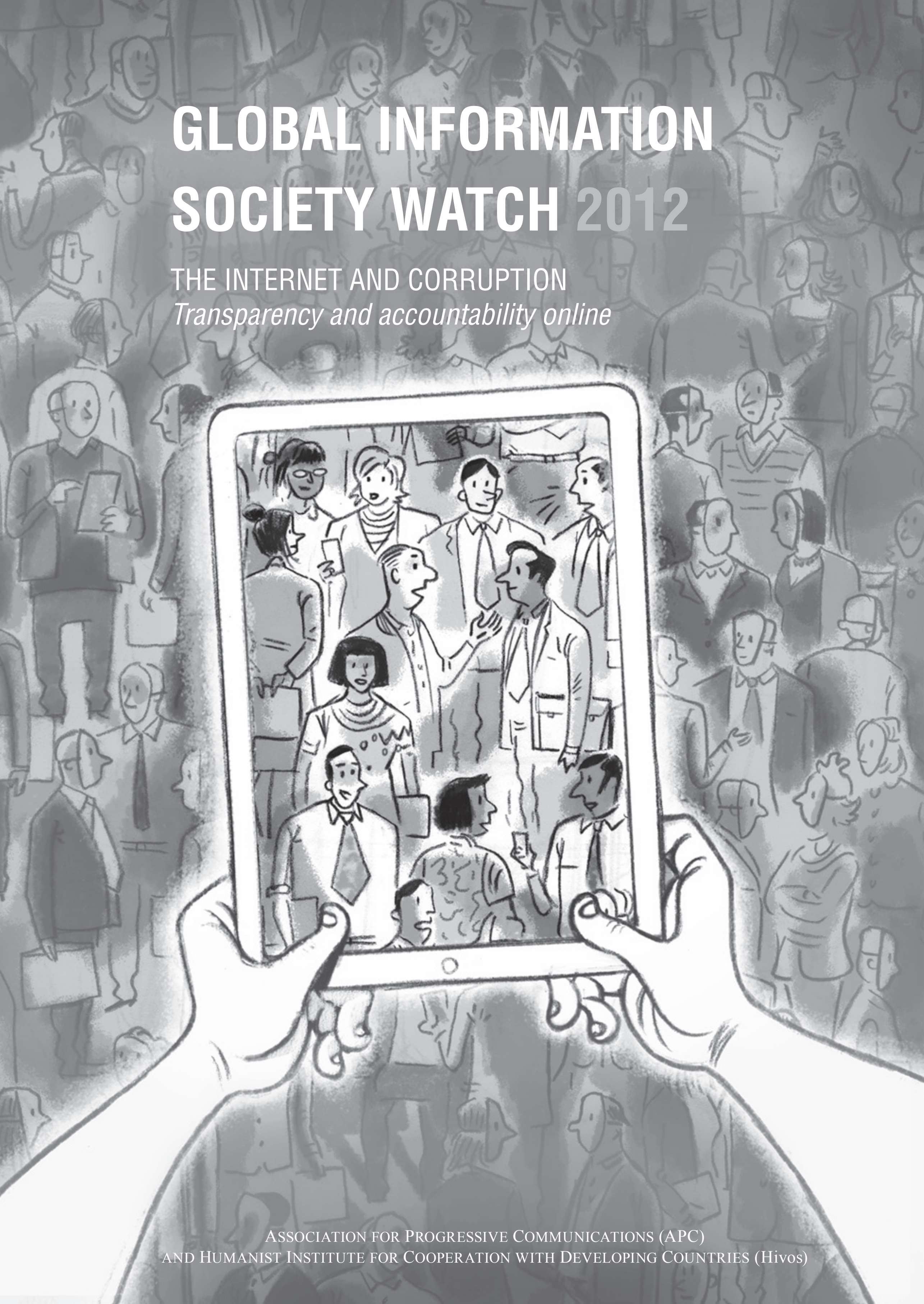
GLOBAL INFORMATION SOCIETY WATCH 2012

THE INTERNET AND CORRUPTION

Transparency and accountability online



Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

Global Information Society Watch

2012

APC

Hivos
people unlimited

Steering committee

Anriette Esterhuysen (APC)
Loe Schout (Hivos)

