Canada’s Privacy Plan
A Crowdsourced Agenda for Tackling Canada’s Privacy Deficit
## Contents

Acknowledgements .................................................................................................................. 3

**Executive Summary** ........................................................................................................... 4

**Three Key Recommendations** .......................................................................................... 6

**Our Policy Agenda** ............................................................................................................. 10

**Introduction:** Privacy Matters ........................................................................................... 12

**Chapter 1:**

Outlining Canada’s privacy deficit ......................................................................................... 18
  - Background .......................................................................................................................... 20
  - Case Study 1: Bill C-51 - Sweeping new spy powers but no new oversight .................. 22
  - Case Study 2: The CSE and mass surveillance ................................................................. 28
  - Case Study 3: Bill C-13 and S-4 - Undermining the privacy of every Canadian .......... 34

**Chapter 2:**

How Canadians want to address our privacy deficit ............................................................. 38
  - Recommendation 1: Get a Warrant ................................................................................... 40
  - Recommendation 2: End Mass Surveillance .................................................................... 48
  - Recommendation 3: Embrace Accountability .................................................................... 52

**Chapter 3:**

Setting a global standard ......................................................................................................... 58

**Chapter 4:**

The Process: Working toward a crowdsourced pro-privacy agenda ..................................... 64

**Conclusion:** Listen to Canadians! ....................................................................................... 76

**APPENDIX I:** The results from our Crowdsourcing Tool ................................................. 78

**APPENDIX II:** Methodology .............................................................................................. 88

**REFERENCES** ....................................................................................................................... 92
“Canada’s Privacy Plan” was only made possible because of the support, time, and effort of countless groups and individuals across Canada and around the world. While they are too numerous to name individually, this plan is built on a wide range of grassroots and academic public policy initiatives that have raised awareness of, and proposed solutions to, Canada’s privacy deficit. We’ve tried our utmost to give that impressive body of work consideration throughout this process.

We are particularly indebted to the over 125,000 everyday Canadians engaged in our privacy work, many of whom participated in our crowdsourcing project by taking the time to contribute their often-detailed ideas, and to spread the word to their friends and colleagues. We also thank the volunteers and organizations who arranged on-the-ground events to make sure people could have their say. The outcomes of this report are primarily based on this wealth of grassroots input and we couldn’t be more grateful.

We are especially thankful for the contributions of our Protect our Privacy Coalition partners, whose expert advice helped shape this project from start to finish. We owe special thanks to peer reviewers who provided in-depth feedback, comments, and suggestions to strengthen the rigour and quality of this report. Any weaknesses or shortcomings in this final product are in spite, not because, of their contributions, and are entirely the responsibility of the authors.

This report marks a milestone in a longer campaign that aims to ensure, quite simply, that every Canadian can use the Internet without fear of being watched. This work is inspired by the energy of OpenMedia’s grassroots community of over half a million people who have used our platforms to speak out for strong privacy safeguards in a digital age. We simply couldn’t do what we do without them – thanks!
Executive Summary

A crowdsourced agenda for tackling Canada’s Privacy Deficit

This report is about each and every one of us. The scale of the privacy intrusions revealed by National Security Agency (NSA) whistleblower Edward Snowden is such that hardly anyone, anywhere with an Internet connection has remained untouched.

We now know that the threshold for getting trapped in the government’s surveillance dragnet is problematically low – phone records are being spied on\(^1\), private Internet activity is being monitored,\(^2\) and even our private emails to Members of Parliament are now being collected and stored in giant government databases, in some cases for years.\(^3\)

**Internet Voice**

“Protection of privacy and strong safeguards and oversight of any collection of private data is of paramount importance if our democracy is to thrive. We cannot forego our privacy out of fear.”

– Brent M.

*Internet Voices* come from the over 10,000 people who have used OpenMedia’s Crowdsourcing Tool (found at openmedia.org/privacyplan), attended an OpenMedia crowdsourcing event, or spoke out on OpenMedia’s social media platforms to submit comments as part of this process. We quote these everyday Canadians throughout the report to bring more attention to the lived experiences of Internet users with privacy issues. See the chapter on “The Process” for more information about the Crowdsourcing Tool and the tens of thousands of people across Canada who have spoken out for strong privacy safeguards.

All this with little grounds for suspicion, no warrants, and no independent oversight. On top of this, Canadians have seen the federal government introduce a suite of legislation – Bills C-51,\(^4\) C-44,\(^5\) and C-13\(^6\) – that amounts to a sweeping expansion of the surveillance state and a disturbing dismantling of Canadians’ privacy rights.

It’s clear that Canadians are concerned: Over 94.1% now want a Parliamentary Committee to conduct a comprehensive review of existing oversight mechanisms.

Privacy is a fundamental human right. As crowdsourcing participant Brent says, “Protection of privacy and strong safeguards and oversight of any collection of private data is of paramount importance if our democracy is to thrive.”
Supporters like Brent inspired us to create “Canada’s Privacy Plan.” At OpenMedia, participatory values are at the heart of everything we do. We believe the best ideas come from our pro-privacy community of engaged citizens – the people whose lives are impacted the most by reckless government policies. Canadians have told us they feel disempowered by their government; we empower them by providing the tools they need to push back.

That’s why we worked with some of this country’s top privacy experts in the large, non-partisan Protect our Privacy Coalition to craft a crowdsourcing tool, along with other online tools and offline dialogues, to give everyone a say in shaping this report. The crowdsourcing tool was then used to ask Canadians some straightforward questions: What is most important to you when it comes to privacy? What will it take to tackle our privacy deficit? What safeguards do you think are necessary to protect our human rights in a digital age?

The response we received was overwhelming — over 10,000 Canadians took the time to share their views with our drag-and-drop crowdsourcing tool, often in great detail, as part of the over 125,000 people who engaged with our privacy work overall. Their collective input determined both the direction and recommendations of this report. We will highlight direct quotes from these everyday Canadians throughout.
Three Key Recommendations
Three Key Recommendations
Our crowdsourcing process identified three key concerns that Canadians want to see addressed in order to tackle our privacy deficit: i) warrantless access to personal information, ii) widespread dragnet surveillance of entire populations, iii) insufficient oversight and accountability of surveillance activities. From their input, and the many other elements of our crowdsourcing process, we have distilled three key recommendations.

Canadian strongly support the principle that the government should be required to obtain a warrant to access their sensitive, personal information. 93.8% said such searches are only permissible when a judge grants a warrant based on evidence that a crime is soon to be, or has been, committed. When Canadians were asked to rank six privacy priorities in order of preference, “Require a warrant” came first, with fully 68.9% choosing it as one of their top three priorities.

Given these strong sentiments, our first recommendation focuses on how to end warrantless surveillance by the government. We outline ways to safeguard Canadians’ privacy, such as by ending legal immunity for the ‘voluntary’ warrantless disclosure of personal information, stronger reporting and transparency mechanisms, and tougher privacy laws to ensure government agencies use personal information strictly for the reason it was provided. These measures would roll back widespread warrantless surveillance, and create stronger judicial safeguards to protect every Canadian’s private life.
Canadians expressed strong opposition to mass online surveillance, with fully 68.9% choosing “End Blanket Surveillance” as one of their top three key privacy priorities. 89.1% want to make all surveillance activities require a warrant approved by a judge against a specific target. 92.2% also said the government should not be monitoring law-abiding individuals and organizations not posing any known threat to national security.

Our second recommendation focuses on ending suspicionless mass surveillance. We propose an audit of all ongoing surveillance activities, halting any that involve the warrantless collection of Canadians’ personal information, including the bulk collection of metadata. We also propose that surveillance activities, including those by the Communications Security Establishment, require judicial, not political, authorization. We also call for an end to the government’s practice of collecting and analyzing Canadians’ social media posts.

Canadians overwhelmingly support much stronger accountability, oversight, and transparency for government surveillance activities. 94.1% want a Parliamentary Committee to conduct a thorough review of existing oversight mechanisms. 91.8% want the CSE to produce regular unclassified reports, detailing how often the agency intercepts Canadians’ personal information. 88.2% agree with the Privacy Commissioner that spy chiefs should testify regularly before Parliamentary committees. 87.9% want an independent body to oversee spy agencies and issue regular reports to the public.

We propose a range of measures to tackle the oversight deficit, including ensuring strong, independent oversight and review bodies for the CSE and the Canadian Security Intelligence Service (CSIS). We call for a cross-party Parliamentary Committee, elected by secret ballot of all MPs and chaired by a member of the largest opposition party, to conduct ongoing review of spy agency activities. We also propose reining in the steep costs of surveillance, by requiring the Parliamentary Budget Officer and Auditor General to develop clear cost projections for surveillance activities.
The following are the concrete policy proposals of the Canada’s Privacy Plan project. The full report gives more plain-language explanations of how these policies will work, and the impact they will have.
RECOMMENDATION 1

Get A Warrant

1. End legal immunity for ‘voluntary’ warrantless disclosure of personal information
2. Strengthen transmission data warrant thresholds to “reasonable belief”
3. Mandatory reporting of subscriber data requests
4. Require greater transparency from telecom companies
5. Bring Canada’s 35 year old Privacy Act into the digital age
6. Mandatory notification of surveillance targets
7. Require a warrant to search cell phones and other digital devices
8. Prohibit the ‘voluntary’ disclosure of personal information by organizations
9. Safeguard privacy in emergency situations
10. End the use of drones to conduct warrantless surveillance

RECOMMENDATION 2

End Mass Surveillance

1. End all suspicionless mass surveillance, including the bulk collection of metadata
2. Require judicial not political authorization for surveillance
3. No future expansion of surveillance without a verifiable need
4. Prevent government agencies monitoring what Canadians say on social media

RECOMMENDATION 3

Embrace Accountability

1. Reinstate the Office of the CSIS Inspector General
2. Create strong, independent control of the CSE
3. Implement the CSE oversight recommendations proposed in Bill C-220
4. Establish a cross-party Parliamentary Committee tasked with ongoing review of spy agency activities
5. Fully implement the Privacy Commissioner’s January 2014 ‘Checks and Controls’ recommendations
6. Ensure that the Security Intelligence Review Committee can perform its role effectively
7. Implement the oversight recommendations of the 2006 O’Connor Report
8. Establish an Interception Commissioner to review the interception of private communications by spy agencies
9. Rein in the steep costs of excessive government surveillance
10. Going forward, ensure that oversight keeps pace with new spy agency capabilities and powers
Introduction

Privacy Matters
We wrote this report because privacy matters. With each new spying revelation, it has become clear that Canada faces an alarming privacy deficit, with dangerous and lasting consequences for the health of our democracy, for our liberty, and for our daily lives. Strong privacy rights need to be at the heart of any healthy democracy, because they are the foundation of many other democratic rights we hold dear.

Experts estimate that over 700 million people have changed their online behaviour as a result of the NSA revelations. A Pew Research poll found that 30% of Americans have “taken steps to shield or hide their information from government digital dragnets” in the wake of the Snowden revelations.

Privacy violations are also having more acute effects: in the last year over 200 Canadians have come forward to say their personal or professional lives have been ruined due to information disclosures, despite never having broken the law. Some have faced career limitations, while others have had to deal with travel restrictions. False charges that were subsequently dropped or dismissed, never resulting in criminal records, or even brief contact with the mental health system can create flags that send misleading and damaging messages to future employers on what should be private records.

These stories in many cases point to the more banal threat regarding the government’s handling of our sensitive data; that without safeguards in place government bureaucrats will simply act recklessly and make life-impacting mistakes. In recent years federal government agencies have seen over 3,000 breaches of the highly sensitive private information of an estimated 725,000 innocent Canadians.

These findings contradict the odd view that those who have nothing to hide have nothing to fear. We should all fear the chilling effect on free expression, lasting restrictions on our movement or career opportunities that could haunt any one of us, and the undermining of the human rights not just of Canadians, but of people all over the world.

Put simply, people who believe their words and activities are being monitored become less willing to speak out, to express views outside the mainstream, or to express dissent about government policy. Privacy violations lead to the hollowing out of our public space. It is precisely this type of free expression that democracies require to flourish, change, and adapt.

Privacy is about trust and security: ensuring people are free to be themselves, without fear that their every word and every move is being watched, logged, analyzed, and retained in secret databases for future use against them. This is all the more important given that lives have been ruined by data disclosures, as outlined in more detail below. Privacy is security in its most basic sense.

So there is little doubt that privacy matters. And there is little doubt that Canada is in the midst of an unprecedented privacy crisis. We’re at a tipping point where Canadians need to decide whether to continue to evolve into a mass surveillance society or take a stand and start reining in the government’s surveillance apparatus. A surveillance society is not inevitable, and this report will outline a positive crowdsourced vision for how Canadians can take common sense steps to strengthen privacy safeguards.

A false choice

Canadians are clearly concerned. A detailed survey recently undertaken by the Privacy Commissioner found that 9 in 10
Canadians are worried about privacy, with 78% expressing concern about government surveillance, and a large majority opposed to warrantless searches. The same survey also revealed that Canadians feel a sense of powerlessness, with 73% of participants saying they believe they have less protection of their personal information than they had a decade ago. The government’s message to Canadians — that invasive mass surveillance and loss of privacy are somehow necessary in order to “keep us safe” — has deepened this sense of disempowerment.

This presents a false choice between privacy and security. In fact, experts have made clear that mass surveillance does nothing to make us safer. There is increasing evidence that it actually makes us less safe, by drowning our intelligence agencies in reams of useless data. In other words, when you collect the entire haystack, everything starts to look like a needle.

We seek to overturn the view that in order to have security, we must effectively give up our right to privacy. Instead, we believe that what is needed are measures designed to provide for both security and privacy, in an accountable and transparent manner.”

Former Ontario Privacy Commissioner Ann Cavoukian

Following a detailed study, the Council of Europe’s Legal Affairs Committee concluded that “mass surveillance is not even effective as a tool in the fight against terrorism and organised crime, in comparison with traditional targeted surveillance.” The same committee found that aspects of mass surveillance, such as deliberate weakening of encryption, “present a grave danger to national security.”

We do not dispute that targeted surveillance can be a necessary tool to tackle crime and protect national security. However, common sense safeguards are required to ensure that such surveillance is only conducted against specific targets in the event of a potential threat, and only in proportion to the risk. Such surveillance should be subject to judicial authorization, parliamentary oversight and due process, be consistent with the Charter of Rights and Freedoms, and be conducted in accordance with international principles of human rights.

This type of targeted, necessary, and proportionate surveillance is the opposite of the kind of mass, indiscriminate surveillance revealed by National Security Agency (NSA) whistleblower Edward Snowden. Blanket surveillance tactics invade our privacy, chill our freedom of expression, and undermine our most basic human and democratic rights.
Human consequences

We must not forget the grave practical dangers to individuals of overly-weak privacy safeguards. Canadians’ lives are already being turned upside down by the government’s privacy deficit. Businesses have been ruined, familial connections broken, and people’s ability to travel undermined by the improper disclosure of Canadians’ personal information to foreign governments, for example.21

And that’s just scratching the surface: according to the federal Privacy Commissioner, in recent years there have been over 3,000 breaches of sensitive citizen data, affecting approximately 725,000 individuals.22 In just a single 12-month period, the personal information of over 780,000 Canadians was casually handed over to the government by telecom companies – without a warrant or due process.23

With numbers like this, people in every village, town, and city block in the country have been affected. Given the current government’s policy direction, this situation will continue to get worse unless Canadians come together to turn things around.

Let’s get started

The issue of privacy is a rich and nuanced topic, and not a week goes by without a significant new development. We’ve tried to keep things simple by dividing the core of this report into three key areas – first, setting out the problem; second, identifying solutions; and third, looking at the international context.

• We’ll start by laying out some background, to outline precisely how our privacy deficit has widened alarmingly in recent years. Our case studies of recent proposed and passed legislation, and of the activities of the Communications Security Establishment (CSE), will make clear the extent of the privacy challenges this country faces.

• We’ll then identify solutions: three key recommendations, shaped by crowdsourced input from Canadians, that aim to systematically address our privacy deficit. Taken together, these recommendations would put a stop to warrantless searches, end mass surveillance (including the bulk collection of metadata), and place government agencies responsible for surveillance under much stronger oversight.

• Finally, we’ll look at the international context and at how Canada can play a leadership role on the world stage in tackling the global privacy crisis.

This report will focus primarily on the government’s handling of Canadians’ personal data. This is not a report about commercial privacy policies and the practices that govern private companies. Similarly, this report does not deal with technological workarounds to protect privacy, such as the use of encrypted services like Tor. While use of these tools can be an important way for people to speak out about government surveillance, nobody should be forced to resort to technical measures to safeguard their privacy from their own government.

These proposals are not intended to be a precise or detailed roadmap. In a report of this nature, we know it’s impossible to cover every angle and unwise to attempt to create model legislation. Our intention is to set out a high-level outline of what Canadians want to see done to address our privacy deficit. Our hope is that experts and decision-makers will use this to guide more detailed legislative work that’s clearly needed to translate these ideas into real change.

In that sense, this report and crowdsourced plan marks the end of one process, but the beginning of another. There is much work to be done if Canadians are to win back the strong privacy protections that older generations took for granted. This is a debate that will determine the shape of our democracy and impact our daily lives for decades to come.
There is increasing evidence that mass surveillance actually makes us less safe, by drowning our intelligence agencies in reams of useless data. In other words, when you collect the entire haystack, everything starts to look like a needle.
There is increasing evidence that mass surveillance actually makes us less safe, by drowning our intelligence agencies in a haystack, everything starts to look like a needle. In other words, when you collect the entire haystack,
CHAPTER ONE

Outlining Canada’s Privacy Deficit
In this section of our report, we examine in detail some of the legislation, agencies, and technologies that have led to our current lack of legal protection against large-scale breaches of privacy and online spying.

Canada’s privacy deficit has widened alarmingly in recent years — largely as a result of the current government’s overt legislative initiatives and covert authorization of mass surveillance activities.

These overt and covert actions have exploited the fact that fast-paced technological growth has outstripped the ability of our privacy laws to keep up. The Internet, one of humanity’s greatest inventions, now risks becoming a dangerous tool of mass surveillance.

Our privacy laws are designed for another age. We have strong safeguards to prevent the government from opening letters sent by mail. However, the situation online is much different: governments have gained the ability to keep track of where, when and to whom digital messages are sent. If we expect privacy over our pen-and-paper postage system, why should our online communications be any different?

After all, if the government proposed building a system to keep track of the who, where, and when of our postal correspondence, Canadians would be outraged.

Yet we know from multiple reports that Canada’s electronic eavesdropping agency, the Communications Security Establishment (CSE), along with its “Five Eyes” partners (the U.S., U.K., Australian, and New Zealand surveillance agencies) is spying on private online activity on a massive scale.

It is clear that when it comes to Canada’s privacy deficit, many troubling factors are at play. Over the past decade, the government has greatly expanded the funding and powers of spy agencies such as CSE, and its partner agency, the Canadian Security Intelligence Service (CSIS).

Know your Bills

Bill C-51: The Anti-Terrorism Act
- Sweeping expansion of sensitive information disclosure across government
- Turns CSIS into a secret police force
- Opens the door to violations of our Charter rights
- No commensurate oversight or accountability

Bill C-13: The Protecting Canadians from Online Crime Act
- Allows wide range of government officials to access your information
- Grants legal immunity to telecom companies who disclose your private information
- Makes it easier for government to obtain highly revealing metadata

Bill S-4: The Digital Privacy Act
- Massively expands disclosure of personal information without consent to hostile organizations
- Permits telecom companies to hand your information to potentially hostile organizations without due process
At the same time, the government has introduced a series of legislative initiatives that dramatically expanded the power of the state to spy on its citizens, while doing nothing to update our privacy protections.

