Surveillance & Society

Article

Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications

Colin J. Bennett

University of Victoria, Canada.
cjb@uvic.ca

-

Abstract

This paper surveys the various voter surveillance practices recently observed in democratic states and discusses the broad implications for privacy and democracy. Four broad trends are discussed: the move from voter management databases to integrated voter management platforms; the shift from mass-messaging to micro-targeting employing personal data from commercial data brokerage firms; the analysis of social media and the social graph; and the decentralization of data to local campaigns through mobile applications. The de-alignment of the electorate in most Western societies has placed 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. This paper builds on previous research to consider the theoretical tensions between concerns for excessive surveillance, and the broad democratic responsibility of parties to mobilize voters and increase political engagement. These issues have been insufficiently studied in the surveillance literature. They are not just confined to the privacy of the individual voter, but relate to broader dynamics in democratic politics.

-

Introduction

Surveillance has arguably become routine, normal or "everyday" and reaches into every corner of modern life (Bennett et al. 2014). It 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" (Lyon 2001: 2). And surveillance is not simply about large organizations using sophisticated technology; it is also something that individuals increasingly engage in. It is good and bad, top-down and bottom-up, and directed to humans, non-humans and spaces. It is a mode of power and central to the new forms of governance within modern and post-modern societies (Haggerty and Ericson 2006).

High-level conceptualizations about the nature and causes of surveillance help associate current practices with broad and profound structural transformations in contemporary societies (Lyon 2007). But macro-level theorizing only takes us so far in understanding the nature of individual and social risks in particular contexts (Nissenbaum 2009). Thus, surveillance has particular, and somewhat different, effects depending on whether we are consumers, employees, immigrants, suspects, students, patients or any number of other actors. Theorizing surveillance on a grand level tends not to expose the more subtle relations, norms and harms associated with the institutional and informational relations that attend the particular roles that we play and negotiate in our everyday lives. As Haggerty and Samatas remind us: "A global community of scholars has produced excellent case studies of the dynamics and normative implications of different surveillance practices, but run into more difficulty when it tries to make generalizations about surveillance

Bennett, C.J. 2015. Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications. *Surveillance & Society* 13(3/4): 370-384.
http://library.queensu.ca/ojs/index.php/surveillance-and-society/index | ISSN: 1477-7487

tout court, often because the surveillance dynamics and implications of, say, spy satellites, are wildly different from those of DNA testing" (2010: 3).

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 we can speak of "voter surveillance." In our capacities as participants, non-participants or potential participants in the democratic electoral process, personal data is increasingly captured and processed about us for the purposes of regulating the fair and efficient conduct of elections and also to influence our behaviors and decisions (Bennett 2013a, 2013b). The norms, dynamics, and dilemmas are, and should be, different in this voting context.

Very little has been written in the broader academic literature about voter surveillance. There is a certain amount of important journalistic commentary on the contemporary trends in micro-targeting in the United States (Issenberg 2012), and on how these practices have been imported to Canada (Delacourt 2013). Communication scholars have analyzed the new "tech-driven" politics as part of a larger assessment of changing campaign techniques (Howard 2006; Hendricks and Kaid 2011). And a number of political scientists have tried to evaluate whether or not new media campaigns affect voter engagement and behavior (Lees-Marchment, Stromback and Rudd 2009; Small 2010; Lees-Marchment 2011; Davies and Newman 2012). Very little of this commentary, however, engages with the larger question about how data about voters is being mined and profiled, nor evaluates the individual risks to privacy and the general implications for democratic politics.

This paper is intended to begin to fill that gap and inspire further analysis and research. The first section of the paper draws upon previous research to distill some of the most important trends in political campaigning, which has implications for the capture and processing of personally identifiable data. The paper then analyses how these practices are likely to influence the democratic politics of different states depending on different electoral practices and party systems. It then offers a set of broader theoretical reflections about the implications for democratic practice, drawing upon the recent literature on the complex and paradoxical tensions between surveillance and democracy (Haggerty and Samatas 2010).

Trends in Voter Surveillance

Generalizations about patterns and trends in this area are very difficult. Voter surveillance practices are inherently dynamic and shrouded in considerable secrecy as a result of natural jealousies and proprietary instincts between political parties and among the consultants they employ. Most innovations in this context are from the United States, and it is important not to infer universal trends from this American experience. There are some important differences that explain why voter surveillance is more prevalent in the United States and constrain their export to other democratic countries: the liberal campaign finance laws; a decentralized two-party system that permits much local autonomy; a polarized political system that encourages a competitive race for increasingly sophisticated data mining and analytical tools; a First Amendment that defines campaign contributions as "speech"; a widespread commercial market in personal data; and the absence of any comprehensive data privacy law (Bennett 2013b).

The term "voter surveillance" is admittedly an inaccurate and incomplete way to capture the range of practices currently observed in the broad campaign and electoral contexts of different Western societies. In reality, some political parties (and their associated groups and consultants) try to capture data on everyone in a society, whether we vote or not. Furthermore, as we shall see below, the analysis and profiling of voters is increasingly supplemented by data on consumers, and the mining of those data to target increasingly narrower slices of the electorate in key electoral districts. Politicians shop for votes, and increasingly find data on consumers increasingly valuable in that endeavor. Where voter surveillance begins and consumer surveillance ends is increasingly difficult to determine (Delacourt 2013).

Nevertheless, we can observe a number of general patterns and offer a preliminary assessment about the nature and extent of voter surveillance. Four trends seem crucial: the shift from stand-alone voter management databases to more integrated voter management platforms (popularly called "the campaign in a box"); the shift from mass messaging to micro-targeting, including the integration of personal data from commercial data brokerage firms; the increasing and more unstructured capture of user-generated data from social media; and the development of mobile applications for political messaging and campaigning.

