of surveillance* (MIT Press, 2008); *Playing the identity card: Surveillance, security and identification in global perspective* (Routledge, 2008 co-edited with David Lyon); and, *Security games: Surveillance and control at mega-events* (Routledge, 2011, co-edited with Kevin Haggerty). He has completed policy reports on privacy protection for various Canadian and international bodies. He is currently the co-investigator of a large Major Collaborative Research Initiative grant entitled "The new transparency: Surveillance and social sorting." Web: <http://www.colinbennett.ca>
E-mail: cjb [at] uvic [dot] ca

Notes

1. This paper is inspired in part by a report written for the Privacy Commissioner of Canada: Colin J. Bennett and Robin M. Bayley, "Canadian federal political parties and personal privacy protection: A comparative analysis" (March 2012), at http://www.priv.gc.ca/information/research-recherche/2012/pp_201203_e.asp, accessed 28 June 2013. I am grateful to Ian Brown for comments on an earlier version of this article.
2. Lyon, 2001, p. 2.
3. An example would be [aristotle.com](http://www.aristotle.com) which "provides high-quality political data for political organizations, campaigns, consultants and governmental agencies worldwide. Our massive and ever-expanding database includes over 190 million U.S. voters from 3,100 counties and political data from 157 nations."
4. Howard and Kriess, 2010, pp. 17–19, at <http://firstmonday.org/article/view/2975/2627>, accessed 28 June 2013.
5. <http://www.aristotle.com/political-data>, accessed 28 June 2013.
6. <http://www.google.com/ads/politicaltoolkit/>, accessed 28 June 2013.
7. <http://nationbuilder.com/political>, accessed 28 June 2013.
8. <http://www.organizer.com>, accessed 28 June 2013.
9. <http://www.gofootwork.com/features>; <http://www.moonshadowmobile.com/data-visualization/ground-game/>, accessed 28 June 2013.
10. "CIMS Electoral District Association Agreement," at <http://cpccims.ca/forms/CIMS%20EDA%20Agreement%20Form.pdf> (my emphasis), accessed 28 June 2013.
11. A training presentation for CIMS can be found on the blog of the *Toronto Star* at www.thestar.blogs.com/files/cims.ppt, accessed 28 June 2013.
12. <http://liberalist.liberal.ca/about-us/>, accessed 28 June 2013.
13. <http://www.cfl.labour.co.uk/images/uploads/166988/9b6fc688-c195-be24-2db3-b7f130f35c08.pdf>, accessed 28 June 2013.
14. Data Protection Register entries nos. Z5909711 (Conservative Party) and Z5487298 (Labour Party), at <http://www.ico.org.uk/esdwebpages/search>, accessed 28 June 2013.
15. Bennett and Bayley, 2012, p. 32.
16. See the report of the Canadian Access to Social Media Information (CATSMI) Project, at www.catsmi.ca, accessed 28 June 2013.

References

- Amberhawk Training Ltd., 2013. "Could the Conservative Party's electoral database breach the Data Protection Act?" *Hawktalk* (5 March), at <http://amberhawk.typepad.com/amberhawk/2013/03/could-the-conservative-partys-electoral-database-breach-the-data-protection-act.html>, accessed 28 June 2013.
- Australia Law Reform Commission, 2008. "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>, accessed 28 June 2013.
- Allison Brennan, 2012. "Microtargeting: How campaigns know you better than you know yourself," *CNN* (5 November), at <http://edition.cnn.com/2012/11/05/politics/voters-microtargeting>, accessed 30 June 2013.
- Canadian Broadcasting Corporation (CBC), 2011. "Online donors data breached: Conservatives" (8 June), at <http://www.cbc.ca/news/politics/story/2011/06/08/pol-conservatives-hacker-donors.html>, accessed 28 June 2013.

Colin J. Bennett, 2013. "Data Point — What political parties know about you," *Policy Options*, volume 34, number 2, pp. 51–53, and at <http://www.irpp.org/en/po/aboriginality/new-policy-options-article-11/>, accessed 23 July 2013.

Colin J. Bennett and Robin M. Bayley, 2012. "Canadian federal political parties and personal privacy protection: A comparative analysis" (March), at http://www.priv.gc.ca/information/research-recherche/2012/pp_201203_e.asp, accessed 28 June 2013.

Robert M. Bond, Christopher J. Fariss, Jason J. Jones, Adam D.I. Kramer, Cameron Marlow, Jaime E. Settle, and James H. Fowler, 2012. "A 61-million-person experiment in social influence and political mobilization," *Nature*, volume 489, number 7415 (13 September), pp. 295–298.

Andrew Chadwick. 2006, *Internet politics: States, citizens, and new communication technologies*. Oxford: Oxford University Press.

Commission Nationale de l'Informatique et des Libertés (CNIL), 2012. "Deliberation no. 2012-020 du 26 Janvier 2012 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 <http://www.cnil.fr/documentation/deliberations/deliberation/delib/259/>, accessed 23 July 2013.

James Crabtree, 2010. "David Cameron's battle to connect," *Wired* (24 March), at <http://www.wired.co.uk/magazine/archive/2010/04/features/david-camerons-battle-to-connect>, accessed 28 June 2013.

Bill Curry, 2012. "Robo-call furor focuses attention on massive Tory database," *Globe and Mail* (29 February), at <http://www.theglobeandmail.com/news/politics/robo-call-furor-focuses-attention-on-massive-tory-database/article4092455/>, accessed 28 June 2013.

Russell J. Dalton, 2004, *Democratic challenges, democratic choices: The erosion of political support in advanced industrial democracies*. Oxford: Oxford University Press.