Meanwhile, public officials have left citizens largely in the dark when it comes to their government’s spying capacity. Much of what we know about the CSE’s activities comes not from the work of our resource-starved official watchdogs, but instead from whistleblowers like Edward Snowden.

Despite being excluded from high-level decisions impacting their privacy, members of the public are now beginning to demand answers about how much their right to privacy is being compromised and why.

Given that we know government surveillance capabilities are expanding rapidly, it is imperative that Canadians engage in an open, informed, democratic discussion surrounding their right to privacy in a digital age. Clearly, privacy rights are already under siege. Sadly, the current government’s culture of secrecy acts as a serious impediment to ensuring surveillance issues get the rigorous debate they deserve.

The following three case studies will examine some of the core dynamics at play when it comes to contemporary threats to online privacy in Canada. We will take a detailed look at Bill C-51, the government’s new so-called “Anti-Terrorism Act.” We will outline what’s known about how the CSE is undermining the privacy of Canadians and people around the world. Finally, we will review how Bills C-13 and S-4 have weakened key privacy safeguards.

We believe these case studies make clear that there is an urgent need for sustained, systematic action to address our privacy deficit before it’s too late.

**Internet Voice**

“The pendulum has swung WAY too far in the direction of limiting our privacy. Standards need to be adjusted to make privacy the default and transparency must be mandatory.”

— Katherine M.

The time has come for Canadians to examine the accountability and functionality of their state surveillance apparatus. Canadians need to ask searching questions: How is our government undermining our right to privacy without our consent? How specifically will legislation like Bills C-51 and C-13 undermine our digital privacy? What impacts will our loss of privacy have on democratic participation? How will the loss of privacy rights impact our daily lives?

**Internet Voice**

“It is a threat to autonomy, trespass to the mind. Your most basic human right is your right to be yourself.”

— Sal R., high school student
Case Study 1

Bill C-51: Sweeping new spy powers but no new oversight
In February 2015, the government published its new Anti-Terrorism Act, Bill C-51. Government lawyers were reported as wrestling with the Charter implications of the Bill right up to its publication — and it’s easy to see why.

The Bill amounts to a sweeping expansion of the surveillance state, a shift that has been described by one former Conservative senator as “unprecedented in peacetime.” The Bill makes provision for broad new spy agency powers and undermines the privacy of Canadians. At the same time, it does nothing to improve insufficiencies in oversight and accountability mechanisms for law enforcement and surveillance agencies. At the time of writing, the Bill is currently before Parliament, with the government seemingly determined to rush it through as speedily as possible.

Prime Minister Stephen Harper never tires of telling Canadians that we are at war with the Islamic State. Under the cloud of fear produced by his repeated hyperbole about the scope and nature of the threat, he now wants to turn our domestic spy agency into something that looks disturbingly like a secret police force.”

The Globe and Mail editorial team

For example, Bill C-51:

• empowers CSIS to detain subjects without charge for up to 7 days;
• allows CSIS to interfere with and “disrupt” people or organizations it views as a “threat to the security of Canada”;
• makes it far easier for CSIS to place Canadians on a no-fly list.

CSIS is even explicitly empowered to undertake illegal activity and breach people’s Charter rights. The Bill doesn’t bother to specify what such activities may include, although it does prohibit CSIS from harming, torturing, murdering, or “violating the sexual integrity” of an individual. In the context of such sweeping new powers, this clause offers scant reassurance.

Secret Police in Canada?

Bill C-51 contains a number of deeply troubling proposals. Most notably, it expands the powers of CSIS to the point where The Globe and Mail’s editorial team has warned it amounts to the creation of a secret police force:

“I am a card-carrying Conservative member that does not agree with the current direction and lack of transparency the Government is taking in regards to protecting the privacy of Canadians over the right to security. I do not want quick reactionary legislation as it does not fully take into account the citizens’ rights and needs.”

– Andrew J.

In Canada, you’re way more likely to be killed by a moose than by a terror plot.

Don’t let politicians manipulate you.

Take action @ you.leadnow.ca/p/reject-fear

Canadians are coming up with creative ways to push back against Bill C-51.
Anyone could be a target

All this raises a critical question: who will be targeted by these unprecedented new secret police powers? How does Bill C-51 define a “threat to the security of Canada”? Given that the government justifies the legislation by pointing to global terrorism, and to the threat posed by ISIS in particular, you might expect that Bill C-51 would apply strictly to these targets.

Unfortunately, many elements of Bill C-51 use broad language that could well be unleashed on law-abiding, non-violent protesters around the country. As Green Party leader Elizabeth May notes, “The words that are found under the definition of activities, which affects ‘the security of Canadians’, is so broad that it can apply to almost any activity including nonviolent civil disobedience. This bill could now treat peaceful protesters as potential terrorists.”

This prompts an obvious concern – you may think you have “nothing to hide,” but what if the government disagrees? Professors Craig Forcese and Kent Roach are two of Canada’s foremost privacy experts. They have outlined in detail how C-51’s new spy powers could be applied to democratic protest movements:

“If you apply this ambiguity to “democratic protest movements”, it is possible that the “threats” definition covers this sort of scenario: a foreign environmental foundation funding a Canadian environmental group’s secret efforts to plan a protest (done without proper permits) in opposition to the Keystone Pipeline Project, a project that the government of Canada sees as a priority and strongly in ‘the interests of Canada’.”

The Assembly of First Nations has also expressed its concern, warning that the Bill could lead to the “unjust labelling of First Nations activists as ‘terrorists’.”

Forcese and Roach conclude that Bill C-51 threatens a return to the widespread abuses committed by the RCMP during the 1970s when they were responsible for domestic security—abuses that were precisely why CSIS was first established in 1983.

A chilling effect on Free Expression

Given this context, it is clear that Bill C-51 will have an impact on Canadians’ willingness to speak out and engage in the democratic process. As Jim Emberger of the New Brunswick Anti-Shale Gas Alliance says:

“It has a chilling effect on the public. For instance ... if I stand in front of a truck, or parade in front of a business, if I don’t know if that’s going to put me in jail with a criminal record for terrorism, I’m much less likely to voice my opinion or take part in public discourse.”

These concerns have been compounded by the fact that CSIS, even with its existing powers, has already been caught spying extensively on law-abiding Canadians and sharing the information they collected with private companies. By instilling fear in law-abiding citizens, the vague and sweeping measures set out in Bill C-51 will chill free expression and curtail public debate on issues that are critically important for Canadian democracy.

One of the Bill’s provisions directly criminalizes the advocacy or promotion of terrorism. As it stands, it is illegal to aid or abet in a terrorist act, but the new Bill bans the advocacy or promotion of terrorism based on what many worry will be a loose interpretation.

This may sound sensible on the surface – who wouldn’t want to safeguard people from being “seduced” by terrorist propaganda? But again, Bill C-51’s frustratingly vague wording could easily entrap everyday Canadians. For example, it criminalizes not just the advocacy and promotion of terrorism, but also “being reckless” as to whether a statement might encourage others to commit a terrorist offence.

As legal analysts at the Canadian Centre for Policy Alternatives (CCPA) point out, this new offence “will bring within its ambit all kinds of innocent speech, some of which no doubt lies at the core of freedom of expression values that the Charter was meant to protect.”

The scope of these new measures are so wide that even the Conservative Party appears to have breached its own proposed law by posting a social media share image, depicting an Al-Shabab terrorist threat against the West Edmonton Mall. The image could be interpreted to contravene the clause in C-51 prohibiting “any writing, sign, visible representation, or audio recording that advocates or promotes the commission of terrorism offences in general.”
Luckily for the Conservative Party’s social media team, Bill C-51 was not yet in effect – but the incident does serve to illustrate how easy it would be for any Canadian to be criminalized and potentially face a 5-year jail term for innocent speech.

Warrantless access to your personal information

The Bill also proposes to allow CSIS to gain access to vast amounts of Canadians’ private, sensitive information without their knowledge or consent.

Canadians provide a great deal of personal information to the government during the course of their everyday lives. Whether it’s completing a passport application, filing your taxes, or applying for a new health card, it’s practically impossible to live one’s life in Canada without entrusting personal information to the government.

Under the Privacy Act, the government promises in return to keep such information secure and use it only for the purpose it was intended for. The Privacy Act also stipulates that government departments should not share your personal information widely with other government departments or agencies.

We are on the cusp of losing these necessary checks on government power. If passed in its current form, Bill C-51 will undo these safeguards, allowing CSIS to access a vast range of private information about Canadians – including passport applications and sensitive commercial data – without any requirement to obtain a warrant.

The federal Privacy Commissioner, Daniel Therrien, has fiercely criticized the impact these measures would have on Canadians.

“\The scale of information-sharing between government departments and agencies proposed in this bill is unprecedented. The new powers that would be created are excessive and the privacy safeguards proposed are seriously deficient.\”

“All Canadians – not just terrorism suspects – will be caught in this web. Bill C-51 opens the door to collecting, analyzing and potentially keeping forever the personal information of all Canadians in order to find the virtual needle in the haystack. To my mind, that goes too far.”

Following this criticism, the government barred Commissioner Thérien from testifying before the parliamentary committee studying the Bill.

Privacy expert and University of Ottawa law professor Michael Geist conducted a detailed analysis of these information sharing provisions, concluding that:

“The cumulative effect is to grant government near-total power to share information for purposes that extend far beyond terrorism with few safeguards or privacy protections.”
An expanded domestic spying role for the CSE

Finally, there are grave concerns that Bill C-51 will also result in a dramatically expanded domestic spying role for the CSE. As the next case study will explain, we already know that, contrary to government assurances, the CSE has long been engaged in large-scale surveillance of Canadians – and doing so is only going to get easier.

It looks like Bill C-51 will lead to a significant expansion of these domestic spying activities, given that the CSE is mandated to assist CSIS with its efforts. Michael Geist has described the Bill as a “punch in the gut” for privacy and civil liberties. He argues that the Bill, combined with what we already know about CSE activities, will have serious negative implications for the privacy of Canadians’ online activities:

“Moreover, these programs point to the fundamental flaw in Canadian law, where Canadians are re-assured that CSE does not – legally cannot – target Canadians. However, mass surveillance of this nature does not distinguish between nationalities. Mass surveillance of a hundred million downloads every week by definition targets Canadians alongside Internet users from every corner of the globe. To argue that Canadians are not specifically targeted when it is obvious that the personal information of Canadians is indistinguishable from everyone else’s data at the time of collection, is to engage in meaningless distinctions that only succeed in demonstrating the weakness of Canadian law.”

All this with no new oversight whatsoever

This enormous expansion of CSIS powers has not been paired with any commensurate increase in oversight - despite over two-thirds of Canadians and both leading opposition parties calling for precisely that.

In response, the government’s message amounts to not much more than “just trust us.” Officials from the Ministry of Public Safety even described additional oversight measures as “needless red tape.” Meanwhile, as we shall examine in more detail later, the current system responsible for oversight of CSIS is dangerously weak.

The government abolished the Office of the CSIS Inspector General in 2012, despite the crucial role the office played in overseeing day-to-day CSIS operations. All we’re left with now is the underfunded, part-time Security Intelligence Review Committee, which barely has the capacity to review CSIS activities years after the fact, let alone provide day-to-day oversight.

It is not that increased oversight and accountability alone will make up for Bill C-51’s other flaws — far from it. As Geist points out, “If we fail to examine the shortcomings within the current law or within Bill C-51, no amount of accountability, oversight, or review will restore the loss of privacy and civil liberties.”

That said, greatly improved oversight, accountability and transparency measures are a critical piece of the puzzle. We will later examine in more detail how the current shortcomings in this area can be addressed.

Canadians from across the political spectrum are speaking out against Bill C-51.
Case Study 2

The CSE and mass surveillance
The CSE (Communications Security Establishment) is Canada’s electronic eavesdropping agency. Operating within a global spy alliance called the ‘Five Eyes’, CSE works very closely with its counterpart agencies in the U.K., the U.S., New Zealand, and Australia. CSE’s roots date back to the Second World War, when it began as a military signals corps collecting foreign signals intelligence (SIGINT).

While CSE has been consistently active in spying operations since its beginnings in the 1940s, its surveillance capability, staff capacity, mandated powers and financial resources have expanded significantly since December 2001, when the Anti-Terrorism Act 2001 was ratified. Under this legislation, CSE was mandated to intercept the online communications of Canadians as long as it targeted foreigners. Since this time, CSE’s staff has more than doubled in size and the agency now employs over 2,000 people.

Online spying on a massive scale
CSE describes its work as being “focused on collecting foreign signals intelligence in support of the Government of Canada’s priorities, and on helping protect the computer networks and information of greatest importance to Canada.”

Despite these benign-sounding claims, we know from Edward Snowden that the CSE, along with its ‘Five Eyes’ partners, is in fact engaging in massive surveillance undertakings that are collecting, storing, and analyzing vast amounts of personal information and private communications from around the world, including from here in Canada.

Two recent revelations illustrate the vast scope and scale of CSE’s mass surveillance activities. According to government documents revealed by CBC News in partnership with The Intercept in January 2015, CSE is monitoring millions of Internet users’ file downloads every day, including Canadians’ file downloading activities.

These documents, sourced from Edward Snowden, reveal that Canada’s spy agency has been collecting and analyzing up to 15 million file downloads daily. Journalists Glenn Greenwald and Ryan Gallagher conclude that this dragnet search program, codenamed LEVITATION, reveals that the Canadian government has “launched its own globe-spanning Internet mass surveillance system.”

"CSE should start offering free online backup services. They seem to be collecting everything anyways."
- Josh, talking about CSE spying revelations

One OpenMedia community member’s response to the LEVITATION revelations.
Just a few weeks later, **CBC News** and **The Intercept** again teamed up to reveal that CSE is systematically collecting millions of private emails being sent by Canadians to the government, including emails sent to their local Members of Parliament. The content of these emails is being stored in giant government databases for months, with some information retained for years.

There is no doubt that the type of information being collected by CSE can be used to paint a highly revealing portrait of any individual. For example, according to surveillance expert Professor Ron Deibert, the bulk collection of metadata gives intelligence agencies the power to “pinpoint not only who you are, but with whom you meet, with what frequency and duration, and at which locations.”

**Innocent citizens under the microscope**

Of course, any system of mass online surveillance by definition ensnares innocent people. The process by which CSE sifts through large volumes of information exposes the private activities of millions of Internet users, including Canadians, who are completely innocent of any wrongdoing. As privacy expert Michael Geist points out:

“The program removes any doubt about Canada’s role in global Internet surveillance and highlights how seemingly all Internet activity is now tracked by intelligence agencies. They are able to track who visits various websites and what they do from the outside, confirming the existence of a massive surveillance architecture of global Internet traffic that improved oversight in Canada alone would do little to address.”

As recent revelations show, just clicking a link or writing to your Member of Parliament is now enough to place you under the government’s microscope.

**Canadians spying on Canadians**

Remarkably, until a couple of years ago, CSE remained largely hidden from public attention. Most Canadians were unaware of the agency’s activities, and many were not even aware of its existence.

In June 2013, however, **The Guardian** and **The Washington Post** published a number of confidential documents, sourced from whistleblower Edward Snowden, that revealed details about the pervasive and extensive government spying activities of the U.S. Government. The revelations included information on PRISM, the spy program that gives the U.S. NSA direct access to vast quantities of private communications hosted by Google, Facebook, Apple, and many other Internet companies.

Subsequent Snowden leaks exposed a wide range of other covert government spying projects being conducted in Canada. These revelations have made clear that the ‘Five Eyes’, including CSE, are engaged in online spying on a previously unheard-of scale.

For many Canadians, the mid-2013 Snowden leaks marked the first time secretive agencies such as CSE and NSA were drawn into the media spotlight and subjected to public scrutiny. At the time, the government explicitly assured Canadians that they were not being “targeted” by CSE surveillance. Peter MacKay, then serving as Defence Minister responsible for CSE, told the House of Commons in June 2013 that:

“This program is specifically prohibited from looking at the information of Canadians. This program is very much directed at activities outside the country, foreign threats, in fact. There is rigorous oversight. There is legislation in place that specifically dictates what can and cannot be examined.”

Now, with the exposure of the CSE’s LEVITATION and email surveillance programs, Canadians have learned that, contrary to those clear assurances, their own government is in fact engaged in online surveillance on an indiscriminate, mass scale — and that Canadians are clearly among those impacted. As Michael Geist points out, “mass surveillance of a hundred million downloads every week by definition targets Canadians alongside Internet users from every corner of the globe.”
A long track record of harmful surveillance

A wide range of other CSE programs make clear that this agency is engaged in activities that are undermining democracy here in Canada, while tarnishing Canada’s reputation overseas. Key examples include:

- **Spying on law-abiding Canadian air travellers:** In January 2014, it was revealed that CSE monitored the free airport Wi-Fi at Pearson Airport to collect data on thousands of air travellers, including many Canadians, who were passing through the airport. The surveillance, conducted without a warrant, went as far as tracking travellers’ precise movements around the world for weeks afterwards. Responding to these revelations, privacy expert Ron Deibert described the activity as illegal and unconstitutional, telling the CBC, “I can’t see any circumstance in which this would not be unlawful, under current Canadian law, under our Charter, under CSEC’s mandates.”

- **Spying on the Internet’s backbone:** Documents published by Germany’s *Der Spiegel* have revealed that CSE, under a program codenamed EONBLUE, is actively monitoring vast amounts of private Internet traffic travelling across the Internet’s core. They have established over 200 locations from where, using a technique known as Deep Packet Inspection, they can examine almost everything that people do online, including the content of unencrypted communications. As Motherboard’s Matthew Braga points out, “Though the agency maintains it cannot legally track Canadians at home or abroad it is hard to fathom how such data could be exempt.”

- **Spying on the Toronto G20 and G8 summits:** The Snowden documents also reveal that CSE facilitated a huge U.S. NSA spying operation on Canadian soil during the Toronto G20 and G8 summits. According to the documents, the purpose of this operation was to “support U.S. policy goals.” The revelations sparked global outrage, particularly among Canada’s G20 partners.

- **Spying on Brazil’s Mining and Energy Ministry:** In 2013, it was revealed that CSE was conducting invasive surveillance against Brazil’s Mining and Energy Ministry, a key government department. Unsurprisingly, these reports triggered outrage in Brazil, and even prompted Brazilian President Dilma Rousseff to denounce Canada on Twitter.

Everyday activities can place any Canadian under a government microscope.

Brazilian President Rousseff: “The report reveals Canada’s spying on our mining area. The Foreign Minister will demand an explanation from Canada.”
While this last example may not have directly undermined the privacy of Canadians, it certainly tarnishes Canada’s international reputation and other allies’ goodwill when it comes to respecting Canadians’ privacy and security. The exposure of this type of economic espionage also directly refutes the government’s oft-repeated claim that CSE’s spying activities are necessary to safeguard Canada’s national security. In this case, the spying was clearly aimed at undermining the economic interests of Brazil, supposedly a key Canadian ally in the Americas.

**Guess who is footing the bill?**

Of course, none of these activities come cheap. CSE’s rapidly increasing annual budget now costs taxpayers over $800 million each year. In large part this is due to the construction of an elaborate new headquarters building, dubbed a ‘spy palace’ by CBC News, featuring state-of-the-art architecture and luxury accommodations for government workers.

“The fritted glass on the curtain wall features patterns suggestive of the activities within and will be designed by the users.” – WZMH Architects, Overview of CSE HQ project

This new headquarters will cost $1.2 billion to build and a further $3 billion to operate, making it the most expensive Canadian government building ever constructed. The extravagance of this project has understandably raised serious concerns about how enormous amounts of taxpayer money are being funneled into surveillance activity.