From Voter Management Databases to Integrated Voter Management Platforms

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 practices, 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, and the tracking of issues across key geographic and demographic constituencies.

Over the last twenty years or so, desktop-based and internet-based software have proliferated and provided "off-the-shelf" solutions for these voter management purposes. There are now a number of technology providers whose basic platforms have been adapted by political parties and other campaigning organizations. The Voter Activation Network is that preferred by those left-of-center parties, such as the US Democratic Party, as well as 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 data may be 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 clients for campaigning purposes. The most obvious example is *Catalist* that serves the "progressive community" and boasts a continually updated database on over 280 million persons, based on four main sources of data: Registered Voters and Non-Registered persons (with contact information); Commercial and Census Data; Specialty Data; and Synthetic Data, derived from modeling of a range of political and demographic variables (www.Catalist.US/products). Another longstanding example is *Aristotle*, 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" (www.aristotle.com).

Howard and Kreiss (2010: 17-19) 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, both public and private.

We do know that the voter management software used by US 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. 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 preferences (Curry 2012). The published training materials on CIMS reveal that each voter is assigned a score of -15 to +15 on the basis of these data (see below). Walk lists, phone lists, e-mail lists, lawn sign allocations and other campaigning tools are then generated which then allow the party to more efficiently target voters, and thus use its human and financial resources to best effect to get-out-the-vote. It was reported that a new Conservative voter management system, entitled C-Vote, was scrapped in 2013, costing the party millions of dollars (Payton 2013). The Canadian Liberal Party has a similar "voter identification and relationship management system" called *Liberalist*, originally based on the Democrats' Voter Activation Network platform.

The main political parties in the UK have also operated voter management databases for several years, using similar proprietary software to their counterparts in the United States. They too augment the basic address information from the electoral roll with additional personal data on supporters and non-supporters alike (Amberhawk 2013). The Conservative Party originally used the "Voter Vault" software and now uses MERLIN (Managing Elector Relations through Local Information Networks) (Crabtree 2010). Since 2008, the Labour Party has operated a system called Contact Creator, and for the recent 2015 election also enlisted the assistance of the American company, Blue State Digital. Voter management databases have also been used in Australia for at least a decade (van Onselen and Errington 2004). In advance of the 2010 state election in Victoria, the *Melbourne Age* published details of the voter management database operated by the Australian Labor Party which then reportedly used software called "Electrac." The Liberal Party used a system entitled "Feedback" (Millar and Mackenzie 2010).

Evidence of similar voter management tools in other countries is spotty. In Europe, it would generally be regarded as illegal under data protection legislation to process sensitive data on political opinions and affiliations on people other than those who had explicitly signed up as members of, or who had regular contact with, established political parties. There are also important constraints imposed by wider electoral regulations and traditions. In many societies, the practice of individual communication and targeting is simply not regarded as culturally acceptable. 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 (Bennett 2013b).

More centralized database technologies are now giving way to more integrated platforms that provide parties with the full range of campaign tools. Commercially available "campaigns-in-a-box" offer more responsive and integrated instruments for an entire campaign operation, and are increasingly popular in several democratic countries. These tools include: website design and development; the set-up of Facebook, Twitter, YouTube, WhatsApp and other social media; the generation of geo-targeted lists for e-mail and texting; the management of volunteers; as well as the publication of more traditional campaign materials (bumper stickers, business cards, buttons, and so on). These services are intended to allow local campaigns to leverage the entire technology and communications infrastructure in one integrated "solution," freeing candidates and campaign managers for more important tasks.

As an example, one major company, Trailblazer, now advertises (www.trailblz.com):

> Every campaign tool you'll need to succeed is integrated into one easy-to-use platform. From targeting and tracking to voter outreach and messaging, we've got you covered. Trail Blazer's political campaign management software tools coordinate your entire political campaign or political action committee (PAC) or Super PAC.
>
> Our political campaign software tools track contributions and pledges, manage your volunteer's grassroots efforts, handle political campaign finances, coordinate GOTV and

> polling, generate walk lists and call lists, broadcast mass email, identify and target voters, increase political fundraising donations and file FEC compliance reports.
>
> Run your political campaign with easy-to-use targeting tools. With our political software, enjoy using a single database and keep your political campaign organized. No more rifling through Excel spreadsheets. Our powerful tools allow you to plan your tactics and strategy, drive voters to the polls and win your election.

Thus, centralized party databases may be a thing of the past. In this regard political parties are no different from any other public, non-profit or commercial organization that wishes to reach a target audience with its message.

From Mass Messaging to Micro-Targeting

As political parties and campaign organizations have been able to access an increasing volume and range of data on voters, so they have been able to target their messages more precisely. Rather than convey their messages to broad geographic or demographic communities, the availability of these data have facilitated the "micro-targeting" of more precise segments of the electorate. Increasingly, elections in many countries are fought over the votes of important swing voter groups in key districts or constituencies. Increasingly, the electorate is "sliced and diced" and messages tailored and targeted accordingly, and communicated through the individual's preferred communication medium.

Micro-targeting uses whatever individual-level information is available and combines it with demographic, geographic and marketing data about those individuals to build statistical models better to understand the attitudes and behaviors of voters. There is no precise time and place when micro-targeting emerged, although the 2004 re-election of President Bush, engineered by Karl Rove, is often cited as a watershed campaign (Delacourt 2013: 257). It also probably arose out of some necessity. With more voters having caller ID, unlisted numbers, or using cell phones as their primary method of contact, it has become increasingly difficult to reach potential voters through telephone polling to ascertain their voting intentions.

