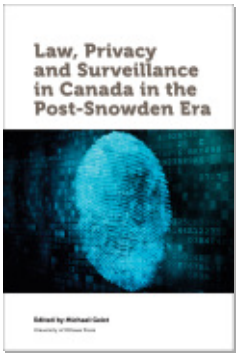
Law, Privacy and Surveillance in Canada in the Post-Snowden Era



Michael Geist, Wesley Wark

Published by University of Ottawa Press

Geist, Michael and Wesley Wark.
Law, Privacy and Surveillance in Canada in the Post-Snowden Era.
University of Ottawa Press, 2014.
Project MUSE.muse.jhu.edu/book/40610.

CHAPTER IX

Stuck on the Agenda: Drawing Lessons from the Stagnation of "Lawful Access" Legislation in Canada

Christopher Parsons

Concerns surrounding government access to communications data are not a new social problematic. Letter mail, the telegraph, phone calls, and other technologically mediated forms of communication have routinely given rise to social privacy concerns.[1] And the politics of such surveillance have often been explosive when new technologies have been made subject to government interception requirements, and even more explosive when it is found that government has surreptitiously engaged in the surveillance of its citizens without publicly declared legal authorities. At this point, proposed legislative expansions of government agencies' surveillance capacities in Western democracies often fall under the heading of "lawful access" powers, which captures expansions of government agencies' search and seizure, communications interception, and subscriber data production powers. Governments routinely justify such expansions as needed to catch up to contemporary criminal activities, to defray or prosecute acute criminal activities, or to equalize law enforcement authorities' powers across international jurisdictions.

Governments' legislative attempts to expand state agencies' lawful access powers are not always successful. The failures of successive Canadian governments to pass such legislation is a case in point. These failures are often the result of governmental indifference and/or successful advocacy protesting expanded powers. This chapter examines the Canadian failures in order to identify some

political conditions that should be met if similar legislation is to be successfully opposed in other jurisdictions.

The chapter begins by outlining how agenda setting operates and the roles of different agendas, tactics, and framings. Next, it turns to the Canadian case and identifies key actors, actions, and stages of the lawful access debates. The agenda-setting literature lets us identify and explain why opponents of the Canadian legislation have been so effective in hindering its passage and what the future holds for opposing similar legislative efforts in Canada. The final section steps away from the Canadian case to suggest that there are basic as well as additive general conditions that may precede successful political opposition to newly formulated or revealed government surveillance powers that focus on either domestic or signals intelligence operations.

Agenda Setting and Expanded Policing Powers

Before analyzing the politics that drive Canadian lawful access legislation it is helpful to turn to the agenda-setting literature to understand why certain issues are more or less successful in being placed on an agenda and then advanced to legislative action. Agendas constitute broad collections of problems, issues, solutions, and causes of problems that rise to the attention of the media, the public, and policy makers. While agendas can be as formal as lists of bills before a legislature or long-running news stories that have been planned for some time, they can also include beliefs about the significance of problems, about the need for particular solutions, or about the roles of various actors to address a problem or implement a solution.

The media agenda "mediates between policy and public agendas, constructs the public agenda and seeks to influence policy agendas."[2] This agenda is often important for amplifying, translating, or linking issues that might be on the policy or public agendas. The public agenda, in turn, refers to key issues that are in the minds of the public generally, and typically accounts for no more than five to seven items at a time.[3] In contrast, the policy agenda is composed of issues or items that the government of the day regards as its most pressing; this agenda is often made manifest through the bills that are on an Order Paper or issues being debated privately amongst influential legislators. These bills, topics, or issues may be moved to be implemented as law or withdrawn from the legislative process

depending on whether the other two agendas also prioritize an issue on the policy agenda or, alternately, if these agendas are not used to stymie the passage of items on the policy agenda.