Coordinating committee

Karen Banks (APC)
Monique Doppert (Hivos)
Valeria Betancourt (APC)

Project coordinator

Valeria Betancourt

Editor

Alan Finlay

Assistant editor

Lori Nordstrom

Publication production

Mallory Knodel

Proofreading

Valerie Dee
Lori Nordstrom

Graphic design

Monocromo
info@monocromo.com.uy
Phone: +598 2 400 1685

Cover illustration

Matías Bervejillo

Financial support provided by

Humanist Institute for Cooperation with Developing Countries (Hivos)
Swedish International Development Cooperation Agency (Sida)

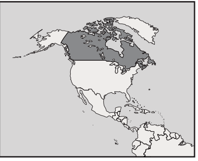
APC Hivos people unlimited Sida

Global Information Society Watch
Published by APC and Hivos
2012

ISSN: 2225-4625
ISBN: 978-92-95096-85-1
APC-201301-CIPP-R-EN-DIGITAL-176

CANADA

TRANSPARENCY, ACCOUNTABILITY AND THE INTERNET: THE "ROBOCALLS" SCANDAL



APC and Open Technology Institute
Lisa Cyr and Grady Johnson
www.apc.org and www.oti.newamerica.net

Introduction

The summer of 2011 saw Canadian headlines marred by controversy. After tens of thousands of Canadians filed complaints with the electoral commission, it soon became evident that an unknown number of voters had been the victims of ICT-mediated electoral fraud throughout the country. The since-named "robocalls scandal" has left a scar on the Canadian political process, with members of civil society and opposition parties calling for by-elections in several contested ridings.

On 2 May 2011, Canadians set out to the polls for the fourth time in seven years. Since 2004, no party had won a majority of seats in the House of Commons, and a rising lack of confidence in the minority government gave way to federal elections once again, in which the Conservative Party would win a majority government this time around.

In the days leading up to the 2011 federal election, voters from across the country received calls asking whether they would be voting for the Conservatives. On election day, opposition party supporters in over 200 ridings received an automated message claiming to be from Elections Canada, citing an unanticipated increase in the number of registered voters and directing them to a new – and false – polling station.

The Conservative Party has acknowledged that there was some wrongdoing but claims that these were the actions of an unnamed rogue campaigner, acting on his or her own initiative, and not reflective of party policy.

However, the question on everyone's mind, as articulated by opposition Member of Parliament David Christopherson, is: "How likely is it that it's one rogue person who's behind this?"[1]

The answer is, very.

What is worrisome about this case is not that one of Canada's political parties might be engaged in electoral fraud (as reprehensible as that is), but rather that the accused party may in fact be telling the truth. The larger issue is not whether the Conservative Party is culpable or not; the mere fact that their explanation is *plausible* is cause for concern.

The emerging landscape of cheap and wide-reaching communications media means that it is entirely possible that an overzealous campaigner, sufficiently motivated, could have orchestrated these "robocalls" with little risk or cost to themselves, right from their living room. Such super-empowered individuals with a minimum of computer skills and sufficient motivation could have a significant impact on future elections.

How one call changed an election

Early on election day it became clear that something was amiss. Elections Canada received hundreds of calls from confused poll clerks and frustrated voters, having been directed to the wrong polling station – or, in some cases, to empty parking lots or addresses that did not exist. Stories emerged of angry citizens tearing up their voter cards in frustration.

No election is without its hiccups, but clearly this was unusual.

It did not take long for the confusion of 2 May to transform into outrage and indignation. Disenfranchised voters lodged scathing complaints with Elections Canada while opposition parties made public demands for an explanation.

As the reports came flooding in from ridings across the country, a troubling picture began to emerge. It quickly became evident that these were not isolated incidents but in fact a deliberate effort to disrupt the voting process. Final tallies showed that Elections Canada had received over 31,000 complaints from 200 of Canada's 308 federal ridings.