Ultimately, the micro-targeting of voters seeks to find so much about our individual preferences that campaigns can actually personalize messages and interact with and appeal to voters on an individualized basis. Segmentation, it is argued, "brings target voters alive" and permit campaigns to understand the particular voting groups necessary to win a particular election (Lees-Marchment 2011: 21). In the 2004 presidential election, for example, the Republicans targeted Hispanic females with children in New Mexico, believing that they would be responsive to President Bush's "no child left behind" message. New Mexico voted Democrat in 2000, and Republican in 2004 (Lees-Marchment 2011: 23). Many similar examples convinced political marketers that segmentation was the new way to win elections, and "micro-targeting" became the new buzzword.

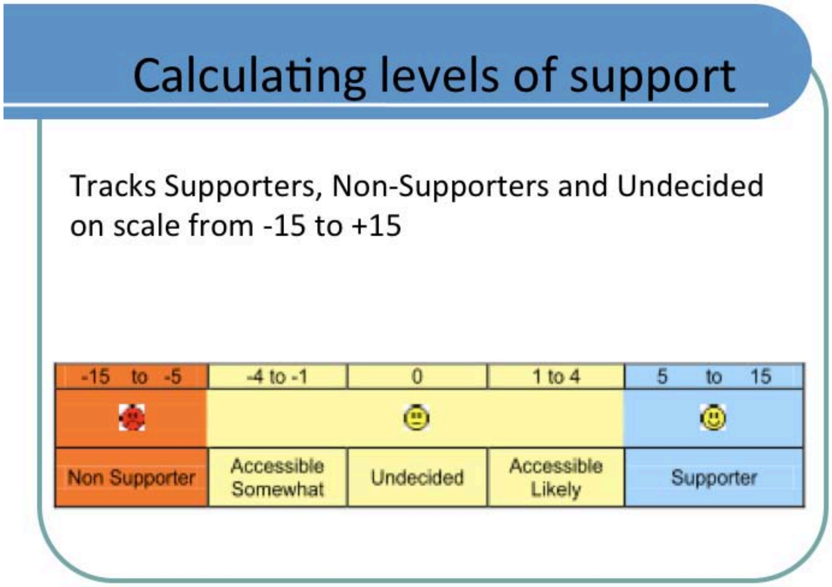
These techniques also belie some traditional assumptions about voter allegiances based on crude measures of income and class. They assume a crosscutting, multi-faceted and fragmented electorate, which might shift party allegiances if given the right message on the right issue. Simple "horse-race" journalism that focuses on who is the superior campaigner or strategist is also profoundly inadequate. As Sasha Issenberg wrote in a blog post in the New York Times before the 2012 US Presidential election (Issenberg 2012):

> Over the last decade, almost entirely out of view, campaigns have modernized their techniques in such a way that nearly every member of the political press now lacks the specialized expertise to interpret what's going on….It's as if restaurant critics remained oblivious to a generation's worth of new chefs' tools and techniques and persisted in describing every dish that came out of the kitchen as either "grilled" or "broiled."

As Issenberg (2013: 174) reports, however, most commercial marketing databases were too expensive and insufficiently tailored for political campaigns. Retail companies, for example, typically require a narrow range of variables in order to make a decision about where to locate a new store, or how to pitch a product. Political campaigns required more variables combined with politically relevant information gleaned from polls. Voter management databases needed, therefore, a higher level of expertise than those in the commercial world, as well as more computing power. These resources were only available to the most wealthy and national campaigns.

Such high level of precision can lead to the erroneous assumption that the model will tell you exactly whom to target. Rather, micro-targeting acts as a tool for prioritizing targets, and is, like all statistical models, inherently probabilistic. When a micro-targeting model is applied to a voter file, each voter gets a score giving the per cent likelihood that they exhibit the behavior or characteristic being modeled. These scores allow the campaign to focus their persuasion efforts on those voters most likely to be undecided, and to select particular communication strategies to as many individuals as the budget and campaign plan allows.

The following screenshot from the Conservative Information Management System (Conservative Party of Canada) in Canada shows how the Conservatives rate voters on a sliding scale of -15 to +15. Presumably the target voters for the Conservatives are the individuals graded in yellow in the middle of the scale. Phones, mail, e-mail and door canvassing can be targeted to the most appropriate target universes, saving the campaign money and delivering the campaign's messages to the most receptive audiences.



Calculating levels of support

Tracks Supporters, Non-Supporters and Undecided on scale from -15 to +15

-15 to -5	-4 to -1	0	1 to 4	5 to 15
☹	😐			☺
Non Supporter	Accessible Somewhat	Undecided	Accessible Likely	Supporter

This example is, however, dated and static. Increasingly campaign information might be supplemented by the purchase of information from commercial databases through which parties are able to perform far more sophisticated cluster analysis on the data based on geo-demographic neighborhood classification systems. Marketers tend to assume that people with similar cultural backgrounds, means and perspectives naturally gravitate toward one another to form relatively homogeneous communities. Once settled, people emulate their neighbors, adopt similar social values, tastes and expectations and, most important of all, share similar patterns of consumer behavior toward products, services, media and promotions. This behavior is the basis for the development of classification systems such as the PRIZM lifestyle classification from Environics, through which one can look up a postal code and find the dominant social group in that neighborhood: “Startups and Seniors” or “Grey Pride” or “Single City Renters” (Environics Analytics 2015). Political parties in the US and Canada thus tweak these data to fit political categories, and draw inferences about what policies such groups might be interested in hearing about (Delacourt 2013: 258).