Of course, not all issues command similar degrees of importance, with importance often based on whether actors with high degrees of public, political, or media capital have prioritized a given issue. Events can arise, however, without the guidance of any particular actor or community; when a focusing event manifests even well-capitalized actors may be limited in how they can control a given issue's ascendance on the media, public, and policy agendas. A focusing event occurs suddenly and is "*relatively rare, can be reasonably defined as harmful or revealing the possibility of potentially greater future harms, inflicts harms or suggests potential harms that are or could be concentrated on a definable geographic area or community of interest, and that is known to policy makers and the public virtually simultaneously.*"[4] There might, however, only be a "loose connection between the character of the happenings and their becoming a key event. The fact that an occurrence becomes a key event therefore still gives no information as to why it became one."[5] As a result, while high-capitalized actors might have their own agendas disrupted by a focusing event, all involved actors might struggle to successfully define the problem and solution within the context of the focusing event and, for parties that fear losing control of the agenda, such actors might try to use the event to suppress the issue off relevant agendas.[6]

The power of focusing events is accentuated when associated with a symbol or drawn into a pre-existing or rapidly developed narrative: in such cases, these events are "more likely to be characterized by high levels of support, high likelihood of action, and low freedom of action than those that enter through 'normal' political processes."[7] Moreover, events that are linked to symbols or narratives are more likely to rise on all agendas, simultaneously, to the point where a common consensus emerges amongst experts and non-experts alike that "something must be done."

More specifically, symbols operate as referents to deeply held social or cultural roots, and by appealing to them actors try to clarify how their framing of an issue resonates with the symbol. So, by linking a policing or security issue to protecting innocent children, for example, a set of assumptions and values (the right for children to be protected, the appropriateness of stopping harm before it occurs, the legitimacy of using force and surveillance to dilute or prevent such

harms, and so on) can immediately come into play. Narratives can complement the use or cooptation of symbols insofar as they paint storylines of how to interpret a symbol, often in a reductive fashion. So, to protect children, it is important for police to have the same capabilities today as they did twenty or thirty years ago, such as the ability to passively monitor for suspicious activity and stop and ask for identification of parties who seem suspicious. Of course, in a contemporary digital policing framework, that passive monitoring might include abilities to be automatically notified by telecommunications service providers (TSPs) when the providers register a deviant activity or action, and request for identification might include the mandatory and warrantless receipt of subscriber information from a TSP. Whereas proponents for such powers may play on the reductive logic of their arguments, opponents might spin a narrative that captures the duplicity or falsity of such reductive stories or use of a culturally significant symbol.

Of course, the means by which parties are more or less successful in advancing their interests corresponds with their abilities to place issues on institutional decisional agendas that are amenable to specific actors' identifications of problems, solutions, and mechanisms of implementing solutions. Attempts to forum shop often enjoy prominent placement in the agenda-setting process. Actors routinely case their favoured forums as the most appropriate to take up a given problem and identify a suitable solution. The decision of which forum takes up an issue can be critically important when actors believe that policy debates will be settled very differently based on which adjudicator and accompanying institution comes to own the issue.[8]

As will become clear, the issue of expanding lawful access powers in Canada has followed a meandering road. Successive governments have taken up the issue, often with differing levels of interest or commitment. Aligned communities, such as TSPs and civil liberties groups, have fractured. Different narratives have been adopted to try to justify implementing the legislation, and considerations of these powers have escaped legislative institutions. And, somewhat surprisingly, one majority federal government failed to pass lawful access legislation when offered the opportunity to do so. In what follows, I argue that lawful access has been stuck on the Canadian policy agenda as a result of weak governments, strong opposition to the legislation, and damaging consequences of framing events, and that the Canadian situation provides insights for other jurisdictions

where actors oppose the maintenance or expansion of novel government surveillance powers.

