Data Point

What political parties can learn about you...and why robo-calls may be yesterday's scandal.

The ongoing furor about apparent abuse of robo-calls in the last federal election has raised wide concern about the impact of new technologies on election campaigns. The Chief Electoral Officer is expected to report to Parliament this spring on how to respond to the increasing ability of political parties to harness data technology for their own ends. And, as the following articles show, the rise of data based campaigns raises questions that go far beyond the relatively clunky technology of robo-calls.

WHAT POLITICAL PARTIES KNOW ABOUT YOU

COLIN J. BENNETT

Canadian political parties are gathering more and more data on voters all the time. It's time we regulated what data they glean, and what they can do with it.

Les partis politiques accumulent un nombre grandissant de données sur les électeurs canadiens. Il est temps de réglementer la cueillette de ces données et l'utilisation qui en est faite.

The allegations of vote suppression through the practice of robo-calling using automatic dialing and announcing devices during the last Canadian federal election campaign has raised troubling questions about the impact of technology on the way political parties conduct modern campaigns. Both the RCMP and Elections Canada are conducting investigations, and Parliament has resounded with partisan denunciations and denials of wrong-doing. But the rise of robo-calling is merely the tip of the data revolution that is raising deeper questions about what information our political parties actually know about voters, how they collect it, and what they do with it.

The recent US election cycle revealed the extent and sophistication of personal data mining and profiling by political campaigns as never before. The modern political consultant's arsenal includes smartphone applications for political canvassers. It boasts integrated platforms such as NationBuilder or Google's Political Campaign Toolkit that provide campaign Web sites, e-mail services, "social customer relationship management," and fundraising software. Targeted e-mail and texting campaigns match IP addresses with other data sets showing party affiliation, donation history, and socio-economic characteristics.

Campaigns now extensively use both "robo-calling" and "robo-texting." And no political strategy is complete without the use of social media to plan campaigns, target likely voters and donors, and measure the impact of policies and advertising on engagement.

Some of these data are gathered from the conscious activities of individuals. Others are gleaned surreptitiously from the digital trails that people leave through their various online activities. Reports suggest that there were no fewer than 76 different tracking programs on barackobama.com. The capture of personal data by political parties is no longer self-generated, obvious or consensual.

Surveillance during Canadian elections has been less extensive and intrusive — so far. Canadian parties and candidates have a minute fraction of the resources that are available to their American counterparts to fund the same degree of data collection. Nor do they have the same ease of opportunity to gather it. In the US, parties play a central role in registering voters for both primary and general elections.

But Canadian political consultants are always drawing lessons from south of the border, and it is not unusual for the latest campaign techniques to filter north. Furthermore, these new integrated campaign technologies can be easy to use, and cost far less than the more traditional and labour-intensive methods of acquiring information by going door-to-door.

The 2011 robo-call scandal was not the first time that privacy issues involving Canadian political parties have surfaced. A string of incidents over the last decade raises troubling, if subtly different, issues about the ways that parties and politicians use personal data for political purposes.

In 2006, Conservative Party MP Cheryl Gallant sent birthday cards to her constituents using data from passport applications, an incident that was later investigated by the Office of the Ethics Commissioner. The same year, the RCMP found lists of voter names and addresses in the office of a Toronto cell of the Tamil Tigers, a group classified as a terrorist organization. In October 2007, the Prime Minister's Office

Colin J. Bennett is a professor at the Department of Political Science, University of Victoria. www.colinbennett.ca.

sent Rosh Hashanah cards to supporters with Jewish sounding names, many of whom were unsettled and left wondering how such a list could be compiled.

During the 2011 election, a Conservative candidate from Winnipeg mistakenly sent a misdirected e-mail containing the names, address, phone numbers and e-mails of 6,000 of her constituents to a local environmental activist during the 2011 federal election. And in the same year, about 10,000 people signed a petition addressed to Jason Kenney and his ministry, Citizenship and Immigration Canada, demanding that a young gay Nicaraguan artist who was facing deportation be allowed to stay in Canada. Kenney later sent out an e-mail to those who had signed the petition, extolling what the government of Canada has been doing to promote "gay and lesbian refugee protection." Many in the gay community were startled that a federal minister had their contact information at his disposal.

All these cases occurred in an uncertain legal and ethical environment. Elections Canada responded to the robo-call incidents with a discussion paper on "Issues Arising from Improper Communications with Electors," and the Chief Electoral Officer is to make recommendations to Parliament in March of this year. The Federal Privacy Commissioner, Jennifer Stoddart, lacks the jurisdiction under Canada's privacy laws to act. But Stoddart did commission Robin M. Bayley and me to conduct a study of the issues. Our analysis appeared in a report, "Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis," which outlined the vast quantity and variety of information processed by federal parties on voters, donors, members and supporters.