Most of these data are purchased in aggregate form and tend not, therefore, to raise alarms about privacy issues. In the US, where few privacy protection laws govern the personal data brokerage industry, campaigns can purchase more personalized marketing lists, from which quite precise inferences might be drawn about political affiliation. 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 (Issenberg 2013). In the United States, the merging of such consumer files with publically available voter information files is generally legal; elsewhere it is not.

Social Media, the Social Graph and Targeted Sharing

Parties in many countries are becoming increasingly adept at using social media to target messages, recruit volunteers and donors and track issue engagement. Social media can provide a far cheaper way to communicate to a larger audience than more traditional broadcast methods. The use of Facebook, Youtube, Twitter, Flickr, Google+ and other social media is now a commonplace feature of political campaigns in most Western democracies. WhatsApp has also become particularly popular in countries such as India (Gupta 2014). Political parties, like commercial organizations, do not need to actively monitor behavior. They can sweep up the wealth of “user-generated” content, that individuals “voluntarily” upload to social media platforms, and draw inferences, connections and conclusions using contemporary “big data” analytical techniques (Mayer-Schönberger and Cukier 2013).

In the political world, it is also commonly recognized that social media are not a replacement for traditional communications but additive, and need to be fully integrated into the wider communications strategy of a campaign (Small 2010). Politicians know that a large social media following can lend credibility to their campaigns. Just as a packed town meeting can add to the perception that a candidate is worth following, the same holds true for social media. Conversely, of course, an empty meeting or few followers can demonstrate weakness. So there is a powerful motivation to drive these “vanity metrics” higher, simply because it looks good. They can also, of course, be artificially manipulated by “social robots” or “bots” that can increase or decrease likes, dislikes, fans, followers and friends (Bilton 2014).

A basic count of Twitter followers, or Facebook ‘Likes’ will not tell much in isolation, and having lots of Facebook friends or Twitter followers does not necessarily translate into political support. Other analytics are more valuable and are relatively easy to track. Colin Delany of epolitics.com advises attention to the following questions (Delany 2014): “Who’s following you? (Follow up questions: Do you recognize them? Are they in your district? Are they “influencers” you’re trying to reach?); Is your following increasing, decreasing, or holding steady? What’s the trend over time? Are people interacting with your content? On Facebook, are they Liking/Commenting/Sharing? On Twitter, are they re-tweeting your info or replying to it? Which of your posts are generating activity on Facebook or Twitter? Certain issues? Particular kinds of content, for instance photos/images vs. links to articles?”

In most cases, social networking is still used as a “push technology” where the audience is a passive subject receiving messages at the discretion of those social media sites being “followed” (Small 2010). There is the perennial problem of how to translate the relatively quick and superficial actions in a social media environment into behavior in the real political world—voting, donating, volunteering and communicating the message. The transition from the “slacktivism” into real effort is not just a problem for the electoral campaign. There is plenty of evidence that the relative ease of online activist behavior can appease our consciences but actually reduce the likelihood of real effort and real engagement (Kristofferson, White and Peloza 2014).

The transition from a social media environment to action in the offline world also tends to cut against the business models of the social networking companies who want to keep their users interacting within those online environments for as long as possible. We are enticed through fully compatible applications to remain within the "Google world" or the "Facebook world" for the vast majority of our needs. One solution lies in the integration of customizable applications that work within the Facebook platform, making it easier for an individual, with the click of a mouse, to donate, join an e-mail list, sign petitions, sign up for events, or volunteer. A contemporary example is *Actionsprout*, a "platform for social action" which allows users to develop e-mail lists through Facebook and more effectively target fundraising or advocacy efforts (www.actionsprout.com).

The ultimate goal is for campaigns to have full access to the "social graph" by, for instance, tapping Facebook supporters' social connections and by comparing their "friend" lists with the wider voter databases. There are several products currently being tested. The Democratic firm NGP VAN has pioneered a Social Organizing Application for this purpose providing clients with the ability to match their Facebook friends to the voter file as they take part in everyday campaign activities like voter identification and persuasion, grassroots fundraising, crowd building, volunteer recruitment, and get-out-the-vote activities. NGP VAN has reportedly developed a new and more sophisticated tool called "Recruiter" in time for Hillary Clinton's 2016 Presidential election campaign (Fung 2014). Another company, *NationBuilder*, increasingly popular in the US and Canada, is an inexpensive community-organizing tool, which is now used by individual political candidates at local levels for campaign outreach and communications, thus by-passing party organizations (www.nationbuilder.com).

The analysis of a user's social graph can lead to what 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 5 million contacts that potentially saw each other registering to vote, giving money, sharing videos on the campaign, and voting on or before Election Day. And, when matched against other voter files, were prioritized for further contact.

A larger shift in campaign logic underlies many of these new trends, namely that voters are more likely to be persuaded if they see their peers supporting a particular party or candidate (Issenberg 2013). Polling evidence suggests that voters, and particularly young voters, do not trust parties or media organizations, but they are more likely to be influenced by the attitudes and behavior of those in their peer groups. Scientific studies have also 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).