**As we shall see later, it’s also notable that the government watchdog tasked with reviewing CSE activities is starved of funds, operates with a staff of just eight people, and has to make do with a budget of just $2 million per year.**

In sum, Canadians are spending billions on a secretive, unaccountable government agency that is engaged in mass, suspicionless surveillance. Canadians, along with Internet users across the globe, are being caught in CSE’s spying dragnet, whereupon their personal information is shared with foreign agencies including the U.S. NSA.

There is no effective independent oversight whatsoever of this agency’s activities, which evidence increasingly suggests are actually making us less, not more, safe. It’s no wonder that debate is now turning to what needs to be done to rein in CSE and restore Canadians’ privacy rights.

**Internet Voice**

“A budgetary limit should be placed that adequately represents [the] value the agency provides Canadians. A billion dollar facility is just complete irresponsible spending. A billion dollars in health care would have saved more lives in one month than a spy agency could even help in several decades.”

– Steve S.

“Horrifying that the Harper government decided The Great Lakes Research Centre that needed a few million dollars was too expensive and yet this CSE Spy Palace is justified.”

– Moira R., Internet Town Hall participant
How Canada’s secret spying program sees you

Here’s what your online activity could tell the government

1. This is Jane. Jane has friends and relatives all over the world. She keeps in touch with them via email, phone calls, text messages and video chats.

2. Jane’s information could be scooped up by the ultra-secretive Communications Security Establishment Canada (CSEC) under secretive ministerial directives—directives that allow CSEC to collect & analyze the online and phone activity of Canadians and communications with someone outside the country.

3. (Here’s one way) CSEC could be collecting your private, sensitive information:

   - **CSEC Databases**: A sea of CSEC analysts (CSEC employs over 2,000 people)
   - **Phone**: Your phone data, including a phone call to a contact in any country, is sent to analysts.
   - **Internet**: Your sensitive, private information is scooped up by technologies that capture internet traffic & communications (e.g., metadata, internet address, your telephone address, the time of each call).

4. Some of what CSEC spying could reveal about you:

   - Jane’s friends, family & intimate relationships & their friends, family & intimate relationships
   - Medical Conditions
   - Sexual Orientation
   - Political Beliefs
   - Financial Information
   - Religious Beliefs

Take action now to stop secret spying on Canadians: OpenMedia.ca/CSEC
Case Study 3

Bills C-13 and S-4: Undermining the privacy of every Canadian
Recently passed, Bill C-13, the Protecting Canadians from Online Crime Act, poses substantial threats to our privacy online. When first tabled, the government touted C-13 as an anti-cyberbullying bill. However, it rapidly became clear that only a few pages of the Bill dealt with cyberbullying, while over 60 pages greatly expanded the state’s capacity to spy on citizens.

OpenMedia’s Executive Director Steve Anderson crowdsourced concerns from Canadians about Bill C-13, which he then reflected in his testimony to the parliamentary committee studying the Bill. The three key concerns Canadians wanted Steve to highlight were:

- Immunity for activities that victimize innocent Canadians;
- Accountability and oversight; and
- Data security

A wide range of experts, including federal Privacy Commissioner Daniel Therrien, have also warned about how Bill C-13 undermines the privacy of Canadians. The Bill grants immunity to telecom providers who disclose private information about their customers to law enforcement, without a warrant. The Bill also makes it far easier for government to obtain deeply revealing metadata on targets, based merely on suspicion.

Under Bill C-13, a wide range of government officials and public officers can now access Canadians’ personal information without their knowledge or consent. Writing in the National Post, journalist Justin Ling warned readers that “the officers obtaining that data can be anything from tax agents to sheriffs, reeves, justices of the peace, CSIS agents, and even, yes, mayors.” This means that a local police officer, or even your local town mayor, could have access to your personal information, often without a warrant.

While Bill C-13 provides these officials with substantial power over your information, it leaves the targets of such surveillance with little by way of legal recourse – not least because they are not even informed that their privacy has been breached.

As the NDP’s Digital Issues critic Charmaine Borg told Parliament, Bill C-13 allows companies like Bell and Rogers to voluntarily disclose their customers’ personal information to government officials without the need for a warrant and with no judicial oversight.

This is not a minor issue – statistics obtained by the federal Privacy Commissioner revealed that these kind of warrantless requests for information were happening at a staggering rate of over 1.2 million times a year, with over 725,000 individual Canadians affected.

Thankfully, last year’s Supreme Court of Canada R. v. Spencer ruling should shield Canadians from the worst of these abuses. The court ruled unanimously that warrantless requests from law enforcement are unconstitutional. Despite this ruling, however, the government pressed ahead with Bill C-13, choosing to overlook the fact that the legislation clearly encourages unconstitutional behaviour.

Internet Voice

“Stop passing Bill C-13 now because it does not protect Canadians from cyberbullies, it violates their privacy laws. Bill C-13 is just a lie, to trick you into thinking that they will protect you from cyberbullies even though they are becoming the bullies by watching or monitoring all of your activities online and on multiple devices.”

– Mohammed V.
Parents speak out

Despite being promoted as an anti-cyberbullying bill, C-13 could in fact make things worse for teens online by undermining their right to privacy. Parents of cyberbullying victims have protested the Bill’s sidestepping of proper legal action, noting that the Bill opens up dangerous provisions for surveillance and erodes privacy. Carol Todd, mother of cyberbullying victim Amanda Todd, spoke out against the provision, saying, “I don’t want to see our children victimized again by losing privacy rights.”

By removing legal protections against warrantless surveillance, Bill C-13 could create more victims than it prevents.

This dangerous piece of legislation also reflects a broader pattern in Canadian politics: the erosion of privacy accompanies the erosion of democratic values. As privacy expert Tamir Israel of the Canadian Internet Policy and Public Interest Clinic (CIPPIC) says,

“Privacy is essential for a healthy democracy. If left unchecked, the activities of Canada’s state surveillance apparatus are harmful to all Canadians. We’re calling on the government to take its obligation to protect privacy seriously.”

While many Canadians have requested strong, transparent and properly enforced safeguards to secure privacy rights online, the government has proceeded with warrantless spying projects without proper consent from the broader public.

Ultimately, over 73% of Canadians opposed the Bill, including a majority of the government’s own Conservative Party supporters. Despite this widespread opposition, the government pushed the legislation through Parliament, and it became law in early 2015.

Bill S-4 and the expansion of information disclosure

Bill S-4, the Digital Privacy Act, is another example of how the government appears to be systematically dismantling Canadians’ online privacy rights.

According to privacy expert Michael Geist, the government assured Canadians that this Bill “will provide new protections for Canadians when they surf the web and shop online,” but it actually allows your Internet provider to sell you out to anyone looking to sue you by handing over your private data without consent or a court order.

Bill S-4 proposes amending Canada’s private sector privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), to “specify the elements of valid consent for the collection, use or disclosure of personal information,” among other things.

These amendments “permit organizations, for certain purposes, to use and disclose, without the knowledge or consent of an individual, personal information,” without a court order in any situation where another organization claims you have violated its rights. They will also permit organizations to give state agencies such as CSE massive amounts of private data implicated in a cybersecurity breach, which can include sensitive financial, medical or other information of innocent Canadians. These agencies can keep this data indefinitely and use it for other purposes, all without a warrant.
Essentially, this problematic Bill is yet another example of how the government has eroded legal safeguards online in favour of providing potentially hostile organizations, such as U.S.-based copyright trolls,\(^8^9\) with unfettered access to our personal data. This is highly worrying insofar as it leaves your legal rights in the hands of private organizations, rather than in the court of law.

**Systematic dismantling of privacy safeguards**

Together, C-13 and S-4 threaten to dismantle important legal protections against the warrantless disclosure of personal information. They effectively encourage private companies, including Internet providers, to hand private customer information to the government, and even to other private entities. These disclosures would be made without a warrant or court order, and without any requirement to notify the victim – thereby preventing victims from legal remedy.

When looked at against the backdrop of sweeping CSE mass surveillance, and the government’s new Bill C-51, it’s clear that Canadians face a privacy deficit of alarming proportions.

"Privacy is essential for a healthy democracy. If left unchecked, the activities of Canada’s state surveillance apparatus are harmful to all Canadians.”

Tamir Israel of the Canadian Internet Policy and Public Interest Clinic (CIPPIC).
CHAPTER TWO

How Canadians Want To Address Our Privacy Deficit
Recommendation 1

Get a Warrant
We presented participants with a range of options, asking in which circumstances government agencies should be able to access the sensitive, personal information of Canadians. The result was clear: Canadians overwhelmingly believe government agencies should require a search warrant based on evidence that a crime is soon to be, or has been, committed in order to access citizens’ personal information.

The traditional process of obtaining a warrant features a number of safeguards to protect the privacy of Canadians. Under the Charter, police must usually provide *reasonable and probable grounds, established upon oath, to believe that an offence has been committed and that there is evidence to be found at the place of the search.*

The standard to obtain a warrant is therefore stronger than mere suspicion. The judge assessing the warrant application must be satisfied that evidence of an offence is reasonably likely to be found if a search is approved. This system ensures that Canadians are protected from law enforcement overreach, while also ensuring that law enforcement agencies can do their job.

93.8% of participants in our crowdsourcing said warrants should be necessary for police to conduct a search. Only 5.4% of respondents would allow police to conduct searches based merely on suspicion that an offence has been committed. Just 0.4% believed personal information should be generally available to government agents, and a further 0.4% said police should be allowed to access information based on broad demographic descriptions (e.g. “all middle-aged white females living in Hamilton.”)

### Internet Voice

“Follow democratic principles and protect Canadians from being watched without a warrant or justification.”

– Soraya M.

**Q2. In what circumstances should government agencies, such as CSE, CSIS, or law enforcement, be able to access the sensitive, personal information of Canadians?**

- When a judge grants a search warrant based on evidence that a crime is soon to be, or has been, committed: 93.8%
- When a police officer or government agent suspects that someone is possibly involved in wrongdoing, but they don’t have enough proof to get a warrant: 5.4%
- When they fit a broad demographic description (e.g. “all middle-aged white females living in Hamilton”): 0.4%
- Personal information should generally be available to the government when it is conducting investigations, without their needing to obtain a warrant: 0.4%

**n = 1,916**

**Internet Voice**

“We NEED to set up some good safeguards to protect citizens’ privacy. Privacy is a right and one of the most pressing issues of this digital age.”

– Assyja M.

Canadians have a straightforward request for government agents seeking to obtain their personal information: get a warrant.
When Canadians were asked to rank six key privacy priorities in order of preference, “require a warrant for government to spy on personal information” came top of the aggregate priority rankings. 22.7% of participants chose it as their top priority, and fully 68.9% chose it as one of their top three priorities, alongside “ending blanket surveillance of law-abiding people,” and “more transparency around govt collection of personal data.”

These findings are broadly consistent with other studies. The federal Privacy Commissioner’s recent detailed survey of attitudes to privacy found that warrantless information requests topped the list of concerns. By a margin of 3.5:1 Canadians said they were “very uncomfortable” with the government requesting personal information from telecom companies without a warrant. A Forum Research poll found that 69% of Canadians disapprove of telecom companies handing over information to a public official without their knowledge or consent; only 18% of respondents approved.

Police require a search warrant to enter your home – but what about your digital home?

Based on these findings and the response to our crowdsourcing process, Canadians feel a strong attachment to the judicial safeguards inherent in a legal system that requires a warrant to search or obtain one’s personal information. This is unsurprising given the deep historical roots of this basic privacy protection in common law systems.

As far back as 1765, chief justice Lord Camden, presiding over the Court of Common Pleas in England, condemned the government’s use of an illegal warrant to “search, seize, and carry away” the papers of an allegedly seditious London writer named John Entick. Lord Camden’s ruling first established in common law the general principle that the state may not invade the privacy of a citizen unless expressly authorized by law.

The legal principle that “your home is your castle” goes back even further, to the days of Ancient Rome, and was first established as common law by Sir Edward Coke in 1628.

For a man’s house is his castle, et domus sua cuique est tutissimum refugium [and each man’s home is his safest refuge], for where shall a man be safe, if not in his house?.”

Sir Edward Coke, The Institutes of the Lawes of England (1628)
In Canada, government authorities have long been required in many circumstances to obtain a search warrant to access people’s personal information. In modern times, this requirement balances law enforcement’s needs with the privacy protections rooted in section 8 of the Charter:

Everyone has the right to be secure against unreasonable search or seizure.

Section 8. Charter of Rights and Freedoms

There are exceptions: for example, police can use diminished suspicion-based grounds to obtain information during the search of a motor vehicle. But when it comes to entering your home, the rules are clear. In all but a very limited number of cases, police require a search warrant to enter your bricks-and-mortar home.

However, when it comes to entering our digital homes, things are different. Although the Charter does establish safeguards on when the government can use electronic surveillance powers, the law has not kept pace with rapid technological advancements in recent years, especially when it comes to searching our personal electronic devices. For example, the Supreme Court recently ruled that police can, with some restrictions, search the smartphones of people they arrest.

What is especially concerning is that our smartphones, laptops, and other digital devices store so much information on us, that searching them can, if anything, be even more revealing than a thorough search of one’s actual home. We also know from experts that our communications metadata can expose the most intimate details of our private lives – everything from our financial status, to medical conditions, political and religious beliefs, and even our sexual orientation.

Undermining trust in our digital security

A number of recent developments have made it far easier for government to obtain Canadians’ personal information either without a warrant or with a weak standard that is disproportionate and ignores the targeted approach adopted in traditional warrants. These developments have further undermined Canadians’ trust in the security of their digital homes:

Weak thresholds for obtaining a search warrant:

The government’s Bill C-13 received Royal Assent in December 2014 after over a year of fiercely contentious debate. As mentioned in our earlier case study, the new law makes it far easier for law enforcement agencies to obtain a transmission data warrant. Such a warrant allows police to obtain deeply revealing metadata about a surveillance target.

Under Bill C-13, police now merely need to demonstrate a “reason to suspect” that a target is involved in criminal wrongdoing, rather than a “reason to believe.” This may not seem like much on the face of it – but legally, it means a great deal. This lower threshold makes it significantly easier for the
government to sweep up many innocent people’s personal information, based merely on suspicion. As federal Privacy Commissioner Daniel Therrien points out:

_The bulk of the new powers may be used where investigators have a mere suspicion of wrongdoing, as opposed to a higher threshold of reasonable belief that the search will provide evidence of a specific crime. The difference between these two thresholds represents a marked difference in privacy protection._

Law professor and privacy expert Michael Geist underlined how revealing such transmission data can be. In testimony before the Senate’s Legal and Constitutional Affairs Committee, Professor Geist said:

_There has been some confusion regarding how much metadata is included as ‘transmission data’. This is far more than who phoned who for how long. It includes highly sensitive information relating to computer-to-computer links. This form of metadata may not contain the content of the message, but its privacy import is very significant._

The rapid pace of technological change over recent decades, in addition to the fact that Canadians increasingly store and transmit large quantities of sensitive information through their digital devices, means that there is now a very high level of privacy interest in this type of information.

These provisions of Bill C-13 show a worrying disregard for this privacy interest. The last thing Canadians want is even weaker safeguards protecting their metadata. Search warrant requirements should reflect the privacy significance of the information sought, and the new threshold set out in Bill C-13 wholly fails to do so.

**Warrantless disclosure of personal information:**

Bill C-13 granted full civil and criminal legal immunity for the voluntary disclosure by telecom companies of their customers’ personal information without a warrant. This provision has prompted a great deal of controversy, particularly given revelations from the Privacy Commissioner that Canadian telecom companies were asked to disclose personal information about their customers a remarkable 1,193,630 times, affecting 785,000 individual Canadians, in a single 12-month period.

In fact, the Supreme Court of Canada definitively ruled in June 2014 that it is unconstitutional for law enforcement agencies to request subscriber information without a warrant, in _R. v. Spencer_. Despite this pronouncement by the highest court in the land, the government pressed ahead with the immunity provision in Bill C-13.

The ruling also showed that telecom providers have a duty of privacy toward their customers, meaning that it may even be illegal for them to voluntarily disclose such information without a request. Although some telecom companies have responded to this ruling by pledging to cease warrantless disclosure, others such as Bell have remained silent.

This provision is a major concern, particularly given the often vast quantities of personal information held by telecom providers about their customers. Even handing over something as apparently innocuous as a name and address can be hugely revealing if also linked to an IP address – potentially exposing an individual’s entire digital trail.

---

**Internet Voice**

“If the privacy rights of law-abiding Canadians are compromised we will have broken with perhaps the best descriptors a country can proudly bear: Strong & Free. Government in Canada needs to implement measures that raise awareness around our privacy rights and freedoms.”

– Rachel C.
STEPS TO IMPLEMENTATION:

This recent trend toward weaker privacy safeguards is not unstoppable. It’s clear that Canadians want to see this trend reversed: a Forum Research poll revealed that 79% expect their online personal information to remain “private and confidential.”

What steps need to be taken to restore Canadians’ trust in their system of warrant safeguards? What needs to be done to ensure that law enforcement practices are brought back into compliance with the letter and spirit of the Charter?

Based on research and consultations with Canadians and experts from across the country, Canada’s privacy deficit should be addressed by implementing the following recommendations:

1. **End legal immunity for ‘voluntary’ warrantless disclosure of personal information:**

   Bill C-13 granted telecom providers legal immunity for ‘voluntarily’ handing their customers’ private information to the government without a warrant. This clause (now section 487.0195 (1) and (2) of the Criminal Code) should be repealed.

   Although *R. v. Spencer* prohibited law enforcement from requesting personal information without a warrant, ambiguities remain regarding its application to a number of voluntary information-sharing contexts. With major telecom conglomerates like Bell Canada refusing to confirm whether or not they have ceased the warrantless handover of information, Canadians have little cause for confidence that any remaining ambiguities will be resolved in favour of their privacy. Canadians should have the right to seek legal recourse if their telecom provider discloses their personal information without a warrant.

2. **Strengthen transmission data warrant thresholds to “reasonable belief”:**

   In order to obtain the personal data of Canadians at home or overseas, police and other government agencies must be required to obtain a warrant. For reasons outlined above, the ‘reason to suspect’ threshold enshrined in Bill C-13 is far too weak, effectively allowing for these intrusive searches to be self-authorized by law enforcement.

   Suspicion alone is not enough to place a Canadian’s private online life under a government microscope. There should be a meaningful threshold in order for the government to monitor any Canadian’s private online activity or obtain their personal information.

   As recommended by the federal Privacy Commissioner, police should need to meet the much stronger ‘reason to believe’ threshold in order to obtain someone’s personal online information. A judge would then need to consider whether the proposed surveillance is necessary, legitimate, and proportionate. This common sense step would also be in line with the Supreme Court’s unanimous *R. v. Spencer* ruling and would significantly strengthen online and offline privacy protections for Canadians.

3. **Mandatory reporting of subscriber data requests:**

   We’ve already seen that 1.2 million requests for private subscriber data were submitted to telecom companies within just 12 months. However, the federal Privacy Commissioner had to work hard to bring these alarming statistics into the public domain, battling against delaying tactics by the telecom firms.

   In early 2014, the NDP’s Digital Issues critic Charmaine Borg directed a number of questions to government agencies including the RCMP about these warrantless subscriber data requests. The RCMP’s response revealed that they failed to even keep records of how often they collected subscriber data without a warrant, a fact subsequently confirmed by the Privacy Commissioner.