Russell J. Dalton and Martin P. Wattenberg (editors), 2000. *Parties without partisans: Political change in advanced industrial democracies*. Oxford: Oxford University Press.

Philip J. Davies and Bruce I. Newman (editors), 2006. *Winning elections with political marketing*. London: Routledge.

Elections Canada, 2013, "Preventing deceptive communications with electors: Recommendations from the Chief Electoral Officer of Canada following the 41st General Election," at http://www.elections.ca/res/rep/off/comm/comm_e.pdf, accessed 28 June 2013.

European Union, 2012. "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)" (25 January), at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, accessed 28 June 2013.

European Union. 2009. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:NOT>, accessed 28 June 2013.

European Union, 1995. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>, accessed 23 July 2013.

Graham Greenleaf, 2013, "Global data privacy laws 2013: 99 countries and counting," *Privacy Laws & Business*, number 123, pp. 10–14.

Kevin Haggerty and Richard Ericson (editors), 2006. *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.

Philip N. Howard and Daniel Kreiss, 2010. "Political parties and voter privacy: Australia, Canada, the United Kingdom, and United States in comparative perspective," *First Monday*, volume 15, number 12, at <http://firstmonday.org/article/view/2975/2627> accessed 28 June 2013.

International Conference of Data Protection and Privacy Commissioners, 2005. "Resolution on the use of personal data for political communication" (Montreux, Switzerland; 16 September), at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Cooperation/Conference_int/05-09-16_resolution_political_communication_EN.pdf, accessed 23 July 2013.

Sasha Issenberg, 2012. *The victory lab: The secret science of winning campaigns*. New York: Crown.

Italy, Garante per la protezione dei dati personali, 2012. "Elezioni primarie 2012 e trattamento di dati personali — 31 ottobre 2012," at <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2079275>, accessed 23 July 2013.

Nick Judd, 2013. "Republican party's technology revival hopes hinge on data and data analysis," *TechPresident* (7 February), at <http://techpresident.com/news/23479/republican-partys-technology-revival-hopes-hinge-more-just-skype>, accessed 28 June 2013.

Jeanne Kelly, 2011. "Irish political party suffers data security breach," *datonomy, the data protection blog* (9 January), at <http://blogs.olswang.com/datonomy/2011/01/19/irish-political-party-suffers-data-security-breach/>, accessed 28 June 2013.

Otto Kirchheimer, 1966. "The transformation of Western European party systems," In: Joseph LaPalombara and Myron Weiner (editors). *Political parties and political development*. Princeton, N.J.: Princeton University Press, pp. 177–200.

Jennifer Lees–Marchment, Jesper Strömbäck, and Chris Rudd (editors), 2009. *Global political marketing*. London: Routledge.

David Lyon, 2001. *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.

Coco Masters, 2009. "Japan's Twitter-free election campaign," *Time* (18 August), at <http://www.time.com/time/world/article/0,8599,1917137,00.html>, accessed 28 June 2013.

Royce Millar and Nick McKenzie, 2010. "Revealed: How the ALP keeps secret files on voters," *The Age* (23 November), at <http://www.theage.com.au/victoria/state-election-2010/revealed-how-the-alp-keeps-secret-files-on-voters-20101122-1845e.html>, accessed 28 June 2013.

New Zealand, Privacy Commissioner, 1997. "Report by the Privacy Commissioner to the Minister of Justice on the Electoral Act 1993, 29 April 1997," at <http://privacy.org.nz/electoral-act-1993/>, accessed 28 June 2013.

Helen Nissenbaum, 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, Calif.: Stanford Law Books.

Ontario, Information & Privacy Commissioner, 2012. "Election Ontario's unprecedented privacy breach: A special investigation report" (31 July), at http://www.ipc.on.ca/images/Findings/2012-07-31-Elections-Ont_1.pdf, accessed June 28 2013.

Vincent Oord and Marjolein Kampschreur, 2012. "Dutch political parties violate their own cookie law," *Fleishman–Hillard*, at <http://fleishman.nl/2012/06/dutch-political-parties-violate-their-own-cookie-law/?lang=en>, accessed 28 June 2013.

Harry Post, 1989. *Pillarization: An analysis of Dutch and Belgian society*. Aldershot: Gower.

Michael Sherer, 2012. "Friended: How the Obama campaign connected with young voters," *Time* (20 November), at <http://swampland.time.com/2012/11/20/friended-how-the-obama-campaign-connected-with-young-voters/>, accessed 28 June 2013.

Joseph Turow, Michael X. Delli Carpini, Nora Draper, and Rowan Howard–Williams, 2012. "Americans roundly reject tailored political advertising," at <http://graphics8.nytimes.com/packages/pdf/business/24adco.pdf>, accessed 28 June 2013.

U.K. Information Commissioner's Office, 2005. "Guidance for political parties for campaigning or promotional purposes," at http://www.ico.org.uk/upload/documents/library/data_protection/practical_application/promotion_of_a_political_party.pdf, accessed 23 July 2013.

Peter van Onselen and Wayne Errington, 2004. "Electoral databases: Big brother or democracy unbound?" *Australian Journal of Political Science*, volume 39, number 2. pp. 349–366.

Victoria Parliament, 2001. *Privacy code for members of the Victorian Parliament and compliance checklist*. Melbourne: Scrutiny of Acts and Regulations Committee.

Editorial history

Received 28 June 2013; accepted 21 July 2013.

Copyright © 2013, *First Monday*.

Copyright © 2013, Colin Bennett.

The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies by Colin Bennett.

First Monday, Volume 18, Number 8 - 5 August 2013

<https://journals.uic.edu/ojs/index.php/fm/rt/prINTERfriendly/4789/3730>

doi:10.5210/fm.v18i8.4789