The main federal parties now administer extensive voter management systems: the Conservative Information Management System (CIMS); Liberalist; and NDP Vote. The foundation for these databases is the electoral list provided under the authority of the *Elections Act* by Elections Canada. Upon this framework, a range of other data about voters is added and analyzed. These data come from a variety of sources: telephone polling, traditional canvassing methods, petitions, letters, commercially available geo-demographic and marketing databases, and the analysis of online behaviour, including social media. Overall, however, the contents of these systems are shrouded in secrecy.

Privacy risks come in a number of forms. First, there is the careless handling of personal data resulting in data breaches. Every other kind of public and private organization in Canadian society has experienced the embarrassment and cost (both financial and reputational) of a data breach. The costs of a serious data breach to a political party during an election campaign would be incalculable.

A second area of concern is the nonconsensual capture and use of personal data for campaigning. For example, the Liberal Party of Canada has already announced that it will be using a new smartphone application that canvassers can use to record the results of conversations on the doorstep. Would the average voter reasonably expect that these conversations might be transmitted to central party databases? And then there is the uneasy fear that personal information communicated to MP's constituency offices might filter into party databases. This should not happen, and the parties have stated that it does not happen. But the technology makes it increasingly easy to breakdown any firewalls.

PHOTO: ISTOCK

Parties also undertake analysis of the social circles apparent through Facebook to broaden the range of potential supporters and targets for campaigning. Do people who "like" a party realize that this will be entered on a database and result in their being labelled as a supporter and targeted for fundraising and get-out-the vote efforts?

A third area relates to intrusions through telemarketing. Policical parties are generally exempted from the national do-not-call list administered by the CRTC, and none of the Web sites of the major political parties provide any mechanism through which individuals can register on these lists to avoid a potential barrage of political solicitation. Most voters have to take extraordinary initiatives to avoid intrusive calls.

Canadian privacy protection laws and federal and provincial privacy commissioners are more comprehensive than those in the US. But no commissioner (with the possible exception of the Office of the Information and Privacy Commissioner of British Columbia) has jurisdiction over the personal information captured by political parties. Parties do not engage in much commercial activity and are therefore largely unregulated under the 1999 *Personal Information Protection and Electronic Documents Act* (PIPEDA), or similar provincial laws. Political parties are not government agencies, and therefore remain unregulated by the 1983 *Privacy Act*.

The only federal law that governs their practices is the *Canada Election Act*, but this legislation only applies to voter registration data collected and shared with parties and candidates under the authority of that legislation. Parties are also exempt from the new anti-spam legislation (C-28).

Thus, for the most part, individuals have no legal rights to learn what information is contained in party databases; to access and correct those data; to remove themselves from the systems; or to restrict the collection, use and disclosure of their personal data.

And for the most part, parties have no legal obligations to keep that information secure, to only retain it for as long as necessary, and to control who has access to it.

Virtually every other public or private organization in Canada must abide by these basic rules. Why should political parties be any different? Some argue that because political parties play a crucial role in democracy, they should have access to personal information in order to mobilize and educate voters. These important civic responsibilities, they claim, outweigh the arguments for regulation, and voluntary self-regulation by the parties will suffice.

As our report demonstrates, however, from the point of view of an ordinary supporter or contributor who wishes to exercise control over his or her personal information, the existing voluntary privacy commitments of Canada's main federal parties are often difficult to find, inconsistent and vague. There is little evidence that any federal party (with the possible exception of the Green Party) has given sustained consideration to privacy and to the risks associated with amassing vast amounts of personal data in centralized databases.

There is no link to privacy on the homepages of either the Liberal Party of Canada or the New Democratic Party. The link on the Conservative Party Web site is more prominent, but the policy is incomplete and replete with vague assertions and exemptions. Parties are also supposed to operate internal do-not-call lists. The process for getting on these lists is rarely publicized.

Canadian federal political parties need to be brought within the statutory requirements of PIPEDA, and therefore under the authority of the Privacy Commissioner of Canada. But on the assumption that politicians are going to be reluctant to regulate themselves, far more can be done to make self-regulation work. All political parties should

- revise their privacy policies based on the 10 privacy principles upon which PIPEDA is based, and publish them more prominently;
- appoint a responsible official (the equivalent of a chief privacy officer) who has overall responsibility for the collection, use and dissemination of personally identifiable information;
- more effectively operate their internal do-not-call lists;
- train staff and volunteers on privacy and security issues; and
- adopt appropriate risk management strategies in the case of a data breach.

This process of self-regulation could, of course, be jointly agreed as a common code of ethics. An accredited third party could certify compliance with this code. Obtaining a certification could also be a condition of receiving the list of electors from Elections Canada.