Canada and Lawful Access on the Agenda

Successive Canadian governments sought to pass legislation to extend domestic authorities' access to telecommunications data. These efforts began in earnest following Canada's signing of the *Convention on Cybercrime* in 23 November 2001. In brief, the convention was premised on the fact that criminal activities take place on, and through, computer equipment and that signatory nations must cooperate to detect, investigate, and prosecute criminal computer-based activities. Part of the ratification process required national governments to "create several offences, including unlawful interception, access or interference with a computer system, computer-related forgery and fraud, and offences relating to child pornography and copyright."[9]

In addition, the *Convention on Cybercrime* required the expansion of authorities' investigative powers. Several federal governments have used these requirements to justify the following: requiring TSPs to be able to intercept their subscribers' communications; enabling authorities to compel subscriber data from TSPs without a court order; mandating the creation of new preservation and production orders; potentially establishing a key escrow system for encrypted communications; and authorizing government agencies to install malware on location-aware devices such as smartphones and GPS equipment.[10] In the wake of signing the convention, government spokespersons suggested "that new communications technologies and a deregulated telecommunications environment required some serious legislative upgrading and modernization of electronic surveillance rules… The expectation was that the legislation would follow expeditiously, although there would be time for public and industry consultation before a final draft was prepared."[11] Ultimately, as a result of federal elections and successful civil liberties opposition to the legislation, along with businesses' resistance, lawful access legislation was not expeditiously made into law: it instead languished on the Canadian agenda.

There were a series of moments when lawful access legislation loomed large on public, media, and policy agendas simultaneously. At other moments, the legislation was featured more prominently

on only one or two of those agendas. In each case, however, a core group of actors took part in the debates, with the actors tending to assume similar (and often self-interested) roles. Throughout, actors contested how the proposed powers would manifest as laws, as technical demands, as costs on business, and as transformative to policing practices.

The Actors

A community of governmental organizations advocated for expanded lawful access powers, whereas civil liberties groups, along with some federal opposition parties and privacy commissioners, opposed the expansions. TSPs and academics joined civil liberties groups. Together, these elite actors constituted the principal members of the Canadian policy network that took up lawful access. In the case of government actors, they were often also responsible for deciding on whether, and if so how, lawful access powers would be instantiated in policy or law. These actors also controlled the decisions as to which government policy forums took up the issue of lawful access.

Government organizations that explicitly supported the expanded powers include the federal governments that introduced the legislation and members of Canada's law enforcement community. Successive governments asserted that the powers were needed to protect Canadians from criminals and terrorists,[12] to identify and prosecute pedophiles,[13] to catch violent offenders,[14] and to deal with cyberbullying.[15] As the rationale for the legislation shifted, parties external to the government itself came onside, such as groups that regarded the legislation as useful for preventing child pornography or bullying.

Core groups that opposed the legislation included civil liberties organizations, privacy commissioners, some academics, and (at differing points) TSPs. Civil liberties organizations included the British Columbia Civil Liberties Association (BCCLA), British Columbia Freedom of Information and Privacy Association (BC FIPA), Canadian Centre for Policy Alternatives (CCPA), Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), Canadian Civil Liberties Association (CCLA), and OpenMedia. Organizations with a legal focus (e.g., BCCLA, CIPPIC, BC FIPA, CCLA) emphasized legal rationales for why expansions of lawful access powers were unnecessary, unlawful, or unconstitutional, often with accompanying assertions that constitutional acceptability was the "lowest degree,"

rather than "highest standard," of civil liberties protection.[16] Other civil liberties groups, such as OpenMedia and CCPA, focused on mobilizing popular support and disseminating specialized knowledge produced by legally oriented groups and academics to a broader generalist and policy-oriented public. Academics, in aggregate, wrote extensively on the legal, technical, financial, and normative dimensions of expanded law enforcement capabilities, with publications linked to specific moments of the lawful access debates. Within government itself, provincial and federal information and privacy commissioners argued against the necessity and/or appropriateness of powers proposed by governments of the day;[17] the same was also true of federal opposition parties.[18]

Canada's TSPs played differing roles throughout the times that lawful access arose on the agenda. These companies raised doubts about the necessity of the powers, the reasonableness of businesses shouldering the costs for expanded surveillance practices, the technical requirements needed to implement iterations of the legislation, whether regulatory updates were to be preferred over legislative actions, and the relative value of warrantless disclosure of subscriber information.[19] The opposition to legislative measures on the basis of cost was a high-emphasis point,[20] and subtle or relatively secretive attempts to implement some lawful access powers by way of regulation (as opposed to legislation) resulted in prolific opposition.[21]

Each time lawful access arose on the agenda, journalists intermediated the discussions between the various actors. And each time lawful access arose, there was extensive media coverage in all of the flagship media organizations in Canada, as well as second- and third-tier outlets. This coverage served as a means by which proponents and opponents of the legislation evaluated the effectiveness of the framing of the issue, each time the debate (re)arose.