In the social networking environment, the monitoring of voters by political parties is deeply dependent upon the corporate policies and technical standards and defaults of the social media platforms they use. These practices are varied and fluctuating (see: www.catsmi.ca), and to differing extents, these sites encourage the sharing of personal information. For instance, "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 listed on the parties' social media page. 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 Decentralization of Campaigning through Mobile Applications

The explosion in the use of mobile applications designed for the new generation of smartphones and tablets, often integrated with social media, build upon these existing trends. These technologies are altering the dynamics of modern campaigning and providing new and potentially more intrusive ways to broadcast relevant political information, to influence voters' attitudes and behavior, to encourage campaign donations, and to engage networks of potential supporters. The combination of mobile apps with the technologies described above will probably have the effect of decentralizing many campaign operations. It is difficult to classify an inherently dynamic marketplace, but it appears that in recent election cycles, mobile apps have been used for: more traditional one-way political messaging; for door-to-door canvassing; for event management; for encouraging donations; and for broader civic engagement.

The vast majority of mobile political applications are one-way means of broadcasting and re-broadcasting political messages. In addition to the applications embedded within social media platforms, major party candidates in many countries have developed their own smartphone apps to promote their campaigns to this growing audience of smartphone owners. The simple use of these apps for "push notifications" allows candidates to keep voters up-to-date with latest campaign activities, and often contain built-in templates that allow supporters to share those messages with friends and family. These applications are used as much by individual candidates, as by political parties, further accentuating the personalization of political campaigns, and the greater emphasis on the more "presidential" qualities of leaders in parliamentary systems.

Mobile applications have also been developed for canvassing. A typical example is the "Footwork app" which integrates geo-positioning software to plan routes for campaign workers, and to deliver metrics to campaign headquarters about doors knocked on, time in the field, distance walked and so on. Information conveyed during doorstop conversations can also be entered in real time and conveyed to party databases (www.gofootwork.com). These applications also operate as tools to monitor the efficiency of the campaign workers themselves, encouraging competition for higher and higher levels of voter contact.

The 2012 Obama campaign went one step further, integrating its mobile canvassing application with existing voter information from its database to reveal first name, gender, age and party affiliation of the voter directly on the smartphone of the party worker. This application raised some serious questions about whether or not temporary campaign volunteers should be having such direct access to information on political affiliation. Voter registration data is public in the United States and traditionally available to anybody in a campaign office. Critics questioned whether or not this distribution of voter-related data constituted a qualitative difference that crossed an important threshold and violated peoples' reasonable expectations of privacy (Beckett 2012).

Donating is also becoming quicker and more decentralized. Blue State Digital now integrates a "Quick Donate" feature through mobile e-mail or SMS. Thus an indication of support for a campaign or issue can trigger an immediate response with a "quick donate" button typically preprogrammed for a small amount. This is a way to reduce complex forms and extra keystrokes (http://tools.bluestatedigital.com/pages/quick-donate).

A product called 5ive Points gamefies the campaigning experience. The 5ivepoints mobile campaigner lets any campaign have a mobile app for voter identification, and for geo-located door-to-door canvassing, phone calls, and event check-ins. The company boasts that its products turn the average supporter into "casual campaigners" to add voters wherever you meet them. It provides the ability to "see voters all around you," and share your findings with others through Facebook, Twitter and other social media. And all this is gamefied through a point system, where the goal is to find more voters with +5 scores than your fellow campaigners. Campaign managers in real time can monitor all this activity. "App the Vote" is the company's rally call (www.5ivepoints.com).

In summary, mobile applications seem to have spread throughout the political world with extraordinary speed, and for a number of purposes. Their development raises similar questions about privacy to those adopted in the wider commercial world, and how personal data, such as contact lists, photos and location data, can easily be disseminated without the user's knowledge or consent. The rapid development and dissemination of mobile applications has increased the complexity of the problem and multiplied the range of players who might be able to access personal information, including developers, service providers, app platforms, and advertisers. The assumption of legal responsibility for privacy in this complex and rapidly evolving ecosystem is complicated within a mobile environment characterized by smaller devices. The international privacy community has continually been struggling with how to reach users with the right information about their privacy rights, how to encourage technical design that makes privacy the default option, and how to motivate the major social media platforms to build privacy requirements for applications into their contractual requirements (Office of the Privacy Commissioner of Canada 2012).

In the political world, mobile applications offer an extraordinary potential for inappropriate collection and use of personal data without expressed consent. Sensitive data about political affiliations can be put in the hands of multiple volunteers and campaign workers, who may have no privacy or security training. In a world where data breaches are commonplace and daily occurrences, the decentralization of voter intelligence data could be a disaster waiting to happen.

Voter Surveillance and Political Behavior

It is tempting to conclude that the practices outlined above 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, candidates 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 (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, at least in the United States and probably elsewhere as well.

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 decline of the class attachments to parties that had characterized the industrial era. The trends are by no means uniform, and the causes are hotly contested.

One of the implications of "parties without partisans" (Dalton and Wattenberg 2002) is that political parties have needed to find other and newer ways to engage with the electorate to find donors, volunteers and members. They cannot rely on huge proportions of the voting public based on conventional class or religious identities. Voter surveillance techniques have arisen, therefore, partly to address this fundamental shift in partisan allegiances. 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 (Delacourt 2013).

The nature of political parties has therefore changed. The conventional distinctions were provided by Maurice Duverger (1963) 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 the franchise was extended throughout the late 19th and 20th 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 (Kircheimer 1966). These parties 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. 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 US democratic politics since the early 20th 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 helped elevate 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, however, 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 2012. Based on the Italian experience of 2005 and 2007, the 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 were willing to donate a nominal sum of one euro to the party.

Protests were raised regarding the primary's constitutionality, the legitimacy of employing public facilities for a "private" election, as well as the legality of using electoral lists for an internal party process.