   Clearly, both law enforcement agencies and telecommunications companies should be more attentive to and transparent about what they do with Canadians’ private data. Federal and provincial government agencies should have a statutory duty to report to the public on a regular basis as to the number of subscriber data requests they process. These reports should be made available online in an accessible format, and include not just overall numbers, but also data retention periods and relevant law enforcement agency guidelines. This is the only way for Canadians to gain a clear understanding of the scope of this issue.

4. **Require greater transparency from telecom companies:**

   Telecom providers have a crucial role to play in working for stronger data privacy protections for their customers. They should have a statutory duty to report to the public about the number of subscriber data requests they receive, the number of such requests they approve, and their reasons for doing so.

   All telecom providers should also be required to implement the expert recommendations of Professor Andrew Clement and Dr Jonathan Obar’s recent *Keeping Internet users in the know or in the dark?* report, including publishing annual transparency reports in addition to detailed information on their websites about their data privacy and transparency practices.

   Legislators should update PIPEDA (Canada’s private sector privacy law) to include proactive transparency around privacy policies, and to require proactive notification of third party disclosure requests.
5. Bring Canada’s 35 year old Privacy Act into the Digital Age:

For some time, the Office of the Privacy Commissioner has pushed for reform of the federal Privacy Act, which sets out how federal government departments and agencies should safeguard the privacy of Canadians. Former Privacy Commissioner Jennifer Stoddart made the case for the “urgent need” for reform in a speech at the Library of Parliament in 2013. Her office has also published twelve ‘quick fix’ reform recommendations, which the government has to date ignored. These common sense recommendations deserve to be implemented as soon as possible.

The need for reform has grown all the more urgent given the sweeping expansion of information sharing proposed by Bill C-51. As we have seen, these provisions threaten to overturn the core principle of the Privacy Act – that government agencies should use personal information strictly for the purpose for which it is provided, and should not share that information with other agencies, except in tightly restricted circumstances. The government has failed to make the case for the necessity of these extreme new powers. These provisions in C-51 should be rejected by Parliament. If passed these provisions will certainly need to be repealed by a future Parliament.

6. Mandatory notification of surveillance targets:

Individuals subjected to surveillance should be notified after the fact, unless there is a risk that such notification would jeopardise the initial purpose of the surveillance. Where there is such a risk, notification should be delayed until that risk is lifted. This would afford surveillance targets the opportunity to take legal action and seek remedy for any illegal violation of their privacy. These measures should be in addition to the existing after-the-fact notification regime for warranted wiretaps.

7. Require a warrant to search cell phones and other digital devices:

The Supreme Court’s R. v. Fearon ruling significantly weakened Canadians’ digital privacy, by granting police the power to search cell phones without a warrant pursuant to arrest. The court ruled that such searches are supposed to be limited, but the ‘test’ they proposed opens up a great deal of legal uncertainty, not least for the police officers responsible for interpreting and applying the test.

Given the huge amount of deeply personal information many Canadians entrust to their digital devices, this is a worrying development. As the dissent written by Justice Karakatsanis points out: “The fact that a suspect may be carrying their house key at the time they are arrested does not justify the police using that key to enter the suspect’s home. In the same way, seizing the key to the user’s digital life should not justify a wholesale intrusion into that realm.”

Professor Michael Geist concluded in response to the ruling: “In trying to establish the legality of some warrantless cellphone searches, [this decision] has replaced the important safeguard of a judicial authorization with conditions that do little to protect privacy while complicating the obligations of law enforcement.”

Put plainly, being under arrest does not mean somebody is guilty of a crime. People under arrest should not have their privacy rights stripped away without judicial authorization or oversight. Also of concern is that the Canadian Border Services Agency routinely conduct warrantless searches of the cell phones of people entering Canada, including devices owned by Canadian citizens and permanent residents.

Post-Fearon, it seems Canadians can no longer rely on the privacy protections afforded by Section 8 of the Charter to safeguard the security of their digital devices. For this reason, legislation is required to make clear that a warrant is necessary for police, or any other security or law enforcement agency, to search somebody’s digital device. This is the only way to ensure that the privacy safeguards around digital devices match Canadians’ inherent privacy interest in them.

8. Prohibit the ‘voluntary’ disclosure of personal information by organizations:

Canadians deserve legislative protections that prohibit organizations, such as telecommunications service providers, from disclosing Canadians’ personal information to authorities or private litigants without a court order or demonstrated case of exigent circumstances.

There should also be a comprehensive review and reform of any federal law or regulation that permits, encourages, enables, or requires warrantless voluntary disclosure of online activity to police, the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment (CSE), or private litigants.

9. Safeguard privacy in emergency situations:

In 2013, during the Alberta floods, the RCMP seized over 600 legally-owned firearms from over 100 homes in the town of High River. The RCMP forcibly entered the homes, many of which has already been evacuated, and seized residents’ property without a warrant, including guns that had been properly secured and were not in plain view. The RCMP also failed to notify a judge about their actions, as the RCMP watchdog later found they were required to do by law. In an emergency situation, there needs to some reasonable leeway for police and first responders to, for example, enter someone’s home without a warrant for the purpose of searching for survivors. The recommendations of the RCMP watchdog for stronger guidelines, education of police officers, and better record keeping should be implemented to ensure that future emergencies do not grant police a blank cheque to search and seize private property.
10. **End the use of drones to conduct warrantless surveillance:**

A number of recent reports make clear that Canadian law enforcement agencies are now using drone technology to conduct surveillance. For example, drones were deployed last year to monitor peaceful Mohawk protesters who were calling for an inquiry into missing and murdered indigenous women. A 2013 Queen's University report revealed that the Ontario Provincial Police were operating at least four drones in Northern Ontario, and that drones were also in use by the RCMP.

Some police drone usage is perfectly sensible – for example, when they are used to take aerial photos of traffic collisions to map out what happened. However, there is not adequate regulation of the continued expansive use of drones for surveillance and other purposes by law enforcement agencies. Nor is there sufficient knowledge of how long audio or written surveillance records are kept and used, or even knowledge of whether some drones could become weaponized. There is a need for a proper independent review of uses of unmanned aerial vehicles for surveillance purposes by law enforcement agencies or by private sector entities.

The Privacy Commissioner has pointed out that drones are “a powerful surveillance tool” capable of carrying advanced surveillance technologies. As with all surveillance activity, spying conducted by advanced technology should require a warrant. Such a warrant should only be granted in carefully circumscribed situations – for example, if a judge is satisfied that its use is necessary, targeted at a specific individual, proportionate (the least intrusive way to obtain the information), and based on a reasonable belief that a crime is soon to be, or has been, committed.

In light of the rapid expansion and development of these kind of technologies, the Canadian government must adhere to lawful practices of surveillance by maintaining the necessity for a search warrant in order to exploit any current or future technology for surveillance purposes.
Recommendation 2

End Mass Surveillance
What Canadians Want:

Participants in our crowdsourcing survey expressed deep concern about mass surveillance – they want to see an end to the practice. Key findings from our crowdsourcing process include:

• 93.8% said CSE, CSIS, and other government agencies should only be able to obtain Canadians’ sensitive personal information when a judge grants a warrant to conduct surveillance against a specific target.

• When we presented crowdsourcing participants with six key privacy priorities, “End blanket surveillance of law-abiding people” came second only to “Require a warrant.” Fully 60.8% of participants chose ending blanket surveillance as one of their top three priorities.

• 89.1% want to see all surveillance activities require a warrant approved by a judge.

• 92.2% said CSIS and the RCMP should be forbidden from using public resources to monitor peaceful individuals, organizations, and groups not posing any known threat to national security. Only 2.3% believed this was appropriate.

• Mass surveillance, including the bulk collection of deeply revealing metadata, is by definition conducted without a warrant. Canadians overwhelmingly believe the government should obtain a warrant before spying on personal information. 68.9% listed this among their top three privacy priorities, with 22.7% choosing it as their top priority.

Once again, these findings are reinforced by independent surveys. The federal Privacy Commissioner’s 2014 Survey of Canadians found that 77% were “very concerned” about law enforcement and security agencies collecting their personal information for surveillance purposes. A Forum Research poll also found that just 8% of Canadians trusted the CSE with their personal information, with only 23% trusting CSIS, and 37% trusting the RCMP.

These results are unsurprising, given what has been revealed about Canadian spy agency activities, and those of their ‘Five Eyes’ partners, over the past couple of years. Thanks to Edward Snowden, people are increasingly aware that surveillance is being conducted on a massive scale, and that it takes no suspicion of wrongdoing to find oneself under the government’s microscope. The Privacy Commissioner’s recent survey found that roughly half of all Canadians had seen, read, or heard something about the surveillance revelations in the past year.

As outlined earlier in this report, a number of specific revelations would have laid to rest any notion that Canadians were immune to mass surveillance. People learned that, for example, the CSE spied on thousands of innocent Canadian air travellers. And that under the CSE’s LEVITATION program, just clicking a link could get you caught in the government’s surveillance dragnet.

Our findings and dozens of independent reports confirm that Canadians have a right to be concerned. Mass surveillance contributes to our privacy deficit and weakens our democracy in a number of important ways.

Undermining human rights

A wide range of human rights organizations, international institutions, and privacy experts have spoken out about how mass surveillance activities, especially the bulk collection of metadata, undermine citizens’ fundamental human rights:

• Former Ontario Privacy Commissioner Ann Cavoukian has warned about how metadata can be used to paint a deeply revealing portrait of any individual’s private life. The Ontario Information & Privacy Commissioner’s 2013 report A Primer on Metadata: Separating Fact from Fiction explains how metadata, when collected in bulk, can be even more revealing than the actual content of private communications:

“Metadata surveillance programs gather and analyze private sector metadata involving the activities of the public. In so doing, they facilitate the state’s power to instantaneously create a detailed digital profile of the life of anyone swept up in such a massive data seizure."
Once this data is compiled, detailed pictures of the lives of individuals begin to emerge that may easily be linked to places and events.\textsuperscript{25}

\begin{itemize}
  \item Here in Canada, the CSE’s mass surveillance practices are the subject of an ongoing constitutional challenge from the British Columbia Civil Liberties Association (BCCLA). Stating that “secret and unrestrained government surveillance presents a grave threat to democratic freedoms”, the BCCLA challenged the bulk collection of metadata on the grounds that:

  “The collection of metadata is digital surveillance. CSEC spies on Canadians by collecting information every time an email or text message is sent, every time a phone call is made, every time the internet is accessed. CSEC can collect, retain and analyze this personal information to create a picture of a Canadian and his or her relationships with other Canadians... This kind of widespread surveillance without accountability is fundamentally incompatible with Canadian democracy.”\textsuperscript{26}

  \item Malte Spitz, a German politician and privacy advocate, obtained six months of his mobile phone data from his wireless provider. He provided this to Die Zeit which, combining it with data from other publicly available sources, used it to create a detailed narrative of Mr Spitz’s activities over the six month period. The resulting animated map revealed Mr Spitz’s travels, activities, political speeches, time spent on the phone, and time spent online. Die Zeit concluded that:

  “This profile reveals when Spitz walked down the street, when he took a train, when he was in an airplane. It shows where he was in the cities he visited. It shows when he worked and when he slept, when he could be reached by phone and when was unavailable. It shows when he preferred to talk on his phone and when he preferred to send a text message. It shows which beer gardens he liked to visit in his free time. All in all, it reveals an entire life.”\textsuperscript{27}

  This is significant because it underlines that metadata can paint an incredibly detailed picture of someone’s private life not just in the present day, but going back months or even years, depending on how long the metadata is retained for.

  \item Concerns about how the bulk collection of metadata can undermine human rights are shared in other jurisdictions. For example, the parliamentary assembly of the Council of Europe’s Legal Affairs Committee stated in a January 2015 report that mass surveillance, including the bulk collection of metadata, threatens basic human rights. The report also ruled that the U.K. GCHQ’s mass surveillance activities contravened article 6 (right to a fair trial), article 8 (right to privacy), and article 10 (right to free expression) of the European Convention on Human Rights. The report concludes that:

  “The ‘Snowden files’ have shown the extent of the threat mass surveillance represents for our privacy and other human rights whose effective exercise depends on privacy – such as freedom of expression and information, even freedom of religion, the right to a fair trial and the right to equal treatment.”\textsuperscript{28}

This concern was and is understandable – bulk collection of metadata by definition circumvents the entire system of warrant protections. This practice is also the subject of a constitutional challenge, mentioned above, from the B.C. Civil Liberties Association,\textsuperscript{131} supported by OpenMedia and a range of other pro-privacy organizations.\textsuperscript{132}

The government and the CSE justify the bulk collection of metadata by claiming that metadata does not fit within their definition of “private communications.” However, as we’ve seen, metadata can in fact be used paint a vivid picture of a target’s personal life, past and present. For this reason, Canadians deserve robust safeguards to put an end to the government’s interception and collection of metadata.
**STEPS TO IMPLEMENTATION:**

Participants in our crowdsourcing project expressed clear concern about mass surveillance activity in Canada. We know that Canadians want to put an end to the widespread collection of their private data, and so we worked with experts to outline what that might look like in practice. This is not intended as an exhaustive list, but rather as an overview of what will need to be done to put a stop to surveillance abuses and better protect the privacy of Canadians. Here are the key components:

1. **End all suspicion-less mass surveillance, including the bulk collection of metadata:**

Any government surveillance is inherently invasive. For this reason, surveillance should only be conducted in a targeted manner, and only under a court order or warrant. Canadian intelligence agencies should cease all suspicionless surveillance activities that are directed against the general public, whether here in Canada or overseas.

The government should conduct an audit of all of CSIS and CSE’s ongoing surveillance programs, and halt any that involve the warrantless collection of Canadians’ personal information, including metadata, from the public. The secret Ministerial Authorizations issued by Peter MacKay in 2011 to spy on metadata should be made public and revoked. As proposed by Joyce Murray’s Bill C-622, new legislation should recognize the privacy value of metadata by defining it as protected information, thereby putting a stop to the bulk collection of metadata from the public.

These measures are necessary to stop and prevent any repetition of Canadian mass surveillance programs such as LEVITATION, EONBLUE, or the CSIS monitoring of members of peaceful advocacy groups. All future surveillance activities should be targeted and specific, rather than indiscriminate.

2. **Require judicial not political authorization for surveillance:**

In any democracy, citizens need to know how a law is being applied, in order to have an informed debate about whether that law needs changing. In Canada, the government has often reassured Canadians that surveillance activities are lawful, while keeping secret how “lawful” is interpreted. Much of CSE’s spying activities are approved by secret ministerial authorizations, such as those issued by Peter MacKay in 2011.

All intrusive surveillance activities should be authorized by a serving judge, where possible in an open court, instead of by a government minister. This would ensure that any such activities are consistent with the rule of law, and directed against specific targets instead of whole populations. New legislation governing surveillance powers should therefore take away the power of the Minister of National Defence to secretly authorize surveillance activities. Instead, as proposed by Joyce Murray’s 2014 CSEC Accountability and Transparency Act, this power should instead be vested in an independent judge of the Federal Court.

3. **No future expansion of surveillance without a verifiable need:**

Canadians deserve a clear government commitment to abstain from expanding surveillance, access to citizen data, or transmission of citizen data to other governments or agencies unless there is a clear, publicly accounted-for need that is demonstrated by verifiable evidence. Any expansions of information sharing or surveillance should be debated publicly, be clearly proportionate to the government’s stated needs, be demonstrably effective in meeting those needs, and should expand data collection to the smallest degree necessary to meet those needs.

4. **Prevent government agencies monitoring what Canadians say on social media:**

In November 2014 it was revealed that the government was creating a new system for collecting and analyzing what Canadians are saying on Facebook and other social media services. The system would offer “real-time monitoring and analysis of social media content including Twitter, Facebook, blogs, chatrooms, message boards, social networks and video and image sharing websites.” The move flew in the face of warnings published earlier in the year from the then federal Privacy Commissioner Chantal Bernier about government institutions collecting information from Canadians’ social networking profiles in violation of the Privacy Act.

When Canadians post on Facebook they believe they’re sharing with family and friends, not with a government bureaucrat in Ottawa. Long-standing confusion around Facebook’s privacy settings, however, means that often these messages are made publicly available, as opposed to just being visible to friends. The government’s new social media monitoring system appears to take advantage of this in order to systematically collect these often deeply personal communications.

Nor is this issue restricted to social media monitoring from the federal government. Toronto police chief Bill Blair has boasted about how his force used the geofencing capability of the device of a protester who was active on social media to track the precise locations of people attending a local protest.

This type of pervasive monitoring, collection, and analysis of Canadians’ online communications and social media profiles is incompatible with democratic values. It is also arguably illegal under the Privacy Act, but the fact that it is happening anyway suggests the law needs to be strengthened.

Clear limits must be set around the government’s collection and use of information on Canadians, even when such information is publicly available online. Where there is a legitimate reason for the targeted collection of such information, it is imperative that the targeted collection of such information be conducted transparently, used strictly for the purpose for which it was collected, and that all such information is disposed of when no longer required for a legitimate purpose.

---

**Internet Voice**

“There are places where you should not feel threatened. For example, if you are on Facebook you shouldn’t be scared that something you say or post will have negative impacts against you.”

– Alex S., high school student
Recommendation 3

Embrace Accountability
Participants also expressed strong support for a range of proposals aimed at improving the accountability, oversight, and transparency of surveillance activities:

- 94.1% want to empower a Parliamentary Committee to conduct a thorough overview of existing oversight mechanisms.
- 91.8% want CSE to produce regular unclassified reports detailing their ongoing activities, and to publish statistics on how often they intercept Canadians’ personal information on behalf of partners such as the U.S. NSA.
- 88.2% agree with the Privacy Commissioner that spy chiefs should testify regularly before Parliamentary committees.
- 87.9% want an independent body to oversee CSE and CSIS and issue regular reports to the public.
- 86.8% want to make the commissioner responsible for making sure CSE doesn’t break the law independent of the Department of National Defence.
- 63.9% want a cross-party committee of MPs to provide stronger parliamentary overview of spy agency activities.
- 62.2% want to create an Interception Commissioner to review how spy agencies acquire and disclose communications data.

Unsurprisingly, these findings are again echoed by independent surveys. According to the federal Privacy Commissioner, 89% of those who were aware of surveillance activities believed that these agencies should have to “explain their activities to Canadians.”

Unsurprisingly, these findings are again echoed by independent surveys. According to the federal Privacy Commissioner, 89% of those who were aware of surveillance activities believed that these agencies should have to “explain their activities to Canadians.”

When Angus-Reid polled Canadians shortly after the publication of Bill C-51, they found that 69% wanted additional oversight of law enforcement agencies.

There are a number of glaring weaknesses in Canada’s current oversight system. As we outline below, even where review bodies exist, they lack the resources and independence necessary to effectively hold intelligence agencies accountable to the taxpayers who fund them.

Internet Voice

“It’s simple. Clear and transparent oversight. If people know their decisions will be scrutinized and that unauthorized or frivolous use of the power to invade citizens privacy will be punished then it won’t be abused.”

– Kelly M.

Internet Voice

“It is clear that we need some kind of watchdog, with a bite, to protect law-abiding citizens’ privacy.”

– Roxane T.

Internet Voice

“If we spied on the government, imagine the crimes we’d prevent!”

– Steve F.
No effective independent oversight of CSE

Many experts have raised concerns about the near-total lack of effective independent oversight of spy agency activities. CSE, for example, is overseen by CSE Commissioner Jean-Pierre Plouffe. He has a staff of 8 and an annual budget of just over $2 million. Despite this lack of resources, he is expected to keep tabs on a rapidly growing agency with over 2000 employees and an annual budget of $829 million.