Early Canadian Consultations and the Drawing of Battle Lines

Lawful access has arisen recurrently on the Canadian political landscape since the *Convention on Cybercrime* was signed. Two separate consultations took place in 2002 and 2005 that brought "together a diverse group of stakeholders with sometimes competing interests" and, as the federal government stated, led to legislative proposals that "were informed by the previous consultations, and represent a balancing of the needs of law enforcement, industry and privacy groups."[22] The 2002 consultation received three hundred written

comments and submissions concerning new lawful access powers, and these entries formed the basis for in-depth consultations in 2005. Whereas the 2002 consultations saw a diverse and largely representative set of stakeholders (industry, privacy advocates, law enforcement, and others), the 2005 consultations were principally held with members of industry, vendors, and law enforcement. Following the conclusion of the consultations, the government introduced the *Modernization of Investigative Techniques Act (MITA)* in 2005. *MITA* included expanded access to subscriber number and name information and required TSPs to make new services and products interceptable by government agencies, in addition to new preservation and production orders. *MITA* ultimately failed to get past first reading, with the minority government dissolved mere weeks after introducing the legislation.[23]

In the short time it was on the Order Paper, government attempted to frame the new powers in *MITA* as needed to "ensure that criminals can no longer take advantage of new technologies to hide their illegal activities from the law."[24] Moreover, the legislation was proposed as needed to "reduce the ability of criminals, organized crime members and child pornographers to use sophisticated technologies to carry out their activities undetected."[25] Privacy advocates maintained that it was unclear that the powers were genuinely needed and, regardless, inadequate oversight was included in the legislation — points that they expressed throughout their opposition to the legislation.[26] Similarly, information and privacy commissioners raised doubts about the need for and appropriateness of the legislation.[27] Ultimately, however, *MITA* was short-lived and subordinated to more pressing political issues of the day. Despite appearing on the policy (as a bill), public, and media agendas, there was insufficient time for actors to mobilize prolonged support for or opposition to the legislation. Even its brief period on the Order Paper, however, provided federal public servants sufficient data to recognize that the public had been concerned about the proposed powers, and that the public's "underlying anxiety [was] heightened by the media and [by] statements of privacy and civil liberties advocates."[28]

While each of the mentioned episodes merited media attention, with various actors assuming their usual roles, it was subsequent introductions of the lawful access powers that saw concerted aligning of media, public, and policy agenda-setting windows, to the effect that actors were extensively invested in framing the issues linked to

lawful access. Moreover, by this point, members of the civil liberties community and industry had largely been split from operating as an allied group; this began in 2005 with consultations where government advanced proposals to defray industry concerns (i.e., ambiguity, cost, legality). The result was to make civil liberties groups have to "work harder" to influence lawful access debates.[29]

That requirement to work harder was made clearer in 2007, when Public Safety Canada began another set of consultations that initially excluded many members of the privacy and civil liberties communities. Only after the consultation document was obtained and subsequently publicized by an academic[30] and then discussed by the media[31] did the minister of Public Safety, Stockwell Day, establish a fuller consultation. This incident was a clear example of the government attempting to quietly control an issue on the policy agenda while keeping it off the public or media agendas so as to advance negotiations. As soon as the issue exploded on the media agenda, however, the minister was forced to expand the consultation and state that any proposed powers would be protective of Canadians' privacy rights; legislation would not "grant police the power to get information from Internet companies without a warrant. That's never been a proposal… It may make some investigations more difficult, but our expectation is rights to our privacy are such that we do not plan, nor will we have in place, something that would allow the police to get that information."[32] In effect, government, law enforcement, and industry ceased being the primary actors debating the issue once it was on the media and public agendas. Participants maintained familiar roles in the expanded consultations. It was the minister's statement and not the consultations themselves that played a key rhetorical role when the government introduced subsequent iterations of the legislation.