Primary elections also pose some peculiar and novel challenges for privacy principles, and data protection authorities. Information on political affiliation is considered "sensitive" data under all European data protection legislation, and may only be processed with explicit consent. In practice, therefore, the processing is confined to members, former members or others who have a regular contact with the party (Bennett 2013b). They may not, therefore, build the kinds of general voter management databases common in North America. The French data protection agency (the Commission Nationale de l'Informatique et Libertés) 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 Garante 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 and elsewhere, they will continue to raise interesting issues about the appropriate balance between parties' rights to association and the privacy rights of voters. I have argued elsewhere that other practices will also place an enormous stress on the system of data protection regulation in European countries (Bennett 2013b).

There is, therefore, a range of analytical and comparative questions about trends in party systems, voting behavior and electoral practices that need further research. The extent to which voter surveillance will be engaged in is, at one level, related to structural conditions, legal requirements and cultural practices within different countries. Beyond these more empirical questions lies a range of normative issues about the implications of these trends for democratic politics. The concluding section is suggestive of these wider theoretical concerns.

Conclusion: Voter Surveillance and Democratic Theory

It is widely assumed that surveillance and democracy lie at opposite ends of a normative continuum (Haggerty and Samatas 2010: 1). Despite the insistence from Lyon (2001) and others that it should be framed in neutral terms, surveillance still assumes a place in the popular consciousness as a negative force that compromises those freedoms upon which democratic societies are founded, including privacy, and freedom of speech and association. Surveillance seeks to render individual behaviors and preferences transparent in ways that make them conform to pre-existing categories and norms. It inspires conformity, control, and obedience. It discourages the individualism, autonomy, and creativity that democracy requires and thrives upon. As Paul Schwartz remarks, surveillance has "a negative impact on individual self-determination; it makes it difficult to engage in the necessary thinking out loud and deliberation with others upon which choice-making depends (1999: 1701).

The anti-democratic nature of surveillance is reinforced by the prevalence of Orwellian and Kafaesque metaphor and imagery. Various symbols have been used over the years to equate excessive surveillance with the slippery slope to authoritarian repression. That message is continually reinforced by a network of privacy activists that engage in a symbolic politics to create awareness and expand their networks (Bennett 2008: 106-7). We are currently in the middle of a wide-ranging international debate about the appropriate role for security and intelligence services in the wake of the revelations from National Security Agency whistle-blower Edward Snowden. The bewildering range of surveillance programs initiated without appropriate accountability and oversight by the National Security Agency, and its sister organizations in the "Five-Eyes" countries, are generally challenged because of their fundamentally anti-democratic nature (Greenwald 2014).

If it were discovered that the NSA had backdoor access to the kind of voter management databases described above, then similar denunciations would no doubt occur and be justified. Thus, it is not difficult to find arguments that the practices described above are also, fundamentally undemocratic, or even anti-democratic. These tactics might be criticized for their tendency to treat citizens as unthinking consumers, ready to respond with their votes in the same way that they respond with their money. Micro-targeting divides us into niche markets and avoids the hard work of building consensus and national visions. It arguably creates parties and candidates that do not convey a general ideological framework for governance, but a series of carefully chosen, focus-group analyzed, messages to key segments of the electorate in key marginal districts. This messaging need not be internally consistent, nor framed within a larger set of policy ideas. Thus parties only need to mobilize key voters in key places; and if the votes of others are suppressed, then so be it. In her analysis of these trends in Canada, Delacourt (2013: 328) concludes: "Instead of turning consumers into citizens, it has accomplished the reverse. Canadian politics went shopping for votes, and the voters went shopping." The science of "winning elections" may have the effect of turning people off the political process.

A critical response to voter surveillance, and the consumerization of the political, would contend that the practices surveyed above discourage engagement and deliberation, in favor of the increasing individualization of political space in which we are assumed to have preferences and tastes that only need to be unearthed using the most sophisticated technology to determine what public policies and goods voters "want": a tax break here; a subsidy there; an improvement to the local school; a clean-up of the neighborhood lake; and so on. Thus the critique of voter surveillance might sit comfortably within a broader critique of neo-liberal governance and of the shrinking public sphere.

The argument is more complex, however. Political parties have a responsibility to mobilize and educate supporters. In so doing, they attempt to promote higher levels of participation and engagement in the political process. Voter surveillance practices have, in part, emerged as a response to the failures of traditional and crude forms of mass messaging through television. Arguably parties can encourage more people to vote and reinforce voters' agency, if they know more about their beliefs and preferences. There may be some evidence that the 2008 and 2012 presidential campaigns in the United States, the first to be waged with the full range of new media technology to reach voters of all demographic and socio-economic characteristics did, indeed, have a small, but noticeable impact on participation rates and voter engagement, particularly among the younger "millennial generation" (Hendricks and Kaid 2011).

There will continue to be debate about the extent to which the increase in voter turnout in these elections, and among this age group, is attributable to new media and micro-targeting, but the point remains that voter surveillance is not necessarily anti-democratic. At least, the public interest on the other side of the equation is different. The balance is not between the privacy interest and security, nor between privacy and the profit-motive. Instead, we confront a rather different set of interests that need careful consideration and weighing before condemning or regulating the ways that candidates and parties capture data on citizens and use that information to encourage political engagement and participation. Those issues have not been thoroughly analyzed in democratic theory, nor subjected to rigorous empirical examination in different states with different legal requirements and electoral tradition.