Commissioner Plouffe is also limited in his effectiveness by the fact that he is only able to issue non-binding recommendations, which are often ignored on critical issues. This leaves CSE and the Minister of National Defence (who gives CSE its marching orders) as judge and jury when interpreting the scope of their legal powers.

The inadequacies of the legislation governing CSE oversight have also been raised by former CSE Commissioners Justice Robert Decary and Justice Charles Gonthier, who both complained they had inadequate information to be able to determine whether or not CSE had broken the law.

Annual Budgets
Spy Agency vs Watchdog

<table>
<thead>
<tr>
<th>Agency</th>
<th>Annual Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE</td>
<td>$2m</td>
</tr>
<tr>
<td>CSE Watchdog</td>
<td>$2.8m</td>
</tr>
<tr>
<td>CSIS</td>
<td>$829m</td>
</tr>
<tr>
<td>CSIS Watchdog</td>
<td>$513m</td>
</tr>
</tbody>
</table>

Worsening CSIS accountability and oversight deficit

As is the case with CSE, CSIS also suffers from a severe accountability and oversight deficit. The Security and Intelligence Review Committee (SIRC) is responsible for reviewing CSIS activities and for investigating complaints against the agency. It complained in its 2014 annual report to Parliament that it was encountering “significant delays” in obtaining information from CSIS. It now takes SIRC an average of three years to investigate complaints against the agency.

In the same report, SIRC complained that it had been “seriously misled” by CSIS. The watchdog also reported that it was “struggling to operate efficiently,” particularly in terms of investigating complaints. This is perhaps not surprising given that the government has starved SIRC of staff and resources, while at the same time consistently expanding funding for CSIS.

The government has also neglected to fill vacancies on the five member committee, leaving it to operate for much of 2014 with just three members, only one of whom could hear cases in French. Bill C-51 does nothing to address these accountability and oversight challenges.

Despite this, the government proposes under Bill C-51 to give sweeping new powers to CSIS without any additional oversight. As discussed earlier, The Globe and Mail has editorialized that these powers amount to transforming CSIS from an intelligence agency into “secret police.” As our case study on Bill C-51 demonstrated, many of these proposed new powers have significant negative implications for Canadians’ privacy – for example, under Bill C-51, it will be far easier for CSIS to obtain Canadians’ personal information, including what they write on passport applications, and even including sensitive commercial data.

Internet Voice

“I am really disturbed by the government’s lack of transparency and accountability. We need independent, non-partisan oversight of all surveillance activities. And for there to be full public disclosure thereof; and further sharp penalties for intruding on the privacy of citizens without a warrant... I do not want to live in a police state. That is not what it means to be Canadian and I would like our government to remember that.”

— Patricia M.
STEPS TO IMPLEMENTATION:

The trend in recent years has been clear. The powers and capabilities of Canada’s intelligence agencies have rapidly expanded, with no commensurate increase in oversight, accountability, or review mechanisms. Both of the official bodies charged with overseeing CSIS and CSE have complained about being misled.

Canadians want to see effective, rigorous, and independent oversight of CSE and CSIS. As requested by 94.1% of crowdsourcing participants, an all-party Parliamentary Committee should be empowered to conduct a thorough overview of Canada’s existing oversight mechanisms, and to make recommendations for improvements. There are many measures that should be taken to address the current stark oversight deficit:

1. **Reinstate the Office of the CSIS Inspector General:**

   In 2012, the government shut down the Office of the CSIS Inspector General. While SIRC reviews CSIS activities after the fact, the CSIS Inspector General was tasked with providing near real-time oversight of CSIS activities. The closure of this office has left a glaring hole in Canada’s oversight mechanisms, and this mistake should be rectified immediately. A new Office of the CSIS Inspector General should be made independent of the Department of Public Safety, and mandated to report directly to Parliament and the public without pre-approval or interference from the government of the day.

2. **Create strong, independent control of the CSE:**

   The only current checks on CSE’s activities come in the form of non-binding recommendations from the CSE Commissioner and the Privacy Commissioner. CSE is allowed to ignore these recommendations and has in the past. CSE needs to be brought under judicial control, the CSE and Privacy Commissioners must be empowered to issue binding orders onto CSE as well as penalties for when CSE ignores the law and these bodies need to receive the resources required to fulfil this mandate effectively. Moreover, both Commissioners should be appointed by a non-partisan parliamentary committee with input from civil society.

   The CSE Commissioner should also be mandated to publish regular public reports on the privacy implications of CSE’s activities. As is the case with other arms-length agencies such as the Privacy Commissioner and the Canadian Radio-television and Telecommunications Commission, these reports should not be subject to pre-approval or interference from the government of the day.

3. **Implement the CSE oversight recommendations proposed in Bill C-622:**

   Liberal MP Joyce Murray’s Bill C-622 was voted down by the government, but contained a range of important recommendations to boost transparency, oversight, and accountability for CSE. The Bill would give MPs stronger powers of oversight and review over CSE’s activities. It would also improve CSE’s public reporting obligations, and require the Minister responsible for CSE to obtain a Federal Court order to collect the protected information, including metadata, of Canadians at home or abroad. These sensible suggestions should be implemented in future pro-privacy legislation.

4. **Establish a cross-party Parliamentary Committee tasked with ongoing review of spy agency activities:**

   A cross-party Parliamentary Intelligence and Security Committee should be empowered to provide rigorous parliamentary review of CSE, CSIS, and other government security agencies. Prior to their retirement, Senators Hugh Segal and Romeo Dallaire co-sponsored Bill S-220, which would establish just such a committee, while ensuring its members had the security clearances necessary to adequately review secretive surveillance activities. Liberal MP Wayne Easter has proposed something similar in his Private Member’s Bill C-551.

   *When you talk about a credible oversight body, I would suggest ... that a parliamentary body is going to have more credibility because of its independence and because of the fact that there is also parliamentary accountability that will be brought to bear.*

   Peter MacKay, when he was in opposition in 2005

   At present, Canada is the only ‘Five Eyes’ member without any parliamentary oversight of its security services. This deficiency should be rectified, and Bill S-220, while not without its flaws, provides a useful starting point from which to do so. The committee must be granted the resources required to conduct its oversight role effectively. To reflect the importance of ensuring the committee’s independence, it should be chaired by a member of the largest opposition party, and members should be elected through secret ballot of all MPs rather than chosen by party hierarchies.
5. **Fully implement the Privacy Commissioner’s January 2014 ‘Checks and Controls’ recommendations:**

The recommendations set out in the Privacy Commissioner’s January 2014 *Checks and Controls* report should be implemented in full. This would require strengthening existing reporting mechanisms, require CSE and CSIS chiefs to testify regularly before Parliament, require CSE to produce regular unclassified reports, strengthen existing laws to curb over-collection of personal information, and prevent government agencies from monitoring what people say on sites like Facebook without a legitimate reason. Each of these measures were broadly supported by over 84% of participants in our crowdsourcing process. While not sufficient in and of themselves to ensure sufficient oversight of CSE and CSIS, their implementation would be a positive step forward.

6. **Ensure that the Security Intelligence Review Committee can perform its role effectively:**

SIRC is mandated with investigating public complaints against CSIS, but due to lack of resources and personnel it is struggling to complete even 50% of investigations within a 3-year target timeframe. Vacancies on SIRC should be filled as a priority. SIRC should be provided with the human and financial resources required to fulfil its mandate effectively, and to conclude most investigations within a 6 month timeframe. SIRC’s powers to review CSEC’s activities should also be broadened and deepened, as it has itself requested for years.

7. **Implement the oversight recommendations of the 2006 O’Connor Report:**

In his 2006 report into the Maher Arar affair, Justice Dennis O’Connor made a number of recommendations aimed at boosting oversight of Canada’s security agencies. These included the creation of a new oversight agency for the RCMP, a substantially expanded role for SIRC in overseeing not just CSIS but also the national security activities of a number of other government agencies. Justice O’Connor also recommended a committee to better coordinate the activities of Canada’s various national security watchdogs. Many of his recommendations are reflected in the proposals set out in this report. The government has ignored Justice O’Connor’s common sense recommendations for over eight years. Their implementation is long overdue.

8. **Establish an Interception Commissioner to review the interception of private communications by spy agencies:**

Canada should establish an Interception Commissioner, tasked with reviewing the interception of communications and the acquisition and disclosure of personal information by the government. This proposal was selected as a priority by 62% of participants in our crowdsourcing program. The U.K. has a well-established Interception of Communications Commissioner’s Office responsible for ensuring that the surveillance powers granted to government agencies are being used correctly. However there are a number of serious weaknesses in the U.K. model, including what one expert observer describes as a culture of “passive and highly trusting regulation.” Canada should avoid these weaknesses, and ensure that a Canadian Interception Commissioner has the resources, powers, and teeth necessary to ensure that government agencies comply with the law.

---

Internet Voice

“The oversight committee should be made up of a body of 9 with 3 appointed by each of the 3 major parties. If not 9 then some equal number from each of the 3 main parties.”

— Grant P.
9. Rein in the steep costs of excessive government surveillance:

For years, Canadian taxpayers have shouldered a rapid increase in costs associated with surveillance. We can make a start on reining in these costs through the development of clear cost projections by the Parliamentary Budget Officer, with subsequent evaluation by the Auditor General, for current surveillance and data collection infrastructure as well as that envisioned by any new legislation or regulations.

Cost breakdowns should also cover the ongoing costs for telecommunications providers and online service providers associated with processing requests for information, and the costs of external oversight mechanisms. Particular attention should be paid to whether these costs will impact disproportionately on Canadian taxpayers or businesses. The underlying assumptions for any costs projections should be the subject of public debate. Cost projections for any new or existing privacy-impacting legislation or regulations must include a budget for oversight mechanisms, including but not limited to the federal and provincial Privacy Commissioners’ need for resources.

10. Going forward, ensure that oversight keeps pace with new spy agency capabilities and powers:

Any new powers that may in future be granted to CSIS, CSE, or other government agencies to access or transmit citizens’ personal information must include comprehensive and detailed external oversight mechanisms, a system of enforced deterrents for abuse, and mechanisms to ensure individuals are knowledgeable about and in control of the flow of the dissemination of their information.

Any new powers must involve clear external, independent oversight mechanisms with detailed reporting obligations (to Parliament and the public), which encompass all activities that involve the gathering and sharing of Canadians’ personal information by government authorities. Oversight bodies must be provided with the resources they need to identify and report when government agencies fail to comply with the law.
Setting a Global Standard
The international context

As this report has outlined, there is much that Canada can do to restore its citizens’ privacy rights here at home. These measures are important to restore the democratic balance between the rights of citizens and the state. If implemented, they would give every Canadian the confidence that they are not being watched by their own government - at least not without a warrant issued by an open court based on due process and strict objective criteria.

However these measures only take us so far: What about when other governments spy on Canadians? Or when Canada’s government spies on people overseas?

After all, Canadians are not alone when it comes to wrestling with these crucial privacy issues. People the whole world over are increasingly being subjected to surveillance from a range of governments, often including their own.

In the U.S., the NSA is conducting extensive warrantless spying on American citizens without their knowledge or consent. The Snowden documents have revealed how the NSA has the ability to monitor telephone calls, emails, and private online information. Notably, through its PRISM program, the NSA collects vast amounts of data from popular online services owned by Google, Apple, Yahoo, and other major tech companies.

Britain’s GCHQ has been revealed to be tapping the global Internet backbone, collecting vast amounts of private information which it then shares with its ‘Five Eyes’ partners. GCHQ also partnered with the NSA to steal encryption keys that protect private phone communications by hacking Gemalto, the world’s largest manufacturer of SIM cards. Experts say that these stolen keys enable GCHQ and the NSA to spy on phone communications without requiring approval from telecom companies or foreign governments.

Even far-flung corners of the earth are not immune to government mass surveillance activities. The small southeast Asian nation of East Timor took Australia to the International Court of Justice (ICJ), where it complained that ASIO (Australia’s CSE) was using its own near limitless surveillance powers to spy on East Timor’s legal representative in an ongoing dispute over huge oil and gas reserves in the Timor Sea. The resulting ICJ order prohibited Australia from spying on East Timor for any purpose related to any ICJ disputes between the two.

The Guardian and The Intercept have also reported that New Zealand spies indiscriminately on many small island nations in the South Pacific, and that it shares this information with the U.S. and its ‘Five Eyes’ allies. Victims of New Zealand spying include Tonga, Fiji, Samoa, and the Cook Islands. A separate New Zealand spy program even targeted an anti-corruption campaigner in the Solomon Islands.

So while there is much that needs to be done in terms of Canada putting its own house in order, surveillance is clearly also a global challenge that requires a global solution.

Here again Canada has an important role to play. Canada can become a global leader in reining in excessive digital surveillance practices. By leading by example, and by working with other governments and the United Nations, Canada can work to set a new global standard for privacy protection in a digital age.

A prescient quote from the character Sam Seaborn, in an episode of The West Wing first broadcast in November 1999.

“The next two decades are going to be privacy. I’m talking about the Internet. I’m talking about cell phones. I’m talking about health records and who’s gay and who’s not. And moreover, in a country born on the will to be free, what could be more fundamental than this?”

A prescient quote from the character Sam Seaborn, in an episode of The West Wing first broadcast in November 1999.
HOW CANADA CAN HELP SET A NEW GLOBAL STANDARD:

1. **Endorse and champion international human rights privacy principles:**

   In 2013, following over a year of consultation, dozens of leading international privacy experts, human rights lawyers, and open Internet advocates published the *International Principles on the Application of Human Rights to Communications Surveillance* (commonly known as the *Necessary and Proportionate Principles*). The Principles set out what is required for governments around the world to bring their surveillance activities into line with international human rights law.

   They amount to a comprehensive set of safeguards to protect the privacy of people around the world, wherever they live. If implemented they would put a stop to all programs of suspicionless mass surveillance, including the bulk collection of metadata. The Principles have been signed by over 470 organizations and experts, 350,000 people, and leading decision-makers in Canada, the U.S., continental Europe, and the U.K.

   Canada should ensure that all its domestic and international surveillance activities comply with these principles. Canada should also champion these common sense safeguards at the United Nations and other international forums. Canada should not share personal information obtained via surveillance with nations that do not respect these basic global human rights safeguards.

   Notably, members of the ‘Five Eyes’ have been exposed as deliberately circumventing restrictions on domestic surveillance by spying on each other’s citizens, then sharing the information. Documents have revealed, for example, that the U.K.’s GCHQ is tapping trans-Atlantic fibre-optic cables and passing the information to the U.S. NSA. GCHQ also struck a secret deal allowing the NSA to analyze and store sensitive metadata on British citizens. The NSA reciprocates by circumventing British law to share information about British citizens directly with GCHQ.

2. **Attempt to reform the ‘Five Eyes’ spy alliance:**

   The decades-old surveillance alliance between the U.S., U.K., Canada, Australia, and New Zealand needs to be reformed to bring its activities into line with international human rights principles. Over the decades, the ‘Five Eyes’ have evolved into what Edward Snowden has described as “some sort of a supranational intelligence organization that doesn’t answer to the laws of its own countries.”

   Nor are these abuses restricted to the U.S. and U.K. Australia’s intelligence agency also offered to share information it had collected about Australian citizens with the NSA, including bulk, unredacted metadata. Here in Canada, federal court judge Richard Mosley rebuked CSIS and the CSE for outsourcing surveillance of Canadians overseas to its ‘Five Eyes’ partners.

   Canada should make future cooperation with the ‘Five Eyes’ contingent on their compliance with human rights principles, including those set out in the *Necessary and Proportionate Principles*. At a minimum that means ending all programs of suspicionless online spying, including the bulk collection of metadata.

3. **Enact new safeguards on data sharing with foreign governments:**

   Canada should enact legislative protections to prevent foreign governments from accessing Canadians’ personal information without due process, and to prevent Canadian government entities from accessing Canadians’ data from foreign state entities without due process.

---

**Internet Voice**

“We need to close the recently widened loophole that allows our spy agencies to ask other spy agencies to spy on Canadians on their behalf.”

– Evan P.
The Privacy Act should also be amended in line with the Privacy Commissioner’s January 2014 recommendation to “strengthen the provision relating to the exchange of personal information with foreign authorities to promote privacy”. The amendment should be specifically tailored to address government surveillance, national security, and law enforcement activities.

4.

Work through the U.N. and other global institutions for international privacy safeguards:

Moves toward stronger privacy are already afoot in many key global institutions. The U.N. General Assembly, led by Brazil and Germany, has explicitly recognised that the human right to privacy extends to online activities. In a resolution adopted in late 2013, the assembly called on member states “To respect and protect the right to privacy, including in the context of digital communication.”

“...without the necessary checks, we risk turning into Orwellian states, where every step of every citizen is being monitored and recorded in order to prevent any conceivable crime.”

Germany’s UN Ambassador Harald Braun, addressing the UN General Assembly

Unfortunately, under pressure from the ‘Five Eyes’, including from Canada, the General Assembly has so far failed to support recommendations from the U.N. High Commissioner for Human Rights that metadata collection should cease, and that surveillance should only be conducted when necessary, legitimate, and proportionate.

Other important global institutions are also wrestling with these issues. The OAS Special Rapporteur for Freedom of Expression has declared that limits on surveillance powers are “urgently necessary.” Latin American institutions such as Mercosur and ALBA have declared surveillance to be a threat to their sovereignty, democracy, and peace. Members of the G8, G20, and Commonwealth have all been outraged at revelations that the ‘Five Eyes’ targeted their summits.

Instead of defending surveillance practices that undermine people’s basic rights, Canadians deserve a government that stands up for privacy rights on the international stage. Canada should throw its weight behind efforts in global institutions to develop strong privacy safeguards to protect human rights in a digital age.

Canada is, by and large, a well-respected member of the international community, a middleweight power that wields an influential and often outsize role at international institutions including the United Nations, the G20, the G8, the OECD, APEC, the Commonwealth, the OAS, and La Francophonie. Canada is therefore well positioned to play a leadership role in developing stronger global privacy safeguards.
The Process: Working Toward A Crowdsourced Pro-Privacy Agenda
The Process: Working Toward A Crowdsourced Pro-Privacy Agenda
As a community-based organization, participatory values are something OpenMedia holds dear. We believe that often the best ideas come from our community, and we strive to crowdsource wherever we can. Our community often inspires us to push our work further than we ourselves would have imagined when embarking on a project.

Our experience with a wide range of privacy campaigns and initiatives has helped shape this project from beginning to end.

Canada’s Privacy Plan has been especially informed by OpenMedia’s engagement work over the past 24 months. We gained invaluable experience through this extensive engagement work that enabled us to identify the key issues we wanted to address through this crowdsourcing project.

Since our organization first engaged on privacy issues, our community has been clear that they wanted a voice in important decisions that affect their daily lives. In contrast to a government that seemed intent on exploiting secrecy around spy agency activities to further undermine Canadians’ privacy and exclude citizen voices from the debate, we decided to develop our plan through an open, transparent, and democratic process that all Canadians were invited to take part in.

The response to Canada’s Privacy Plan, and to the series of pro-privacy activities and campaigns that led up to it, was fantastic. Over 125,000 Canadians have engaged directly with our privacy work over the past year. And over 10,000 people, from every province and territory in Canada, took the time to provide us with detailed feedback about what they wanted to see done to tackle our privacy deficit.

One of the greatest successes of this project has been the creation of a vibrant pro-privacy community from across Canada and across the political spectrum. We hope this community will continue to play an integral role in safeguarding our privacy rights and our democratic values. And we hope that decision-makers will listen to this community, and ultimately recognize that privacy rules should be created not behind closed doors, but through the participation of all Canadians.