The implications of these concerns go beyond the well-known risks associated with the unregulated processing of personal data. Lack of attention to the protection of personal information can erode the already low trust that Canadians have in political parties and in our democratic system. In an age of social media, being more proactive about privacy protection and providing those necessary assurances, is good organizational practice. The appropriate management of personal data is in the interests of not only individual citizens, but also the long-term health of our democratic system. ■

IT'S MORE THAN ROBO-CALLS

KEN COSGROVE

New technologies are changing campaigns, and they also raise questions about voters' privacy.

Les nouvelles technologies modifient le déroulement des campagnes et soulèvent des questions sur le respect de la vie privée des électeurs.

The modern political landscape is full of new technologies, new devices and new forms of organization that are re-making the way politics is conducted. Our candidates and their aides are armed with smart devices that keep them perpetually online, able to respond to a news cycle that was once measured in days but now spins in real time. They have an ability to collect massive amounts of data — and apply them in precisely targeted ways. These technological improvements — such as ever-faster Internet speeds and mobile video — have changed and enhanced our lives, but there is one constant: human nature remains fallible. These campaign tools are put to use by real people, and as long as our political behaviour remains imperfect and subject to temptation, they can be used for bad as well as good.

The fallible nature of humanity means that the expanding arsenal of campaign technology has the potential to undermine our institutions and democracy. It therefore becomes important for people and their governments to understand the applications of new technologies in political campaigning in order to preserve the free and fair elections that Canadians expect. Those who are charged with ensuring fair elections need to come to grips with such developments as the explosion of database marketing and the use of tracking cookies on the computers of visitors to campaign Web sites. Much of this remains below the radar of the average voter.

But the aggressive push by political parties to adopt new technologies raises major questions about privacy rights and data security and whether regulation is necessary. Who watches the political parties who are watching voters? How can we ensure that technologies that could be used to enhance democracy, allowing parties to take their policies and messages to all citizens, do not end up weakening it?

In the financially limited, time-constricted politics of Canada, efficient communication is a must. Smart market research becomes vital in the micro-targeted, narrow-casted environment in which victory is gained by presenting multiple small niches with tailored messages. Political campaigns are no different than any other producer with a product to sell: having great data about the customer is very important, and that means employing everything from cookies and pyschographics. As the Barack Obama campaign just showed, the best campaigns are able to amass large databases about their potential customers, knowing their preferences, and are able to pinpoint exactly where they are.

Technology has enabled the modern political campaign to become the personal campaign. Just as in commercial marketing, we have arrived at an era where messages are much more personalized and segmented than they are mass marketed and generalized.

Political campaigns acquire this knowledge about us without our knowing it. They allow us to opt into their Web sites or follow them on Twitter and in the process pull our information and our interests into their data web. Their algorithms become capable of dictating what comes our way before we even realize we're looking for it.

This is a different experience from watching a campaign unfold through mass media or direct involvement in physical political organizations. The modern campaign is the segmented campaign that contains a number of structured conversations that come to resemble a discussion mosaic rather than a single narrative.

The 2012 Obama campaign: knowing their customers.

PHOTO: CP PHOTO

Canadian parties are not — yet — as sophisticated in their use of technology as the Obama juggernaut was (neither was the Romney campaign). But given the way political parties learn from each other, it likely won't be long before they catch up. A lot of Canada's Conservatives' branding design and targeting is at least at par with American practices, though using cookies to track voters is not as developed in Canada. The Liberals are also doing a lot of the top-down crowd sourcing that played a big role in the Obama campaign.

To date, the issue that has garnered the most attention in the convergence of technology and politics in Canada has been the infamous Pierre Poutine robo-calls in Guelph, Ontario, during the 2011 federal election. The activities involved in the case strongly resemble those shown in the HBO series *The Wire*, in which disposable technology and computer security flaws were illicitly exploited. These are easily learned skills.

But many consultants and academic researchers argue that robo-calling is one of the least efficient and effective ways to reach potential voters. Far greater threats are brewing. Future Pierre Poutines may be armed with the results of databased behavioural research that provides a far more effective way of tampering with voter behaviour than the crude robo-call.

For political professionals, there is significantly more of an upside to working within the new data-driven campaigns than there is in taking on the downside risk of being caught in ventures such as the electoral shenanigans in Guelph. I have been impressed by the high standard of ethics and dedication to democratic values among Canadian consultants. They might not like their opponents. But they have great respect for their opponents who did things the right way and scorn for those who did not.

The temptation to engage in illicit activities could be further reduced by fostering a climate of professional responsibility, as is done in the United States through the American Association of Political Consultants and its code of conduct. Most people involved in politics are good, reputable Canadians who would be horrified to see themselves exposed as cheaters or censured by their professional body.