At root the contestation of values is reflected in two broad and rich traditions of democratic theory. The first is a liberal vision, which sees the main test of democracy as a representative system, based on majority rule but with established constitutional protections for minority and individual rights. Privacy has tended to be regarded and justified within a broad liberal paradigm (Bennett and Raab 2006) and plays an important role within liberal democratic theory because it: prevents the total politicizing of life; promotes the freedom of association; shields scholarship and science from unnecessary interference by government; permits the use of a secret ballot; restrains improper police conduct such as compulsory self-incrimination and unreasonable searches and seizures; and it serves also to shield institutions, such as the press, that operate to keep government accountable (Westin 1970: 25). So, under this dimension, privacy is protective of individuals and specific organizations from obtrusive invasions that would detrimentally affect their ability to participate in politics or go about daily life.

A second broad tradition sees the test of democracy less in the protection of rights, and more in the participation of a citizenry to take charge of its own affairs. As the liberal democratic tradition has been strained under increasing levels of partisan de-alignment and voter apathy, so scholars have renewed interest in a more "participatory" forms of democratic practice (Pateman 1970). If one creates a more participatory environment, people will be more prepared for the tasks of self-government. Engagement in social and community institutions raises the stock of "social capital" (Putnam 1993), levels of interpersonal trust, and the ability of individuals to translate the "I" into the "we." As Pateman argues: "individuals learn to participate by participating" (2012: 15).

There may be, however, a less critical response to voter surveillance, which sees the attempt to discover preferences and patterns as a more benign, efficient and legitimate way to reach voters and connect with them about public policy. The conversation on the doorstep, over the phone, or in the social media environment, *can* therefore be more in tune with what voters perceive and desire. Thus, voter surveillance, like surveillance more generally, is "Janus-faced" (Lyon 2001). It at least requires us to analyze and judge its complex dynamics according to a different set of criteria than those used when we evaluate the security practices of the state, or the profit-driven consumer monitoring by the private sector.

References

Amberhawk Training Ltd. 2013. "Could the Conservative Party's Electoral Database breach the Data Protection Act?" Accessed May 20, 2015: 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.

Beckett, Lois. 2012. "Is your neighbor a Democrat? Obama has an App for that," *Propublica*, August 3, 2012. Accessed May 20, 2015: http://www.propublica.org/article/is-your-neighbor-a-democrat-obama-has-an-app-for-that

Bennett, Colin J. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance.* Cambridge, MA: MIT Press.

———. 2013a. "Data Point: What Political Parties Know about You." *Policy Options* 34 (2) (February): 51-53.

———.2013b. "The politics of privacy and the privacy of politics: parties, elections and voter surveillance in Western democracies." *First Monday* 18 (8) August 5, 2013. Accessed May 20, 2015: http://firstmonday.org/ojs/index.php/fm/article/view/4789

Bennett, Colin J. and Robin M. Bayley. 2012. *Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis*. Ottawa: Office of the Privacy Commissioner of Canada. Accessed May 20, 2015: http://www.priv.gc.ca/information/research-recherche/2012/pp_201203_e.asp

Bennett, Colin J. and Charles D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective.* Cambridge, MA: MIT Press.

Bennett, Colin J. Kevin D. Haggerty, David Lyon and Valerie Steeves, eds. 2014. *Transparent Lives: Surveillance in Canada.* Athabasca: Athabasca University Press.

Bilton, Nick. 2014. "Social Media Bots Offer Phony Friends and real Profit," *The New York Times*, November 19, 2014. Accessed May 20, 2015: http://www.nytimes.com/2014/11/20/fashion/social-media-bots-offer-phony-friends-and-real-profit.html?_r=0

Bond, Robert M., 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* 489 (September 13): 295-298.

Crabtree, James. 2010. "David Cameron's Battle to Connect." *Wired Magazine*, March 24, 2010. Accessed May 20, 2015: http://www.wired.co.uk/magazine/archive/2010/04/features/david-camerons-battle-to-connect.

Commission Nationale de l'Informatique et Libertes (CNIL). 2012. *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.* Accessed May 20, 2015: http://www.cnil.fr/documentation/deliberations/deliberation/delib/259.

Conservative Party of Canada. Undated. *CIMS and Your Campaign*. Accessed May 20, 2015*:* www.thestar.blogs.com/files/cims.ppt.

Curry, Bill. 2012. "Robo-call furor focuses attention on massive Tory database." *The Globe and Mail*, February 29, 2012. Accessed May 20, 2015: http://www.theglobeandmail.com/news/politics/robo-call-furor-focuses-attention-on-massive-tory-database/article4092455/.

Dalton, Russell J. and Martin P. Wattenberg. 2002. *Parties without Partisans: Political Change in Advanced Industrial Democracies.* Oxford: Oxford University Press.

Dalton, Russell J. 2004. *Democratic Challenges, Democratic Choices: The Erosion of Political Support in Advanced Industrial Democracies*. Oxford: Oxford University Press

Davies, Phillip J. and Bruce I. Newman, eds. 2012. *Winning Elections and Political Marketing.* London: Routledge.

Delacourt, Susan. 2013. *Shopping for Votes: How Politicians Choose Us and We Choose Them*. Madeira Park: Douglas and McIntyre.

Delany, Colin. 2014. *How political campaigns and advocates can use social media data.* Accessed, May 20, 2015: http://www.epolitics.com/2014/01/14/how-political-campaigns-and-advocates-can-use-social-media-data/.

Duverger, Maurice. 1963. *Political Parties: Their Organization and Activity in the Modern State*. New York: Wiley.

Environics Analytics. 2015. *Lifestyle, Marketplace and Values Information*. Accessed May 20, 2015: http://www.environicsanalytics.ca/environics-analytics/home.