Legislation similar to *MITA* was introduced in June 2009 and generated controversy between the actors invested in the issue. Unlike subsequent efforts, however, the government was not forced to retreat from its proposed legislation: instead, the lawful access bills (C-46 and C-47) were referred to committee but never reviewed because they died on the Order Paper when Parliament was prorogued later that year. Ultimately, the battle lines between members of the policy network had largely been drawn by the end of 2009, and it was understood that successive governments would likely repeat their attempts to pass lawful access legislation.

Aggressive Campaigning and Policy Arena Segmentation

There have been three main explicit attempts to pass lawful access laws since the battle lines were established. In 2010 a series of bills were introduced (C-50, C-51, and C-52); in 2012 Bill C-30 was placed on the Order Paper; and in 2013 the government tabled Bill C-13. C-13 received royal assent in January 2015. The first set of bills were justified by the minister of public safety on grounds that they fit within the Conservative Party's election mandate to "give law enforcement and national security agencies up-to-date tools to fight crime in today's high-tech telecommunications environment," that they were needed to "bring our laws into the 21st century and provide police with the tools they need to do their job," and that the legislation struck "an appropriate balance between the investigative powers used to protect public safety and the necessity to safeguard the privacy of Canadians."[33] While the government maintained that the legislation was balanced, it failed to frame the legislation as a solution to a problem on the public or media agendas: instead, opponents successfully framed the legislation as a problem in and of itself.

Because iterations of the powers had been introduced, and discussed, previous to the 2010 legislation, there was ample pre-existing knowledge about how they might function amongst opponents, the media, and interested members of the public. Further, opponents had been able to test lines in previous conflicts; as a result, opponents could rapidly engage in information politics, or the generation of "politically relevant information and to move it by the most effective means to the place where it will have the most impact, at the most critical time."[34] Since opponents had courted relationships with specific members of Parliament and the media, and within well-mobilized civil liberties organizations, information could be tactically dispensed as needed, often to the effect of upsetting government balancing statements or justifications for the legislation. Opponents could also rely on accountability politics, where powerful agents were held to their previously uttered public statements. Specifically, the former minister of public safety's statement that warrants would be required for information to be disclosed to state authorities was leveraged because C-50, C-51, and C-52 lacked these warranting requirements. While the lawful access legislation was introduced to Parliament, the battle over it was predominantly fought in the media, wherein opponents drew on their technical, legal, and

political expertise to cast the bills in a negative light. Ultimately, the government did not forge ahead and try to pass the legislation; instead, they let it die by calling an election.

The subsequent version of the legislation, C-30, bore strong resemblance to the previously introduced lawful access bills. First given the short title, *Lawful Access Act*, it was renamed the *Protecting Children from Internet Predators Act* immediately prior to being introduced.[35] Shortly after the bill's introduction, the minister of public safety, Vic Toews, asserted that opposition parliamentarians could either "Stand with us [the government] or with the child pornographers."[36] The effect of this statement was overwhelmingly negative from the government's perspective: in his framing, the minister cast well-regarded opponents, such as Canada's privacy commissioners, and any person who had concerns over the legislation, as supportive of child abuse. While the minister and government might have believed that linking the legislation with combatting child abuse would defuse opposition, the verbal framing of the legislation had the exact opposite effect and functioned as a focusing event that activated the media and the public. Ultimately, the minister was forced to apologize for his comment in the face of public pressure just two days after introducing the legislation;[37] this apology failed to relieve the government of charges that it was smearing opponents.