But crowdsourced volunteering activities are going far beyond coding or simple information sharing. Today, crowdsourcing is used to create and increase collective knowledge, community building, collective creativity and innovation, crowdfunding, and civic engagement.”

—*The role of crowdsourcing for better governance in fragile state contexts*, 2014. Maja Bott, Björn-Sören Gigler, and Gregor Young
Crowdsourcing is the process of problem solving by seeking solutions through an open and public platform and in particular, through web-based technologies. Crowdsourcing comes from the technology sector, where it has been applied as a novel method of generating creative solutions; civil society groups and governments are only beginning to recognize that the public and web-based nature of crowdsourcing means it has potential applications for participatory democracy, and could be a new means of drafting public policy.

Like most serious experiments with using technology to transform democracy, crowdsourcing is in its nascent stages. As a result, there are many questions surrounding the effectiveness of crowdsourcing at creating practical and inclusive public policy. Crowdsourcing experiments will encounter problems with the clarity, accuracy or representativeness of the input they obtain, and will need to seize these experiments as learning opportunities – they closely resemble the flaws we find in our current representative democratic processes, such as elections and regulatory hearings. As well, many of the social inequalities and exclusions that exist offline exist online as well -- in some cases, they are even more pronounced.

Nonetheless, we firmly believe in the potential of the Internet to revolutionize democratic decision-making, and that it is up to us to harness it. When it comes to the Internet and the age old matter of who gets what, where and when, it is important that those who will most feel the impact of decisions be in the driver's seat rather than unelected bureaucrats and lobbyists. This is precisely why we believe that when making laws that will greatly affect the future of privacy safeguards, the first step should be to experiment with new forms of decision-making, such as crowdsourcing, that allow Internet users to inform law-makers about the real impacts that different approaches will have on their daily lives. By carrying out this experiment in crowdsourcing, we offer lawmakers insights into the expertise of the Internet community, the values that they hope will guide the evolution of our online culture, and their aspirations for our digital future.

**Our drag-and-drop crowdsourcing tool:**

The drag-and-drop tool, launched in October 2014, formed the foundation for our analysis of Canadian Internet users’ perspectives on privacy, and allowed us to come up with the three recommendations outlined in this report, as well as the more specific policy agenda in the Executive Summary of this report.

We worked with leading experts and organizations in the Protect Our Privacy Coalition to identify a basic set of policy issues pertaining to the government’s collection and use of citizen data. We created an attractive online survey, featuring a drag-and-drop tool to enable Canadians to rank their privacy priorities.

The drag-and-drop tool questions were shaped by input from many people, including OpenMedia staff and community members, and colleagues and organizations from the Protect Our Privacy Coalition. We wanted our questions to reflect a broad approach to the complex issues around privacy, rather than focusing them on any one specific area.

Once the tool was designed and launched, we conducted outreach in multiple ways (including extensive social media publicity, and emails to OpenMedia’s community of over 125,000 supporters engaged with our privacy work) to give Internet users the chance to participate, and ensure a sizeable “crowd” behind our crowdsourcing.

The public input phase of the crowdsourcing tool lasted until the end of November, after which we commenced collation and analysis of the results.
Events reviewed as part of our consultation:

February 2014 & February 2015 Annual Privacy and Security Conference, Victoria, B.C.

This conference is a key annual event for people working in the privacy and security fields in Canada. OpenMedia’s Steve Anderson made a presentation about key privacy and surveillance issues at both the 2014 and 2015 annual conferences. The conference attracts senior attendees from government, privacy organizations, and private industry, and offered an ideal opportunity for us to share ideas, and collaboratively identify key issues and privacy challenges.

May 2014 Politics of Surveillance Workshop, Ottawa

We supported dozens of top Canadian privacy experts by hosting and helping to launch the Ottawa Statement on Mass Surveillance, which sets out high-level recommendations on how to rein in out-of-control government surveillance.

This statement was originally crafted on the occasion of the launch of the book *Transparent Lives: Surveillance in Canada / Vivre à nu: la surveillance au Canada*, at the ‘Politics of Surveillance Workshop’. This event brought together in Ottawa, Canada, May 9-10, 2014, an international group of academics and advocates to debate the various political, legal, social and technological strategies for challenging mass surveillance, protecting civil liberties and advancing democratic rights.

Over 35 academics and 19 organizations endorsed the statement. The statement is hosted on OpenMedia’s website at https://OpenMedia.ca/Statement, with a French-language version available at https://OpenMedia.ca/Declaration

**Ottawa Statement on Mass Surveillance in Canada**

We are entering an age of big data and ubiquitous surveillance. We know:

- That governments and private corporations routinely collect and sort massive amounts of personal data for multiple reasons from national security to marketing;
- That there is extensive targeting and profiling of individuals and groups on grounds of race and ethnicity, political and religious views, social class, age, gender, sexual preference and disability;
- That Canadian privacy and data protection laws and regulations are regularly bypassed, undermined or broken, and are inadequate for dealing with information and privacy rights in the age of big data and ubiquitous surveillance.

We the undersigned are agreed:

1. That all levels of government in Canada must fully respect the Canadian Charter of Rights and Freedoms including the right to privacy, freedom of thought and expression, freedom of association and peaceful assembly,
October 2014
Privacy Coalition consultations

We held a consultation call, approximately 1 hour in length, with individuals and organizations involved in the Protect Our Privacy Coalition to discuss our crowdsourcing project. We also held a number of one-on-one calls and in-person meetings. Although the project is not an official coalition initiative, it benefited a great deal from the skills, expertise, and experience of coalition members, many of whom also helped us publicize our crowdsourcing tool.

October 2014 to January 2015
In-person Crowdsourcing Events (Vancouver, Montreal, Halifax)

Although the drag-and-drop tool was primarily designed to be used online, we also created an offline version of the tool for use at in-person events. With the assistance of volunteers, we helped organize three in-person events as part of our crowdsourcing process - one each in Vancouver, Montreal, and Halifax. We also offered participants at these events an opportunity to provide open-ended feedback.

OpenMedia led two educational events on privacy issues at the B.C. Civil Liberties Association annual event for 16-17 year old high school students. Our privacy campaigner David Christopher delivered an interactive presentation outlining the key privacy challenges facing Canadians today. Following Q&As, we followed up with a pen-and-paper exercise that enabled all the participants to take part in our privacy crowdsourcing initiative.

Our Montreal event was organized by the OpenMedia McGill club, while our Halifax event was organized by local university student volunteers. We received plenty of positive feedback after each event, and it seemed students really appreciated the opportunity to make their voice heard in shaping pro-privacy recommendations.

November 2014
Facebook Town Hall:

As part of our crowdsourcing work for this project, OpenMedia hosted a Facebook Town Hall on Privacy Issues. Tom Henheffer, executive director of our coalition partners at Canadian Journalists for Free Expression co-hosted the event with our Steve Anderson. We had a lively discussion, as Steve and Tom fielded questions from Canadians on privacy issues.

The NDP’s digital issues critic Charmaine Borg also joined the debate. We reached over 46,000 people with this event, and input from this Town Hall helped shape this report.
Spotlight: Key milestones in our campaign to safeguard privacy

June 2013
No Secret Spying campaign

Over 16,000 Canadians signed our SecretSpying.ca petition, which was launched in response to the first round of revelations about CSE and NSA surveillance of law-abiding citizens. We worked with 15 other organizations on the campaign, including Leadnow.ca which co-hosted the campaign with OpenMedia.

October 2013
Launch of the Protect our Privacy Coalition

In late 2013, responding to growing concerns from our community, we worked with dozens of other organizations to form the Protect our Privacy Coalition. Our community strongly emphasized the need to work together to sustain a nationwide movement to fight for stronger legal safeguards to protect the privacy of every resident of Canada.

This coalition has grown steadily to include over 60 major organizations, including innovative technology companies, public interest groups, unions, and small businesses. Underlining that privacy is not a partisan issue, the coalition brings together organizations from across the political spectrum. You know you’ve hit on a common Canadian value when you have the Canadian Taxpayers Federation and the Council of Canadians participating in the same coalition.

The coalition acts as a platform for these diverse voices to work together on privacy issues. Coalition members have agreed to support a straightforward statement calling on decision-makers to support stronger legal privacy safeguards.

Since the launch, over 40,000 individual Canadians have signed on to endorse this statement.

"More than ever, Canadians need strong, genuinely transparent, and properly enforced safeguards to secure privacy rights. We call on Government to put in place effective legal measures to protect the privacy of every resident of Canada against intrusion by government entities." - Protect our Privacy Coalition statement

October 2013
Joint announcement with BCCLA of landmark constitutional challenge against CSE spying

We worked with our Privacy Coalition partners at the B.C. Civil Liberties Association (BCCLA), to jointly announce their landmark legal challenge aimed at stopping illegal spying on Canadians. The challenge was filed in the Supreme Court of British Columbia on October 22nd last year.

WE DESERVE TO KNOW
if our SENSITIVE PRIVATE INFORMATION is being recklessly collected and stored in giant databases, and why

DEMAND WHAT YOU DESERVE: http://SecretSpying.ca
OpenMedia's responsibility was the launch of a nationwide campaign in support of the lawsuit. We launched an action page to enable any Canadian to pledge their support - over 12,800 Canadians took this pledge.

We organized a joint press conference with the BCCLA and worked to secure extensive national and international media coverage of the lawsuit. The Globe and Mail also published a supportive editorial shortly after the announcement.

December 2013
Infographic about CSE spying

In the six months since Edward Snowden first blew the whistle on NSA and CSE surveillance, our community had been asking questions about exactly what CSE's spying and data collection could reveal about their private lives.

We worked with leading Canadian privacy experts to answer these questions. We prepared a detailed infographic, highlighting how the types of metadata collected by CSEC can reveal intimate details about our lives - including our political beliefs, medical conditions, financial status, religious convictions, and sexual orientation.

This infographic was shared widely on Facebook, Twitter, and by members of the Privacy Coalition. It also serves as a handy go-to resource for explaining just how intrusive CSEC's spying and data collection activities really are. Many journalists have already used it as a reference point. It can be viewed at https://OpenMedia.ca/CSECandYou

January to December 2014
Campaign against Bill C-13:

Throughout 2013, we warned our community that the government was gearing up to reintroduce online spying legislation - despite its promise not to do so following the defeat of controversial Bill C-30, which was withdrawn after over 150,000 Canadians spoke up against it.

We were therefore unsurprised when Justice Minister Peter MacKay introduced new online spying legislation under the guise of tackling cyberbullying. On the day of his announcement, we worked with privacy experts to analyze the proposed legislation (Bill C-13), and were quickly out with a media release highlighting how the legislation contained just 2.5 pages about cyberbullying, alongside 65 pages about online spying.

We followed up by working with other members of the Privacy Coalition to oppose the legislation. We also secured the support of the Official Opposition for our proposal to split the Bill, so that measures tackling cyberbullying could be dealt with separately.

In March, we released a hard-hitting video highlighting how the Bill would grant immunity to telecoms who hand over Canadians' private information to authorities without a warrant. This video was widely viewed and shared on social media.
In the end, over 73% of Canadians opposed the Bill, including a large majority of conservatives. Despite this, the government succeeded in pushing the legislation through Parliament, and it became law in early 2015. A number of the recommendations of this report are designed to address the threats posed by Bill C-13 to Canadians’ privacy.

February to November 2014

Toronto Star privacy op-ed series

We arranged for a hard-hitting series of op-eds about privacy issues to run in the Toronto Star, Canada’s largest-circulation newspaper. Contributors included Derek James From (Canadian Constitution Foundation), Cindy Blackstock (First Nations child advocate), Steve Anderson (OpenMedia), and Phillip Djwa (Agentic).

February 2014

Social Media Town Hall about CSE spying

With new stories breaking regularly about CSE spying, we decided to bring together two of Canada’s leading privacy advocates for a Social Media Town Hall — Josh Paterson, Executive Director of the B.C. Civil Liberties Association (BCCLA), and our own Steve Anderson, Executive Director of OpenMedia.

We wanted to give everyone the opportunity to talk directly with Josh and Steve — so we threw the doors open to all Canadians on Facebook, Reddit, Google+, Twitter, and our website.

It turned into a fascinating discussion, covering issues including the court case OpenMedia helped the BCCLA announce last October, whether the Charter of Rights and Freedoms protects us from spying, the information that metadata can reveal, and even whether the Canadian government is allowed to get other countries to spy on Canadians.

February 2014

Day We Fight Back international campaign

OpenMedia played a key role in organizing ‘The Day We Fight Back’, a global campaign aimed at pressuring decision-makers to stop invasive spying. We were involved in organizing this day of action in Canada, the United States, and internationally.

In Canada, we worked with our Privacy Coalition partners to create an interactive website with new online tool to enable Canadians to contact their local MP, to urge them to take a pro-privacy commitment to introduce effective legal measures to protect Canadians’ privacy from government spying.

In the United States, we were part of the core group organizing the Day We Fight Back action. We succeeded in reaching over 37 million people, delivering over 555,000 emails and 89,000 phone calls to Members of Congress.
Internationally, we teamed up with the Electronic Frontier Foundation to rally support for the Necessary and Proportionate International Principles on the Application of Human Rights to Communications Surveillance. Over 245,000 people from around the world signed up to support these principles.

Over 14,000 Canadians took part in the Day of Action, and we secured pro-privacy pledges from senior MPs. We have now turned this ‘Day Way Fight Back’ website into an ongoing effort to encourage MPs to make a pro-privacy commitment. It is available at http://TheDayWeFightBack.ca

March 2014
Letter to the Editor tool

We know from experience that getting letters published in local newspapers is one of the most effective ways to amplify Canadians’ voices across the country.

However we know that people can sometimes find writing such a letter a daunting prospect. OpenMedia launched an easy-to-use letter to the editor tool, to make the process of sending a letter to local newspapers as straightforward as possible.

The tool included prepared talking points, and automatically identified local newspapers based on an individual’s postal code. It also sent the citizen’s letter directly to those newspapers. We know that making this process smooth greatly increases the number of letters sent and published in newspapers across the country.

Canadians from coast to coast have used our Letter-to-the-Editor tool to successfully publish letters in dozens of major Canadian newspapers. The tool is available at https://openmedia.org/privacy/letter.

May 2014
Defend Digital Privacy campaign

Our Defend Digital Privacy campaign was launched in May 5, 2014. The campaign urged Prime Minister Stephen Harper to take responsibility for spy agency surveillance and for the online spying legislation his government was trying to force through Parliament.

Over 11,500 Canadians signed on to support this campaign, along with a number of leading pro-privacy organizations. The campaign website is at: https://OpenMedia.ca/DefendPrivacy
June 2014

Access My Info tool

We worked with privacy experts at the University of Toronto's Citizen Lab and Digital Stewardship Initiative to offer Canadians a new way to learn more about the information being collected about them by their telecom provider. A new online tool simplifies the process of requesting information from telecom providers about the information they collect, and about their disclosure of personal information to third parties.

The Access My Info tool creates a formal letter which, under Canadian privacy law, telecom companies are legally obliged to respond to within 30 days. The launch received solid media coverage. Over 5000 Canadians have used the tool, which is available at https://OpenMedia.ca/MyInfo. We also surveyed users of the tool about the responses they received from telecom providers, and input from this survey helped shape the recommendations of this report.

Steve Anderson’s Crowdsourced Parliamentary Testimony on C-13

On June 3, 2014 OpenMedia’s Executive Director Steve Anderson testified before the Standing Committee on Justice and Human Rights regarding Bill C-13. To help bring the concerns of Canadians to the Parliamentary committee Steve crowdsourced his opening presentation referencing some of their input directly from time to time. Input was collected from OpenMedia’s website, reddit, Facebook and Twitter.

The Canadians Steve heard from had three main concerns about Bill C-13 that he highlighted:

1. Immunity for activities that victimize innocent Canadians
2. Accountability and oversight
3. Data security

The input gathered for Steve’s testimony also helped shape this report and its recommendations.
July 2014
Launch of A Crisis of Accountability report

OpenMedia helped publish a groundbreaking report by Professor Simon Davies at the London School of Economics, which examines the responses of different nations across the globe, including Canada, to the Snowden revelations.

Professor Davies concludes that few, if any, governments have taken concrete steps to rein in secretive surveillance, despite growing concerns from citizens. The report is hosted on OpenMedia’s website at https://OpenMedia.ca/CrisisOfAccountability

October 2014
Video launch about CSE spying

OpenMedia worked with Dafne Melania, a talented local design volunteer, to produce a high-quality online video that makes the CSE’s spying activities tangible for everyday Canadians.

The video launch was a big success, with plenty of partners supporting the launch by sharing it with their communities. It was watched over 15,000 times on YouTube and also helped focus media attention on the issue of CSE spying. You can watch the video at: https://OpenMedia.ca/CSECisWatching

Early 2015 to date
The StopC51.ca campaign

Since the government first announced Bill C-51 in late January, OpenMedia has worked extensively with a diverse range of organizations to rally opposition to the legislation.

Working with the BCGEU and Leadnow.ca, we helped organize a National Day of Action which saw large street protests take place in over 70 communities across Canada.

We are also co-hosting the StopC51.ca action page, which over 200,000 people have used to speak out against the Bill. Our own Steve Anderson delivered this petition to Parliament, during his crowdsourced testimony about Bill C-51 before the National Security and Public Safety committee.

The StopC51.ca page also includes a wide range of downloadable and shareable resources which members of the public are encouraged to use to campaign against the Bill. OpenMedia has also built a Letter to the Editor tool to help people spread the word in local communities, as well as a tool to make it easy for people to contact their local MP. These tools are available at https://OpenMedia.ca/SecretPolice and http://StopC51.ca/MP respectively.

OpenMedia is also working with partners on a national Week of Education about the Bill, that aims to raise awareness of the impacts the legislation will have on Canadians’ daily lives. This week has been timed to coincide with the Easter break when MPs will be at home in their ridings, prior to returning to Ottawa to vote on the Bill.
CONCLUSION

Listen to Canadians!

Surveillance has been with us for thousands of years – Sun Tzu even devoted a chapter to the topic in his 2,500-year-old The Art of War. However it is only recently that governments have acquired the tools to place entire populations under systematic surveillance.
There is now a very real danger that the Internet, the greatest tool for connectivity that humankind has ever invented, will be turned into something it was never intended to be – a tool for governments to spy on the private lives of everybody.

Behind the backs of their citizens, governments have been building surveillance tools unparalleled in their invasiveness, scope, and power. Our oversight mechanisms, designed for a different era, need to make sense in the 21st century. It’s remarkable that much of what we now know, we owe not to our official oversight bodies, but instead to a single NSA whistleblower, Edward Snowden.

This project came in response to these revelations, and to the perfect storm of legislation being advanced by a government seemingly determined to sacrifice Canadians’ most basic human and democratic rights on the altar of an increasingly powerful and unaccountable security bureaucracy.

As an organization, participatory values are at the heart of everything OpenMedia does. We don’t just want citizens to have a seat at the table, we work to place citizens at the heart of decision-making. That’s why we’ve tried to reach out to the broadest possible number of Canadians to help shape this report.

This open, participatory approach is all the more important given the government’s efforts to conceal the dramatic expansion of its surveillance capabilities from Canadians.

Canadians are clearly deeply concerned about their country’s continuing evolution toward out-of-control government surveillance. This is borne out both by our own crowdsourcing work, and by opinion surveys conducted independently.