The situation was worse than anyone had suspected. Two independent studies conducted by Ekos Research and Forum Research determined that the number of Canadian households who received the fraudulent calls was between 50,000 and 250,000, respectively – more than enough to sway an election.

According to official investigators, fraudulent robocalls were used extensively to misinform voters in at least seven ridings in Ontario, Saskatchewan, Manitoba, the Yukon and British Columbia.[2] On elec-

[1] ottawa.ctv.ca/servlet/an/local/CTVNews/20120329/robo-calls-Mayrand-ottawa-20120329/20120329/?hub=OttawaHome

[2] www.cbc.ca/news/politics/story/2012/03/26/pol-elections-canada-committee-thursday.html

tion day, tens of thousands of Canadians in these ridings received the automated calls claiming to be from Elections Canada, telling them their polling station had been changed – but Elections Canada does not use automated calls.[3]

Non-Conservative voters were almost exclusively targeted. According to Ekos Research, in the seven most affected ridings, 10% to 15% of households received the robocalls. Among opposition party supporters, this number was as high as 90%.

Each of these ridings was a close race between the Conservative and opposition candidates, and critical to achieving a much-coveted federal majority. Most of the Conservative candidates in these ridings eked out victories by slim margins – in one case by as little as 17 votes. Whatever their affiliation, if any, to the Conservative Party, the intentions of the robocalls' authors were clear.

Once the scope of the fraud had been revealed, election officials were now tasked with uncovering those responsible and bringing them to justice. As Elections Canada investigators soon discovered, this would not be easy.

One riding, which was particularly targeted and has since become the centre of the investigation, is Guelph, Ontario.

On 2 May 2011, some 7,000 households in the Guelph riding received automated calls directing them to false or non-existent polling stations. Investigators have since traced the calls back to an automated voice-over-IP service hosted by RackNine, an Edmonton-based webhosting company, from an account registered under the name "Pierre Poutine".[4]

The transcript of one robocall from the Guelph riding reads as follows:

> This is an automated message from Elections Canada. Due to a projected increase in voter turnout, your poll location has been changed. Your new voting location is at the Old Quebec Street Mall, at 55 Wyndham Street North. Once again, your new poll location is at the Old Quebec Street Mall, at 55 Wyndham Street North. If you have any questions, please call our hotline at 1-800-443-4456. We apologize for any inconvenience this may cause.

According to RackNine's records, the fake Elections Canada message went out to 7,676 numbers between 10:03 a.m. and 10:14 a.m. on election day – at a cost of just CAD 162.10 (USD 160).

At the time of writing, more than a year has passed and Elections Canada has yet to name any suspects. With Canadians increasingly upset and demanding that someone be held accountable, the question on everyone's mind is, can the perpetrators be brought to justice? This remains to be seen.

Tracking Pierre Poutine

"Pierre Poutine" was meticulous in hiding his (or her) tracks. He registered a PayPal account using an obvious pseudonym, used prepaid credit cards purchased with cash, a prepaid "burner" phone, a fake address and a free Gmail account. To further mask his identity, he accessed his RackNine account through a free IP anonymisation service.

When investigators subpoenaed the IP anonymiser, Saskatchewan-based freeproxyserver.ca, the records were no longer available. Similarly, the surveillance footage from the pharmacy where the prepaid credit cards were purchased had long since expired.

However, there remain a few breadcrumbs to follow. The records released to investigators from RackNine have shed some light on the case, but have yet to provide concrete evidence.

To begin with, the list of numbers uploaded to the RackNine account matches a Conservative Party database, including the names of thousands of "non-supporters" who had been contacted and identified by local campaigners in the days leading up to the election. The Elections Canada voters list does not contain voter preference, nor does it contain voter telephone numbers.[5]

RackNine had also been used extensively (for legitimate calls) during the election by Conservative campaigners, including Andrew Prescott, head of the Conservative campaign in Guelph. As the records show, both Prescott and "Poutine" accessed their accounts through the same proxy service. At one point, both accounts were accessed – within four minutes of each other – using the same IP address, 99.225.28.34.