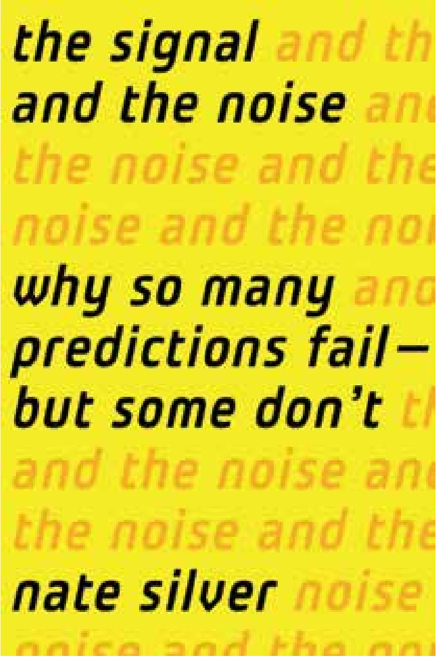
But Elections Canada also needs to help voters protect themselves. In cooperation with political and marketing professionals, Elections Canada should create a public education campaign to make voters aware of how parties collect data and what they are and are not allowed to do. A public education campaign conveying the simple message that Elections Canada doesn't make phone calls to your home, and doesn't move the location of polling stations, could act like a vaccine against devious robo-calls.

But that, increasingly, appears to be an example of generals preparing to fight the last war. The pace of technology, and the eagerness of political parties to use it to their advantage, means the potential for new forms of abuse remains. One day, Pierre Poutine's antics may seem a quaint reminder of a simpler age. ■

Ken Cosgrove is associate professor of government at Suffolk University in Boston. He held the Fulbright Research Chair in North American Integration Studies in 2011, where he researched political party marketing in Canada. His current work focuses on comparative US-Canada political marketing, and his previous work has focused on Republican Party marketing in the US.

BOOK REVIEW

Trust the data



Nate Silver. *The Signal and the Noise: Why So Many Predictions Fail — But Some Don't*. London and New York: The Penguin Press, 2012.

Review by David Herle

If you are the type of person who wishes you'd taken more statistics courses in university, this book is either the one for you or the cure for that yearning. But if you are the type of person who really enjoyed reading Nate Silver's "FiveThirtyEight" blog in the *New York Times* because you appreciated its data-driven insights into the last US election, this is almost certainly going to disappoint you. The blog was one of the political phenoms of the electoral season, but *The Signal and the Noise* is not about politics. It does, however, explain what made his blog so essential.

Silver came to prominence among political junkies during the 2012 presidential campaign. He constructed a predictive model for the presidential election, which integrated and weighted the available opinion polls as well as other variables (the workings of the model are *not* revealed in the book). The model yielded forecasts that continually predicted the strong odds of an Obama victory, so that seemed to its fans — mostly Democrats — to be the most robust and reliable predictor of all in a sea of conflicting election coverage.

By the end of the campaign, 20 percent of visitors to the *New York Times* Web site were headed for Silver's blog. Not all of them were fans of the blog. Republicans, who had apparently invented their own political reality and electorate, attacked him viciously on everything from alleged partisanship to possible sexual orientation. They went to great lengths to demonstrate that it was possible Silver's predictions were wrong (a fact he readily acknowledged by focusing on probability rather than certainty), and in the process apparently devoted no share of mind to the idea that he might possibly be right. The Republicans' arguments only served to elevate Silver to superstar status.

In *The Signal and the Noise* (terms familiar to makers of cassette mix-tapes in the 1970s), Silver uses poker, chess, weather forecasting, climate change, economics, baseball and politics as examples to put forward several principles of effective forecasting. He begins by advising to pick your spots. Silver is the first to admit that it is much easier to call the outcome of an election as voting day nears or to use statistics to determine which shortstop will get on base more frequently than it is to predict the impact of climate change or how much an economic stimulus will lower unemployment.

Another principle is not just to use data, but to trust them. Silver is scathing in his discussion of political punditry, citing his study that shows members of the McLaughlin Group are just as likely to be wrong as right on any given political prediction. The foundation of Silver's election predictions was polls that were, within their limitations, accurately capturing voting intention.

Also, he says, we have to distinguish the signal from the noise. In the past, forecasting was hampered by limits to the amount of data available. Now we are inundated with data, which gives rise to the new challenge of isolating the data that matter (the signal) from the data that distract (the noise). Silver notes that the US government tracks 45,000 economic data points each year, most of which will be irrelevant to forecasting. But which ones should we pay attention to? One of the reasons Silver's

Contributing Writer David Herle, former pollster and chief campaign strategist for the Liberals under Paul Martin, is a principal of the Gandalf Group in Toronto.