The key recommendations we’ve set out in this report are designed to meet the concerns of Canadians, and to ensure that every resident of Canada can live their online and offline lives without fear of being watched. These proposals should form the core ingredients of any future legislation that purports to safeguard the digital privacy of Canadians.

This is a practical agenda, but given the enormous power of entrenched security bureaucracies, we know it will require significant political will to implement.

That said, there’s no doubt that Canadians are deeply unhappy with out-of-control online spying and ongoing privacy breaches. With this report being written during an election year, decision-makers in all parties have a clear incentive to side with Canadians and take a strong pro-privacy stance – but we should be wary of politicians who “talk the talk” on privacy without committing to concrete steps like the key recommendations set out in this report.

The challenge ahead cannot be underestimated. Canadians are trying to roll back a surveillance system that has been growing more and more powerful, behind their backs, for many years.

Responding to this challenge and to future privacy threats will require prolonged vigilance on the part of Canadians and privacy advocates. But we have no doubt that Canadians, working together, are up to this task – when people come together there is nothing they can’t achieve.

We know this is a bold agenda – but it’s one that has been shaped by everyday people from coast to coast to coast from start to finish. Our message to decision-makers is clear: It’s time to listen to Canadians and fix our privacy deficit.

We invite you to endorse the findings of this report at PrivacyPlan.ca

Internet Voice

Our electronic mail should have the same safeguards as our physical mail has had for over a century. The government should require a warrant to read any citizen’s communication no matter the form of transmission of that communication.”

– Maureen Y.

During my years at UBC, I took several courses dealing with political issues in the Soviet Union. Spying on citizens and using fear tactics to keep people contained, obedient, and quiet should be a thing of the past. Should. I refuse to let fear make decisions in my life. I hope my political leaders do the same.”

– Clara S.
APPENDIX I:

The results from our Crowdsourcing Tool
Our final survey comprised 8 questions, covering a broad range of privacy-related topics. These questions were shaped by input from a diverse group of privacy experts and public interest organizations.

Q1. How would you rank these Privacy Priorities?

The first question asked participants to rank six proposals in order of priority if they were developing privacy safeguards relating to government entities. We used a drag-and-drop tool format which presented the proposals in a randomized order to each new participant.

Participants ranked these six proposals in the following order:

1. Require a warrant for govt to spy on personal information
2. End blanket surveillance of law-abiding people
3. More transparency around govt collection of personal data
4. Tough penalties for when govt breaks privacy laws
5. Privacy rules should be shaped democratically
6. Independent oversight and review of spy agencies

In determining the aggregate rankings, each priority level (1-6) was assigned a corresponding numerical value, ranging from 0.6 for Level 1 to 0.1 for Level 6. Submissions from participants were then evaluated according to this scale, leading to a cumulative priority index (pi) for each proposal.

The following chart indicates the aggregate priority rankings for the respective privacy proposals:

10,107 Canadians used our crowdsourcing tool to provide specific input for this report, which we added to feedback from the over 125,000 Canadians who have been involved in our wider privacy work.

Canadians from every province and territory took part in this project:
By far the most preferred priorities were to require the government to obtain a warrant before spying on personal information, and to end blanket surveillance of law-abiding people. Both these priorities were significantly ahead of the other options.

The common theme here is a disinclination to support surveillance aimed at innocent citizens – Canadians clearly reject the notion of blanket ‘catch-all’ surveillance, popularized by the former NSA Director Gen. Keith Alexander’s phrase “collect the haystack and search for the needle later.” And Canadians perceive warrant requirements as the best way to prevent innocent people being caught in these kind of wide-reaching surveillance dragnets.

Interestingly, the order was somewhat different if we look solely at what participants chose as their top priority from the six options available. The following chart sets out the percentage of participants who chose each respective option as their top privacy priority:

Again we clearly see that ending blanket surveillance (28.1%) and warrant requirements (22.7%) came in significantly ahead of the other options available. Significantly more participants chose blanket surveillance as their top priority over any other issue. 15.5% of respondents chose “Privacy rules should be created democratically” as their top priority, while 13.6% wanted more transparency over government collection of personal data.
Q2. In what circumstances should government agencies, such as CSE, CSIS, or law enforcement, be able to access the sensitive, personal information of Canadians?

93.8% of participants chose this option, with just 5.4% willing to allow police officers to conduct searches based merely on suspicion. Only 0.4% believed personal information should be generally available to government agents, and a further 0.4% said police should be allowed to access information based on broad demographic descriptions (such as “all middle-aged white females living in Hamilton.”)

This is clearly a vocal endorsement of the robust approach taken to digital privacy in the Supreme Court’s R. v. Spencer case, and a rejection of government attempts, such as in Bill C-13, to make a wide range of personal information available to law enforcement without a warrant.

Q3. Do you think that government agencies such as CSIS and the RCMP should use public resources to monitor peaceful individuals, organizations, and advocacy groups not posing any known threat to national security?

This question was prompted by revelations that, according to documents obtained under the Access to Information Act, a wide range of civic interest groups had been subject to sustained surveillance from CSIS and the RCMP over a lengthy time period. Groups subjected to surveillance included the Council of Canadians, the Dogwood Initiative, the Sierra Club of British Columbia, and ForestEthics Advocacy.

The surveillance took place despite RCMP analysts concluding that they had “not identified any threats or criminal activity.”

Participants were overwhelmingly opposed to the use of public funds to monitor peaceful individuals, organizations, and advocacy groups. 92.2% opposed using public resources in this way. Just 2.2% supported the concept, while 5.5% said they were not sure.
Q4. What scrutiny mechanisms do you believe are appropriate to ensure spy agencies like CSE and CSIS are held accountable to taxpayers? (check all that apply)

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>87.8%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>81.8%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>71.3%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
<td>63.9%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>62.2%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

n = 1,772

Our fourth question asked participants whether or not they supported implementing a range of potential proposals aimed at improving the public accountability of surveillance agencies like CSE and CSIS.

The options presented covered improved oversight, Parliamentary Review, establishing a U.K.-style Information Commission, public disclosure, and stronger powers for agencies tasked with safeguarding privacy. Respondents could pick more than one of these options.

Of the 1772 participants who responded to this question, there were strong majorities in favour of each of the proposals set out.

A 87.8% favoured empowering an independent, arms-length body to oversee spy agencies and issue regular reports to the Canadian public that are not subject to pre-approval from the government of the day.

B 81.8% favoured requiring spy agencies to publicly disclose how many times they intercept Canadians’ personal communications, and what they are doing to protect our privacy.

C 71.3% favoured stronger powers and greater resources for agencies tasked with safeguarding Canadians’ privacy.

D 63.9% favoured establishing a cross-party committee of MPs to provide stronger parliamentary review of spy agency activities.

E 62.2% favoured establishing a U.K.-style Interception Commissioner to review the interception of communications and the acquisition and disclosure of communications data by intelligence agencies.

The greatest degree of consensus was around proposals to improve independent oversight of spy agencies, and to ensure that spy agencies themselves are required to disclose how often they intercept the personal communications of Canadians.

Notably, there was a significantly higher majority in favour of achieving independent oversight through an independent, arms-length body rather than through a cross-party committee of MPs or a U.K.-style Interception Commissioner.

Q5. What do you believe a new, pro-privacy law (or reforms to existing laws) needs to include if it is to effectively safeguard our privacy from government entities? (check all that apply)

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>94.7%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>89.1%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>89.1%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
<td>83.1%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>80.4%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td></td>
<td>79%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

n = 1,764

This question focused on what respondents believed any new pro-privacy reforms should include if they were to effectively safeguard Canadians’ privacy from the government. Again, respondents could pick more than one option if they wished.

Of the 1764 participants who responded to this question, strong majorities expressed support for each of the proposed new safeguards.

A 94.7% favoured rules to prevent telecom companies from handing their customers’ personal information to third parties (e.g. copyright trolls) without a court order.

B 89.1% favoured ensuring all surveillance activities require a warrant approved by a judge.

C 89.1% favoured forbidding the government from spying on the private communications and activities of law-abiding citizens, whether domestically or through international partners, without a warrant issued by an open court.

D 83.1% favoured requiring government agents at all levels to document all activities, decisions, and processes that may impact on the privacy of law-abiding Canadians.

E 80.4% favoured ensuring the government notifies law-abiding Canadians when it requests their personal information from telecom providers.

F 79% favoured stronger protections to prevent agencies like CSE, CSIS, and the RCMP from collecting the sensitive personal information of Canadians.

Again we see a strong demand that a warrant or court order should be required before government agencies or other third parties can access the personal information of Canadians.

This is in line with responses to questions 1 and 2, where warrant requirements were also heavily favoured.
In January 2014, the then federal Privacy Commissioner Chantal Bernier published a Special Report to Parliament entitled Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance.

Pointing out that the Privacy Act remains “essentially unrevised since 1983”, Commissioner Bernier stated that:

The aim of renewal in this area should be to protect privacy in a complex threat environment; oversee collection so that it is reasonable, proportionate and minimally intrusive; ensure appropriate retention and access controls (among both public and private actors); ensure accuracy of analysis; and control the scope of information requests and disclosures through specific safeguards, agreements and caveats.

Commissioner Bernier’s report made a series of detailed recommendations aimed at safeguarding Canadians’ privacy against this backdrop. The Commissioner’s key recommendations received broad support from the participants who responded to this question:

A 94.1% supported ensuring that an independent and non-partisan Parliamentary committee is empowered with the necessary security clearance to conduct a comprehensive review of existing oversight mechanisms - at present there is no independent oversight of CSE. Just 1.7% were against and 4.3% were unsure. (n = 1,737)

B 91.8% supported requiring CSE to produce regular unclassified reports describing its ongoing activities, and to publish statistics on the number of times they intercept Canadians’ personal information on behalf of other government agencies. Just 2.1% were against and 6.1% were unsure. (n = 1,686)

C 88.2% supported strengthening existing reporting mechanisms, including requiring spy agency chiefs to testify regularly before Parliamentary committees. Just 2.1% were against and 9.8% were unsure. (n = 1,740)

D 87.6% supported strengthening existing laws to “curb over-collection” of our personal information by government entities. Only 1% were against with 11.4% unsure. (n = 1,723)

E 84.2% supported preventing spy agencies from monitoring personal information published on sites like Facebook without a “legitimate reason.” 7.9% were against and 7.9% were unsure. (n = 1,732)

Each of the Privacy Commissioner’s proposals received widespread support—with particularly strong support for creating an independent, security-cleared, non-partisan Parliamentary committee to review how CSE is overseen.

Q6. Earlier this year, the Privacy Commissioner made a number of key recommendations to help safeguard Canadians’ privacy from spy agencies including CSE. Which of these recommendations do you believe should be implemented?

Q7. The CSE Commissioner is responsible for ensuring CSE doesn’t break the law. He reports to the Minister of Defence, who also oversees CSE. Do you believe the CSE Commissioner should be made independent of govt agencies directly involved with CSE?

\[Q6 - \text{For} \quad \text{Against} \quad \text{Not Sure} \]

\[\begin{array}{|c|c|}
\hline
\text{A} & \text{94.1%} \\
\hline
\text{B} & \text{91.8%} \\
\hline
\text{C} & \text{88.2%} \\
\hline
\end{array}\]

\[\begin{array}{|c|c|}
\hline
\text{D} & \text{87.6%} \\
\hline
\text{E} & \text{84.2%} \\
\hline
\end{array}\]

\[\begin{array}{|c|c|}
\hline
\text{For} & \text{86.8%} \\
\hline
\text{Against} & \text{3.2%} \\
\hline
\text{Not Sure} & \text{10.1%} \\
\hline
\end{array}\]

This question focused on the independence of the CSE Commissioner, whose office is responsible for making sure CSE doesn’t break the law. Participants overwhelmingly wanted to increase the independence of the CSE Commissioner. 86.8% supported making the CSE Commissioner independent of government agencies involved with running CSE. Just 3.2% were against this proposal with 10.1% unsure.
Over 600 participants used this open-ended question to provide us with often detailed feedback. We’re grateful to each and every one of them for taking the time – their input played a significant role in shaping this report.

While we don’t have the space to list all 602 responses here, the following comments provide a flavour of the feedback we received:

**Soraya M.**
“Follow democratic principles and protect Canadians from being watched without a warrant or justification.”

**Steve F.**
“If we spied on the government, imagine the crimes we’d prevent!”

**Maureen Y.**
“Our electronic mail should have the same safeguards as our physical mail has had for over a century. The government should require a warrant to read any citizen’s communication no matter the form of transmission of that communication.”

**Andrew J.**
“I am a card carrying Conservative member that does not agree with the current direction and lack of transparency the Government is taking in regards to protecting the privacy of Canadians over the right to security. I do not want quick reactionary legislation as it does not fully take into account the citizens’ rights and needs.”

**Amanda T.**
“If you want my personal information, you’d better have a warrant first.”

**Assya M.**
“We NEED to set up some good safeguards to protect citizen’s privacy. Privacy is a right and one of the most pressing issues of this digital age.”

**Jeff C.**
“We need oversight, from the courts, and from an independent Privacy Commissioner (with some real authority to take action when CSIS or the RCMP step outside of their boundaries).”

**Linda W.**
“Too much information is poor information. Sifting through mega data requires too many generalities and leads to erroneous conclusions. Let’s keep our security defence practical and respectful of Canadian values.”

**David C.**
“A judge must be consulted each and every time a government agency wants to invade the privacy of individuals, and the judge must be free from government influence or interference.”

**Katherine M.**
“The pendulum has swung WAY too far in the direction of limiting our privacy. Standards need to be adjusted to make privacy the default and transparency must be mandatory.”

**Mohammed V.**
“Stop passing Bill C-13 now because it does not protect Canadians from cyberbullies, it violates their privacy laws. Bill C-13 is just a lie, to trick you into thinking that they will protect you from cyberbullies even though they are becoming the bullies by watching or monitoring all of your activities online and on multiple devices.”

**Anne-Marie S.**
“Part of the deal in being a citizen of a free society is the expectation that our personal affairs and physical person are inviolable as long as we remain within the law. In addition, how can we realistically claim free speech as a right if the vast power of a government can be turned, as it so often has during Stephen Harper’s tenure, against a citizen who holds views that members of the government don’t appreciate?”

**James N.**
“If I send a personal letter in the mail to someone I don’t expect it to be opened and read by some government agent. The same privacy expectations should hold true for communication via the internet.”

**Angela W.**
“Warrant required for all searches and requests for private information and strong laws punishing those who try to get around it and/or break the laws regarding privacy.”

**Kay A.**
“Warrant, Warrant, WARRANT!”

**Vincent R.**
“Try actually ASKING Canadians what we want to happen. By attempting to “force through” your unconstitutional bill by using the attack on Parliament as a scapegoat, you are letting terrorism rule over us.”

**Konstantin V.**
“Do not spy on us, we are not in prison.”

**Brian V.**
“These over-reaching laws have not helped Canadians. The security of where the information is stored is not reliable or safe. The actions taken have not been legal, transparent or ethical. Spy agencies are suppose to ignore regular and non-criminal people to focus on real threats. Not harass and criminalize innocent people. The Canadian government and spy-agencies can do a better job.”

**Lorraine R.**
“Perhaps it would help if the privacy issue were made an election issue, during which it should be made clear this isn’t about spying on ‘the other guy’ but could be about spying on anyone/everyone.”
Susan C.
“Our sensitive, private information is being handed over at an alarming rate. Many are not even aware that it is being done. This has to stop. It is a violation of our Rights. It is unconstitutional. Many citizens are not aware of this and I personally have seen people become outraged, shocked and stand in disbelief when they are made aware that agencies like Border Security can access their medical records.”

Will F.
“Get the prime minister to read the Canadian Charter of Rights and Freedoms. Make sure he doesn’t have a big fat felt marker on him. Or an eraser.”

Sandra B.
“The govt needs to stop trying to spread fear and stop spying on law abiding citizens.”

Grant P.
“The oversight committee should be made up of a body of 9 with 3 appointed by each of the 3 major parties. If not 9 then some equal number from each of the 3 main parties.”

Megan T.
“Restriction of warrantless surveillance and data-mining, especially of non-publicly available information; non-partisan oversight of how entities perform/use surveillance; limitation on storing information and developing technical protocols for protecting and eventually deleting gathered information.”

Evan P.
“We need to close the recently widened loophole that allows our spy agencies to ask other spy agencies to spy on Canadians on their behalf.”

Jawed I.
“The government (whichever party is in power) must be transparent with all the activities they are engaging in that violate citizens privacy and must publish reports of their activities.”

Rachel C.
“If the privacy rights of law-abiding Canadians are compromised we will have broken with perhaps the best descriptors a country can proudly bear: Strong & Free. Government in Canada needs to implement measures that raise awareness around our privacy rights and freedoms. They also need to do more to empower upcoming generations who value freedom of information.”

Robert M.
“In less than 25 years all privacy rights for Canadians will have vanished. If the people do not speak up now it will be too late.”

Mike G.
“Individuals who suspect they are being monitored illegitimately should have access to a no-cost, independent vehicle to consider their case and report out as necessary with a result of - no illegitimate monitoring is taking place, or illegitimate monitoring is taking place.”

Roxane T.
“It is clear that we need some kind of watchdog, with a bite, to protect law-abiding citizens privacy. Safety is never a good reason to spy on everyone.”

Kelly M.
“It’s simple. Clear and Transparent oversight. If people know their decisions will be scrutinized and that unauthorized or frivolous use of the power to invade citizens privacy will be punished then it won’t be abused.”

Mike T.
“Items key to Canadians privacy as a whole such as the TPP treaty currently being decided behind closed doors should be transparent. The fact that industry lobbyists are writing the proposed legislation and we as the Canadian public are being kept in the dark is very disturbing.”

Janice K.
“As to the very first question, choosing 1-6 priorities, you need a comment section on it. My opinion, they are ALL #1 priorities. Get the fear-mongering bureaucrats and ‘security’ officials out of our lives and keep them out...”

Duane M.
“Bad things occur every day. Giving up freedom for the illusion of safety is not a good bargain. The people should not be afraid of the government, which already has way too much power.”

Derek W.
“Government agencies and the individuals who work within them must be directly held accountable for violations of privacy. There needs to be jail time, not just financial penalties, as these penalties will be paid out of taxpayer coffers anyways.”

Sam B.
“Basically, security should not be led by the party leading the government. It should be something made of a balanced selection of all elected MPs. Also, security and fear should never be allowed more importance than freedom and rights.”

Lauren V.
“Collection of data should be restricted to information that people share publicly, unless there is reason to believe a crime may be committed, and in that case, a warrant should be required. The government should be required to destroy data on law abiding citizens after a short period of time.”

Heather I.
“Don’t just create the legal framework for bodies doing oversight. They must be given adequate funding.”

Jennifer L.
“Ensure that anyone responsible for third-party review of CSEC has no stake in finding errors or not finding errors. Personal or professional affiliation with anyone within CSEC must be avoided to maintain transparency.”
Valerie B.
“I think Canada would benefit immensely from having a national conversation about privacy rights more generally - why we have them, why it's important that they be safeguarded for everyone. I've heard a lot of "if you've got nothing to hide" talk, which I feel puts Canadians at odds with each other. When the government and the corporate owned media control the message, the voices of ordinary Canadians is lost, and in a democratic state we ought to be considering those voices in a conversation about how best to protect us all.”

Jocelyn N.
“I think the “independent group” who monitors CSEC should be totally independent, not part of the government in any way, shape or form. They should be accountable to the public alone, especially if our tax dollars go into the development of said program.”

Brent M.
“Protection of privacy and strong safeguards and oversight of any collection of private data is of paramount importance if our democracy is to thrive. We cannot forego our privacy out of fear. Without a court order issuing a warrant, no governmental agency should be allowed to request private data on citizens’ communications or activities, and corporations or other 3rd parties who violate this privacy should be subject to legal sanction.”