Fung, Brian. 2014. "Democrats' latest tech mines your relationship data." *Washington Post* July 25, 2014. Accessed May 20, 2015: http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/25/democrats-latest-tech-mines-your-relationship-data.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA and the U.S. Surveillance State.* New York: Metropolitan Books.

Gupta, Hita. 2014. "What election campaigns in India say about marketing on WhatsApp." *Digital Market Asia,* October 16, 2014. Accessed May 26, 2015: http://www.digitalmarket.asia/what-election-campaigns-in-india-say-about-mktg-on-whatsapp

Haggerty, Kevin D. and Richard V. Ericson, eds. 2006. *The New Politics of Surveillance and Visibility.* Toronto: University of Toronto Press.

Haggerty, Kevin D. and Minas Samatas, eds. 2010. *Surveillance and Democracy.* New York: Routledge.

Hendricks, John Allen and Lynda Lee Kaid. 2011. *Technopolitics in Presidential Campaigning: New Voices, New Technologies and New Voters.* New York: Routledge.

Howard, Philip N. 2006. *New Media Campaigns and the Managed Citizen.* Cambridge: Cambridge University Press.

Howard, Philip N. and Daniel Kreiss. 2010. "Political parties and voter privacy: Australia, Canada, the United Kingdom, and United States in comparative perspective." *First Monday* 15 (12), 6 December 2010. Accessed May 20, 2015: http://firstmonday.org/ojs/index.php/fm/article/view/2975/2627H

Issenberg, Sasha. 2012. "Why campaign reporters are behind the curve." *New York Times* blog (September 1, 2012) at: http://campaignstops.blogs.nytimes.com/2012/09/01/why-campaign-reporters-are-behind-the-curve/?_php=true&_type=blogs&_r=0.

———. 2013. *The Victory Lab: The Secret Science of Winning Campaigns.* New York: Random House.

Italy, Garante per la protezione dei dati personali, 2012. *Elezioni primarie 2012 e trattamento di dati personali.* October 2012. Accessed May 20, 2015: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2079275

Judd, Nick. 2013. "Republican Party's Technology Revival Hopes Hinge on Data and Data Analysis." *TechPresident*, February 7, 2013. Accessed May 20, 2015: http://techpresident.com/news/23479/republican-partys-technology-revival-hopes-hinge-more-just-skype

Kircheimer, Otto. 1966. "The Transformation of Western European Party Systems." In: *Political Parties and Political Development*, eds Joseph LaPalombara and Myron Weiner, 177-200. Princeton, NJ: Princeton University Press.

Kristofferson, Kirk, Katherine White and John Peloza. 2014. "The Nature of Slacktivism: How the Social Observability of an Initial Act of Token Support Affects Subsequent Prosocial Action." *Journal of Consumer Research* 40 (6) (April): 1149-1166.

Lees-Marchment, Jennifer. 2011. *The Political Marketing Game*. Basingstoke: Palgrave Macmillan.

Lees-Marchment, Jennifer, Jesper Stromback and Chris Rudd eds. 2009. *Global Political Marketing*. London: Routledge.

Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life.* Buckingham: Open University Press.

———. 2007. *Surveillance Studies: An Overview.* Cambridge: Polity Press.

Mayer-Schönberger, Viktor and Kenneth Cukier. 2013. *Big Data: A Revolution that will Transform how we Live, Work and Think.* New York: Houghton, Mifflin, Harcourt.

Millar, Royce and Nick Mackenzie. 2010. "Revealed: How the ALP keeps secret files on Voters." *The Age* (November 13). Accessed May 20, 2015: http://www.theage.com.au/victoria/state-election-2010/revealed-how-the-alp-keeps-secret-files-on-voters-20101122-1845e.html.

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

Office of the Privacy Commissioner of Canada (OPC). 2012. *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps.* Ottawa: OPC, October 2012. Accessed May 20, 2015: https://www.priv.gc.ca/information/pub/gd_app_201210_e.asp.

Pateman, Carole. 1970. *Participation and Democratic Theory.* Cambridge: Cambridge University Press.

———. 2012. "Participatory Theory Revisited." *Perspectives on Politics* 10: 7-19.

Payton, Laura. 2013. "Conservative campaign database fiasco costs party millions." *CBC News* (October 23, 2013). Accessed May 20, 2015: http://www.cbc.ca/news/politics/conservative-campaign-database-fiasco-costs-party-millions-1.2187603.

Putnam, Robert. 1993. *Making Democracy Work: Civic Traditions in Modern Italy.* Princeton, NJ: Princeton University Press.

Sherer, Michael. 2012. "Friended: How the Obama Campaign Connected with Young Voters." *Time Magazine*, November 20, 2012. Accessed May 20, 2015: http://swampland.time.com/2012/11/20/friended-how-the-obama-campaign-connected-with-young-voters/.

Schwartz, Paul. 1999. "Privacy and Democracy in Cyberspace." *Vanderbilt Law Review* 52: 1609-1702.

Small, Tamara. 2010. "Canadian Politics in 144 Characters." *Canadian Parliamentary Review* 42: 39-45.

Trailblazer. 2015. *Powerful Software for Political Campaigns, PACs and Super PACS.* Accessed May 20, 2015: http://www.trailblz.com/Political-Campaign-Software/default.aspx.

van Onselen, Phillip and Wayne Errington. 2004. "Electoral Databases: Big Brother or Democracy Unbound?" *Australian Journal of Political Science* 39 (2): 349-366.

Westin, Alan F. 1970. *Privacy and Freedom* New York: Atheneum.