Though certainly suspicious, none of this amounts to damning evidence. Under the current legal environment, IP addresses cannot be conclusively tied to an identity – they are recycled on a semi-regular basis and cannot be submitted as evidence in court. Given this reality, can investigators really make a case beyond reasonable doubt? It seems unlikely.

[3] www.cbc.ca/news/politics/story/2012/03/29/pol-robocalls-mayrand.html

[4] Poutine is a French-Canadian dish made of French fries, gravy and cheese curds and is not an actual family name; therefore the name Pierre Poutine at a glance is suspicious to begin with.

[5] news.nationalpost.com/2012/03/29/pierre-poutine-made-6700-robocalls-in-guelph-on-election-day-using-450-number

Conclusion

Necessarily, the robocalls incident brings up the question of privacy versus security. Not being able to trace the fraudster(s) in this case is a major concern for Canadian authorities and for the integrity of the Canadian electoral process. However, privacy is paramount to human rights defenders across the globe who must remain anonymous, especially in oppressive regimes. But the implications are serious. As the robocalls scandal makes clear, ICTs are not a panacea for transparency and accountability – just as activists and watchdogs have been empowered to monitor and safeguard the electoral process, others have been similarly empowered to abuse it.

Robotic call centres allow individuals to orchestrate massive campaigns without the need for volunteers or phone banks, and companies like RackNine provide easy-to-use, affordable services to thousands of organisations worldwide. For a trivial amount of money, it is now possible to reach (and misinform) an audience of thousands in the time it takes to cook a hardboiled egg.

As this case shows it is not only *possible* to sway an election – it is *easy* and *affordable*. Worse, it seems it may even be possible to get away with it.

Unless the perpetrators can be caught – which at this point seems unlikely – or effective safeguards can be introduced, we are likely to see more of this kind of fraud in the future. The robocalls case could be easily replicated in any country, and as the investigation has shown, it is extraordinarily difficult to catch someone determined to remain anonymous. In light of this, the recommendations in this report will focus on strategies for prevention and mitigation.

Action steps

While it may not be possible to catch clever fraudsters, there are measures that can be implemented to immunise the public from similar crimes in the future. As Elections Canada gears itself up for another election, it will also need to consider the additional risks and challenges associated with electronic voting and modify policies and procedures accordingly.

Automated call services like RackNine should be closely regulated. The goal is not to make these companies liable for the content of their customers' calls, as this would constitute an unwarranted invasion of privacy, but to require due diligence when registering new users. "Instant access" (offered by most) should not be an option: those wishing to access these services should have to register using their real names, and this information should be verified. Registration under obvious pseudonyms like "Pierre Poutine" should be forbidden. Companies should also limit the use of prepaid credit cards (which are virtually untraceable) for these kinds of services.

As for Elections Canada, the organisation should distribute pamphlets with every voter card and checklists detailing the election process and what Elections Canada does and does not do. They should warn against the possibility of this kind of fraud and urge citizens to disregard suspicious or misleading phone calls.

Each voter card could also include a unique ID number known only by the individual and Elections Canada. Fraudsters would have to know the address, phone number and ID (which should remain private) of each voter they intended to dupe.

Finally, political parties should be required to implement stronger security measures for their voter databases. These databases should be confidential and full access available only to a select and trusted few. Local campaigns should be subject to random audits to ensure compliance, and access to their data (that is, *private citizens' data*) should be monitored and logged. In this way, should a party list be used to commit fraud in the future, the list of suspects will be short.

Parties (or local campaigns) that fail to comply with minimum security standards should be censured with limited access to voter lists. Safeguarding voters' information (which political parties are routinely entrusted with) should not be an afterthought, but rather should be seen as an imperative – and prerequisite – for elections campaigning.

Officials may well be unable to catch the perpetrators of this election fraud, or prevent others from emulating them in future elections. However, with the proper safeguards in place, it will be possible to limit the scope and damage. ■