Clara S.
“During my years at UBC, I took several courses dealing with political issues in the Soviet Union. Spying on citizens and using fear tactics to keep people contained, obedient, and quiet should be a thing of the past. Should. I refuse to let fear make decisions in my life. I hope my political leaders do the same.”

Kevin C.
“Blanket surveillance of Canadians who have broken no laws, and have not presented themselves to be a known threat should be banned. An agency should only be able to monitor an individual with Just Cause. Just Cause should be clearly defined and continuously monitored to reduce the use of loopholes and grey areas.”

Michael B.
“Domestic spying’ is a euphemism for ‘police state.’ A police state is not the product of a government with a sound mind. Instead of scrutinizing the people of Canada, perhaps we ought to be officially scrutinizing our would-be officials before (and after) allowing them to assume responsibility for our representation.”

Sarah B.
“I think the intrusion of the government on our rights to privacy is of utmost concern. I feel more threatened by the unchecked power of our government than by most other real or PERCEIVED threats. We need a government that is interested in the civil liberties and happiness of the population it represents.”

Marc K.
“0% tolerance to government/RCMP/CSEC or any other agency, group, entity of the government, foreign or domestic, monitoring personal data. Personal data may be reviewed when: A crime has been committed, with a suspect then under investigation for said crime, warrant to glean past personal data issued by a judge, signed off by the head of an independent oversight group.”

Steve S.
“A budgetary limit should be placed that adequately represents to value the agency provides Canadians. A billion dollar facility is just complete irresponsible spending. A billion dollars in health care would have saved more lives in one month than a spy agency could even help in several decades.”

Devon M.
“A complete new draft of a new set of laws that would set multiple levels of safeguards and oversight, without requiring anything that would lead to government secrets being leaked.”

Patricia M.
“I am really disturbed by the government’s lack of transparency and accountability. We need independent, non-partisan oversight of all surveillance activities. And for there to be full public disclosure thereof; and further sharp penalties for intruding on the privacy of citizens without a warrant... I do not want to live in a police state. That is not what it means to be Canadian and I would like our government to remember that.”

Here is a sample of comments we received from participants at our high school event hosted by the B.C. Civil Liberties Association:

Sal R.
“It is a threat to autonomy, trespass to the mind. Your most basic human right is your right to be yourself.”

Darragh L.
“Privacy is important to me because I would like to not have every detail about me known. We are on the precipice of an Orwellian society.”

Michael F.
“Privacy is an intrinsic human right. We shouldn’t be surveilled without reason even if it creates an environment of social control for an ‘optimum society’. It is Orwellian.”

Michaela
“No one should be allowed to go through your stuff. If you’re doing something wrong, get a warrant. The government would flip if you spied on their databases.”

Jogti D.
“Privacy is important to me because I don’t want strangers to know everything about me.”

Felix C.
“Privacy is one of the biggest constitutional rights we own, cousin to freedom of speech. No one should be able to delve into someone’s mind, not even our ‘democratically’ elected government.”
Alex S.
“There are places where you should not feel threatened. For example, if you are on Facebook you shouldn’t be scared that something you say or post will have negative impacts against you. Though I do agree with monitoring dangerous targets with a warrant.”

Keenan S.
“Privacy is important to me because it shapes my behaviour online, and it also allows me to participate in the online community without fear of being persecuted or spied on.”

Kurtis
“Privacy is important because I’d prefer if the government didn’t know I went to an OpenMedia lecture about the trouble with Canadian government spying.”

Melissa B.
“No one wants all their personal information collected and analyzed for the government to make a complete profile of you and everything you’re doing.”

Key input from organizations involved in the crowdsourcing process:

We also invited a range of organizations involved in the privacy sphere to provide input as part of our crowdsourcing process. Here are their priorities:

**B.C. Freedom of Information and Privacy Association:**
B.C. FIPA is a non-partisan, non-profit society that was established to promote and defend freedom of information and privacy rights in Canada. Their top priority in terms of developing new privacy safeguards is *Tough penalties for when government breaks privacy laws*, followed by *Require a warrant for government to spy on personal information* and *End blanket surveillance of law-abiding people*.

**Canadian Access and Privacy Association:**
The Canadian Access and Privacy Association is a national non-profit organization whose goals are to promote knowledge and understanding of access and privacy laws and experiences in Canada. Their top priority in terms of developing new privacy safeguards is *ending blanket surveillance of law-abiding people*, followed by *requiring a warrant for govt to spy on personal information*, and *privacy rules being shaped democratically*.

**Canadian Constitution Foundation:**
The Canadian Constitution Foundation (CCF) is a registered charity, independent and non-partisan. They defend the constitutional rights and freedoms of Canadians in the courts of law and public opinion. Their top priority in terms of developing new privacy safeguards is *ending blanket surveillance of law-abiding people*, followed by *requiring a warrant for govt to spy on personal information*, and *more transparency around govt collection of personal data*.

**Canadian Institute of Access and Privacy Professionals:**
CIAPP is a volunteer-based organization run by access and privacy professionals. Their top priority in terms of developing new privacy safeguards is *ending blanket surveillance of law-abiding people*, followed by *requiring a warrant for govt to spy on personal information*, and *tough penalties for when government breaks privacy laws*.

**National Council of Canadian Muslims:**
The National Council of Canadian Muslims is an independent, non-partisan and non-profit organization dedicated to protecting the human rights & civil liberties of Canadian Muslims (and by extension of all Canadians), promoting their public interests and challenging Islamophobia and other forms of xenophobia. Their top priority in terms of developing new privacy safeguards is *Privacy rules should be shaped democratically*, followed by *End blanket surveillance of law-abiding people*, and *tough penalties for when govt breaks privacy laws*.

**National Firearms Association:**
The National Firearms Association of Canada works for and with Canadian gun owners. The NFA keeps gun owners informed about current and pending legislation and ensures that gun owners know their rights under Canadian law. Their top priority in terms of developing new privacy safeguards is *ending blanket surveillance of law-abiding people*, followed by *requiring a warrant for govt to spy on personal information*, and *tough penalties for when government breaks privacy laws*.

**PEN Canada:**
PEN Canada is one of the 148 centres of PEN International. Founded in 1926, it has a membership of over 1,000 writers and supporters who campaign on behalf of writers around the world who are persecuted, imprisoned and exiled for exercising their right to freedom of expression. Their top priority in terms of developing new privacy safeguards is *requiring a warrant for govt to spy on personal information*, followed by *independent oversight and review of spy agencies*, and *ending blanket surveillance of law-abiding people*.
APPENDIX II: Methodology
This section describes the methodology we used for this crowdsourcing project. It is also designed to inform other organizations, in Canada and around the world, who may be considering using crowdsourcing methods for their outreach or policy work.

Although this project was both topic- and country-specific (“Privacy in Canada”), we believe our methods could quite straightforwardly be adapted for other topics and settings. For example, OpenMedia used similar methodology for a 2013–14 international project aimed at crowdsourcing fair copyright rules.

Project background

OpenMedia has been involved in privacy work since its foundation. As an Internet freedom organization, working for strong privacy safeguards, especially online, is a key pillar of our work.

Accordingly, we had been engaged for many years in a wide range of privacy-related campaigns and initiatives. As outlined in more detail in the introduction to this report, by mid-2014 it was clear that Canada faced a widening privacy deficit, solutions to which needed to be identified.

As a community-based organization, crowdsourcing has always been at the heart of OpenMedia’s values. We know from experience that often the best ideas and most penetrating insights come from everyday citizens. We therefore set out to ensure we could identify solutions to Canada’s privacy deficit through crowdsourcing. We adapted and built on lessons learned from previous crowdsourcing exercises we had been involved in, to capitalize on the potential of the Internet for participatory democracy.

Drafting of the questionnaire

We decided to create a drag-and-drop tool to start our crowdsourcing questionnaire. From previous experience, we learned that the interactive nature of this tool proved popular as a way of engaging people in the subject matter. It also provided a low-barrier way for people to have their say, especially as we offered the option of submitting responses at each stage of the questionnaire, rather than requiring participants to complete the entire questionnaire before they could submit their answers.

The drag-and-drop tool questions were shaped by input from many people, including OpenMedia staff and community members, and colleagues and organizations from the Protect Our Privacy Coalition. Thanks to previous crowdsourcing projects, OpenMedia has built up a good deal of institutional experience in this area, the lessons of which we were able to apply to the design of this report. Key lessons included the importance of being clear about the crowdsourced nature of the project, the role that participants would play, and the scope of the problem we were seeking a solution to. We also know the importance of ensuring that the questions are phrased in a way that clearly explains the issue while being accessible to a non-technical audience.

We also consulted leading privacy experts and organizations, and we are particularly grateful for their assistance when it came to the wording of the more detailed questions about potential privacy reforms.

We aimed to keep the questions fairly accessible and high-level, particularly when it came to the content for the drag-and-drop tool. We decided that we would obtain the most useful information by asking participants to rank a range of pressing high-level privacy priorities in order. Their priorities, in turn, would shape the overall direction of this report. “Require a warrant...” and “End blanket surveillance...” were by some distance the top 2 priorities selected by participants, and each of these recommendations play a prominent role throughout this report.

That said, we also wanted to give participants the opportunity to weigh in on specific potential reforms, such as those proposed by the federal Privacy Commissioner. For this reason, as participants worked through the crowdsourcing tool, the questions became progressively more detailed and specific, although we strove to ensure that all questions were accessible and understandable for the general public.

Finally, we provided participants with an opportunity to provide open-ended feedback. 562 participants (or 5.6% of the total) did so. Again these often detailed comments helped shape and inform the overall direction of the report, and many of them are published throughout.

Development of the online tool

Once the final shape of the questionnaire had been determined, we proceeded to develop the online version of the tool. This was developed by OpenMedia’s in-house web development team. Our team built the tool largely using Drupal 7, with some additional development work required to ensure the drag-and-drop tool functioned as intended.

A number of technical challenges had to be overcome, notably in ensuring that the order in which each drag-and-drop option appeared was randomized for each user. A further technical challenge was
designing a system whereby each user who completed the tool was assigned a unique URL which they were encouraged to share on social media. We also created a leaderboard to publicize which users had succeeded in encouraging the most new participants.

We worked to ensure the tool would be usable by participants on a range of devices, including tablets and smartphones. A separate version of the drag-and-drop tool was built for mobile device users, with a pull-down menu replicating the drag-and-drop functionality. The tool was also able to detect whether a participant was using a mobile device, and to serve up the correct device-specific version automatically. The tool was tested extensively on a range of devices prior to launch.

Launching the questionnaire

In order to maximize participation in this project, we ran an extensive publicity campaign around the launch of the tool. This encompassed sustained social media outreach, including share images, along with securing traditional and online media coverage. We also emailed OpenMedia supporters who had previously been involved with our privacy-related activities to encourage them to take part.

As outlined above, we also encouraged people who completed the tool to share it with their friends, colleagues, and networks via social media. We offered modest prize packages to incentivize this sharing. These prizes were designed to appeal to people interested in privacy, for example by including a year’s subscription to the Canadian VPN service Tunnelbear.

We also created a leaderboard so that people could keep track of their progress, the promotion of which was a key component in our overall messaging. With crowdsourcing it is critical that as many people as possible participate. Using online tools in ways that gamify the user experience can be extremely helpful to increasing participation.

We sustained publicity, especially on social media, throughout the eight weeks in which the tool was ‘live’ and available for people to participate in. High-profile figures including Margaret Atwood and Antonia Zerbisias supported us by taking part in the project, and by encouraging others to do so via their social networks.

We also intensified our publicity activities in the run-up to the deadline, with a “last chance” message to ensure that people who had considered using the tool had a chance to do so before the close of the public participation period.

In-person events

Although the tool was primarily designed to be used online, we also created an offline version of the first drag-and-drop question for use at in-person events. With the assistance of volunteers, we organized three in-person events - one each in Vancouver, Montreal, and Halifax. See Chapter 4: The Process in this report for more details.

Facebook Town Hall

As part of our crowdsourcing work for this project, OpenMedia hosted a Facebook Town Hall about privacy issues. Tom Henheffer, executive director of our coalition partner at Canadian Journalists for Free Expression co-hosted the event with OpenMedia’s Steve Anderson. We had a lively discussion, as Steve and Tom fielded questions from Canadians on privacy issues. The NDP’s digital issues critic Charmaine Borg also joined the debate. We reached over 46,000 people with this event, and input from this Town Hall helped shape this report.

Data collection and analysis

We made the survey freely available online, so that individuals who wished to participate could do so without being contacted by email.
Overall, 10,107 people took part, and we estimate a majority of these were already members of OpenMedia’s community.

We also encouraged and incentivized participants to share the tool through social media, thereby introducing elements of chain referral sampling into our total sample population. In total, 2371 respondents (23 percent of the total sample) were recruited by other participants through social media.

The data collection period spanned from October 22, 2014 to November 30, 2014, after which the results were analyzed.

Adaptation for a regional or international target audience

While this project’s scope was specific to Canada, it should be relatively straightforward to pitch a similarly designed project at a smaller (regional) or larger (international) audience. The scope of the questions could quite easily be adjusted to make sense to the target audience in question.

We would recommend creating multilingual versions of the tool for international projects where a significant percentage of the target audience does not speak English. As noted below, we were unable due to resource constraints to produce a French-language version, dampening response rates in parts of Canada, particularly Quebec.

This project was pitched at Canadians, who live in a country of around 35 million people. For projects pitched at smaller populations, we recommend putting thought into how to ensure your response rate is sufficient. For example, this could mean placing a high priority on publicity activities surrounding the tool to compensate for the smaller target population.

Limitations of our methodology

Due to the design of the survey, respondents had the ability to submit their responses and exit the survey at any time, without needing to answer every question. We thought this was preferable to forcing participants to complete the entire survey at the risk of reducing the response rate.

For this reason, Question 1 of the tool, which asked participants to rank a set of six priorities, received 10,107 responses, as it required a response from users before they could proceed. Other questions received varying numbers of responses, as detailed above and noted throughout the report.

We did not collect demographic information about participants, in part because asking for such information could have dissuaded some people from taking part. For this reason, our sense of the limitations with regards to demographics is speculative. Aside from the limitations of a voluntary response bias introduced by our sampling method, the absence, aside from a small number of in-person events, of an alternative mode of offline data collection would have further limited our sample population to people affluent enough to have easy access to the Internet.

One major limitation of the project and survey was the lack of multilingual content, and therefore the lack of discussion and involvement from non-English speaking Canadians. Most notably, this impacted response rates in parts of Quebec. Resource constraints meant that we were unable to consult them with a French-language version of the tool.
REFERENCES

Because we did our research...

7. The Protect our Privacy Coalition. The coalition calls on Government to put in place effective legal measures to protect the privacy of every resident of Canada against intrusion by government entities.
12. Ibid.
18. Ibid.
19. Specifically including a requirement to get a warrant. For more on this, see Recommendation 1 of this report.
20. Henceforth referred to as the Charter.
24. Metadata is data that describes other data. When collected in bulk, such as by the NSA and CSE, it can reveal a great deal of personal information about individuals.


We strongly recommend Profs. Forcino & Roach's detailed analysis available at http://antiterror.ca


It does allow for information to be shared in certain circumstances, according to strict criteria. For example, see these Treasury Board guidelines: http://www.tbs-sct.gc.ca/aptp-agrpp/csa-eria/eertb-eng.asp


iPolitics: Kej legal voices blocked from c-51 committee debate. Source: http://www.ipolitics.ca/2015/03/17/kejs-legal-voices-blocked-from-c-51-committee-debate/


Angus Reid: February 2015 survey on Bill C-51. Source: http://angusreid.org/53/


See ‘Recommendation 3: Embrace Accountability’ in this report.

It’s now taking SIRC an average of three years to investigate complaints against CSIS. CBC News: CSIS watchdog agency starred off staff, resources. Source: http://www.cbc.ca/news/politics/csis-watchdog-agency-starved-of-staff-resources-1.2965276


CSE recently underwent a name change, and is also familiar to Canadians as ‘CSEC’.


Justice Laws Website: Anti-terrorism Act 2001. Source: http://laws-lois.justice.gc.ca/eng/acts/A-11.7/ [not to be confused with Bill C-51, legislation introduced in 2015 which is also titled the Anti-terrorism Act]


The National Post: How federal bill C-13 could give CSIS agents – or even Rob Ford – access to your personal online data. Source: http://www.thestar.com/news/canada/2014/05/03/how-federal-bill-c-13-could-give-csis-agents-even-rob-ford-access-to-your-personal-online-data/

Parliament of Canada: Bill C-13, 2nd session. Source: http://openparliament.ca/bills/41-2/c-13-

Michael Geist: Canadian telcos asked to disclose subscriber data once every 27 seconds. Source: http://www.michaelgeist.ca/2014/01/07/telco-disclosures/


OpenMedia: Protect Our Privacy. Source: https://openmedia.ca/ourprivacy


For more on how foreign-based private companies are taking advantage of weak Canadian privacy safeguards, see Michael Geist. Rightscorp and BMG Exploiting Copyright Notice and Notice System. Citting False Legal Information in Payment Demands. Source: http://www.michaelgeist.ca/2015/01/rightscorp-bmg-exploiting-copyright-notice-notice-system-citing-false-legal-information-payment-demands/

The Guardian: U.S. and U.K. struck secret deal to allow NSA to ‘unmask’ Britons’ personal data. Source: https://www.theguardian.com/world/2013/jun/21/uk-usa-security-britain-idUKBRE95K10620130621


Justice O’Connor recommended that SIRC also monitor the national security activities of Citizenship and Immigration Canada, Transport Canada, the Financial Transactions and Reports Analysis Centre, and the Department of Foreign Affairs and International Trade.


The Guardian: NSA performed warrantless search on Americans’ calls and emails. Source: http://www.theguardian.com/world/2014/apr/01/nsa-surveillance-loophole-americans-data

The Guardian: Canada ‘allowed NSA to spy on G8 and G20 summits’. Source: http://www.theguardian.com/world/2013/jun/28/canada-nsa-spy-g8-g20-summits


For more on the campaign against Bill C-30, see http://stopspying.ca


The Intercept: New Zealand used NSA system to target officials, anti-corruption campaigner. Source: https://www.theintercept.com/2015/03/04/new-zealand-kegcore-solomon-islands-nsa-targets/

A full copy of the Principles can be found at https://necessaryandproportionate.org/nnap/


Office of the Privacy Commissioner: Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance. Source: https://www.priv.gc.ca/informationsrs/201314/crc.c_e.asp


The Guardian: Canada ‘allowed NSA to spy on G8 and G20 summits’. Source: http://www.theguardian.com/world/2013/nov/28/canada-nsa-spy-g8-g20-summits

CBC News: New tool helps Canadians find out if telecoms are collecting their info. Source: http://www.thecourt.ca/2014/10/01/safeguarding-online-anonymity-r-v-spencer-revisited/

The Court: Safeguarding Online Anonymity: R v Spencer Revisited. Source: http://www.thecourt.ca/2014/10/01/safeguarding-online-anonymity-r-v-spencer-revisited/


For more information about this, see OpenMedia.org/DigitalFuture


The Guardian: NSA performed warrantless search on Americans’ calls and emails. Source: http://www.theguardian.com/world/2013/jun/21/gchq-cables-secret-world-communications

Wired U.K.: GCHQ and NSA hacked SIMs to spy on billions of phones. Source: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications


For more for more information about this, see OpenMedia.org/DigitalFuture