A host of tactics were used to oppose C-30. Social media campaigns explained why the legislation was a problem and mocked the public safety minister.[38] Online petitions that indicated opposition to the legislation were created by activist groups[39] and political parties alike.[40] Mailings that targeted Conservative Party ridings placed pressure on members of the federal governing party.[41] And academics and privacy commissioners continued to dispute the government's statements that the legislation was "privacy protective;" this involved a range of well-reputed individuals taking complementary positions and explaining their critiques in accessible language.[42] In aggregate, this collection of techniques generated politically relevant information and disclosed it to the public at opportune times, successfully took advantage of the minister's initial comments as a focusing event to spin a narrative that the government was smearing opponents and inappropriately trying to wield the symbol of child abuse, included accountability politics in the form of pointing to past promises that warrants would be needed to access information, and finally engaged in leverage politics. This latter kind of

politics involved directing action "towards those who have power in public or private organizations and who can effect change, by imposing a sanction or threat of some manner,"[43] and was manifest in the mailings to select Conservative members of Parliament. The combined result was that the media had a wide range of stories they could run about critical analyses of the legislation, across a range of media spaces.

The debates surrounding C-30 largely took place on the media and public agendas, with the issue landing on those agendas after legislation had been introduced. In reaction, C-30 ultimately was slated to go straight to committee, where it might have been modified to mollify critics. This decision showed that the government was deprioritizing the legislation on its own policy agenda. But the federal government, perhaps in light of the public opposition to the legislation, simultaneously moved to implement aspects of the lawful access powers through another policy forum. During the period of time that C-30 was on the Order Paper, Industry Canada held a consultation about bidding on newly reclaimed wireless spectrum. As part of this consultation, Industry Canada indicated that changes to the *Solicitor General's Enforcement Standards (SGES) for Lawful Interception of Telecommunications* would soon be disclosed by the Department of Public Safety. The SGES outlines how telecommunications companies must integrate interception technologies into their networks as a condition of operating a licensed wireless telecommunications service in Canada. At the same time, Industry Canada proposed making all radio-based transmissions subject to interception requirements, whereas previously only circuit-based communications were subject to such requirements.

This proposal occurred largely outside of the minds of public opponents to the C-30 legislation; the sole public advocacy group that was involved in the consultation failed to raise either of the changes as concerns. But an unexpected group arose to oppose the proposed change: the TSPs, who would have to comply with the changes, if approved. The industry group that represented most of the companies wrote that replacing "circuit switched telephony systems" with "interconnected radio-based transmission facility for compensation" "opens up several additional services to interception requirements, including Internet services, and cable and broadcasting services."[44] The association also stated that any updates to the standards should not incur a cost to the companies in its group, and that

> there has been no enabling legislation passed by Parliament that would require such services be intercepted, and submits that it is inappropriate for the Department to impose such requirements via a COL [Condition of License] — particularly at a time when the Government is engaged in a legislative process covering the lawful access issue at a broader level. The COL should reflect the legislative requirements that exist at the time the licences are issued, and not be crafted in anticipation of legislative requirements that may or may not be in force at some point in the future.[45]

The carriers were not alone in questioning the changes in language or proposed updates to the SGES. Documents obtained through the *Access to Information and Privacy Act* reveal confusion within the government itself: officials at Public Safety Canada, which is responsible for the SGES, believed that if wording in the SGES was modified, then it would apply "more broadly and effectively," though the changes constituted "an interim measure until full implementation of the [lawful access] legislation."[46] It was agreed by officials that the proposed changes to the SGES would not be revealed prior to the 700 MHz auction.[47] Not all of the parties that rely on the SGES were fully drawn into the private intergovernmental debate; a Canadian Security Intelligence Services analyst ended up writing, "I would like to know where this 'exercise' is going!!?? What is its overall purpose…my understanding was that we were simply trying to get the wording in the licensing regime change (& not changing the *SGES* themselves…. do you really want us to re-examine all the standards, etc; up date them to current requirements, [Redacted]?"[48]

Despite shifting lawful access to a new policy forum, and despite the absence of typical opponents of expanded state surveillance legislation (e.g., privacy commissioners or civil liberties advocates and organizations), the government was forced to backtrack: the changes would not expand the range or kinds of communications that had to be interceptable. Instead, the same kinds of communications (e.g., text messages, faxes, and voice communications) that were transmitted using radios would continue to be subject to the historical intercept requirements.[49] When the issue arose before the media a year after the initial proposed terminological changes to radio-based communications, the government asserted, "it never actually had designs on vastly expanding surveillance."[50] Further,

based on documents released under *Access to Information*, it does not appear that a substantive change to the SGES took place.[51] So, the internal confusions and apparent failure to develop a common policy agenda (away from public scrutiny), combined with opposition by TSPs, undermined these backchannel attempts to expand surveillance powers.

Bill C-30 was withdrawn 11 February 2013. The justice minister stated that though efforts to modernize the *Criminal Code* would continue, such modernizations would not contain "the warrantless mandatory disclosure of basic subscriber information or the requirement for telecommunications service providers to build intercept capability within their systems…We've listened to the concerns of Canadians who have been very clear on this and responding to that."[52] Lawful access returned to the Canadian agenda shortly after the minister's statement, this time as Bill C-13. C-13 was introduced 20 November 2013 to crack down on cyberbullying. Casting about for a new symbol, the federal government latched onto the very public suicides of a pair of young women who had experienced systematic online harassment that contributed to their committing suicide. Included in the legislation were amendments to the *Criminal Code* that were identical to those in previous lawful access legislation.

Opposition was mounted in response to C-13 and included assertions that the federal government was strategically appropriating the deaths of a pair of young women for crass political purposes,[53] that authorities did not need the expanded powers to have prosecuted either of the cases,[54] and that the legislation contained clauses that would increase the sharing of information between authorities and telecommunications service providers.[55] Privacy commissioners warned that while the legislation was less problematic, it retained items of concern;[56] similar statements also came from allied academics. Surprisingly, some victims' advocates and family members of victims of cyberbullying and associated crimes also came out to question and sometimes oppose the legislation.[57]

However, having removed the elements of the previous legislation that inflamed the public (warrantless disclosure of subscriber information) and businesses (mandatory interception capabilities within telecommunications networks for new services), as well as by appealing to a powerful symbol that had captured media attention (the deaths of young girls), the government did not experience the same vociferous resistance to C-13 as it had to C-30. The public,

perhaps somewhat wearied and attentive to other issues, was not popularly mobilized to resist the legislation. And the media, while covering the issue, was similarly occupied with other privacy stories: a slate of national security–related privacy issues had arisen to capture the media's and public's attention. The aggregate result was to give the government an opportunity to pass its legislation so long as the media and public agendas did not become so inflamed that the legislation was forced off the policy agenda once again.

Canadian Surveillance Legislation in 2015 and Beyond

At the time of writing, the government has successfully passed its lawful access legislation. Three events failed to disrupt this process. First, national security leaks concerning state access to telecommunications data could have placed the government on the defensive and promoted a retraction of lawful access legislation were the legislation to become associated with the activities described in the leaks. Such associations were not strongly made, however, which meant that lawful access quietly proceeded apace while civil society advocates, members of Parliament, and the media focused instead on revelations that Canada's foreign signals intelligence agency, the Communications Security Establishment (CSE), worked with its closest partners to conduct both targeted and massive surveillance operations.

Second, telecommunications companies have begun to disclose the regularity, conditions upon, and number of Canadians that are affected by state-agencies' surveillance practices in transparency reports. The reports reveal that, in aggregate, government agencies request access to telecommunications data hundreds of thousands of times per year.[58] Rather than primarily exciting attention around C-13, however, the revelations were often framed in the context of signals intelligence surveillance. Though the disclosed data could have called into question whether domestic authorities needed the powers given their existing capacities to compel, or request, data from private companies, these kinds of questions were not prominently raised on the public, policy, or media agendas. In effect, the focus on the activities of the Communications Security Establishment meant that advocates and academics alike did not use the transparency information to rhetorically combat C-13 on the media agenda as much as they might have in years before.

Third, questions put to government agencies by the federal opposition led to revelations that Canadians' personal information is already routinely accessed by these agencies.[59] The Canadian Border Services Agency, for example, made 18,729 requests for telecommunications data, though other agencies such as the Royal Canadian Mounted Police, Canadian Security Intelligence Service, and Canadian Revenue agency were all less forthcoming.[60] Though parliamentarians used the information in the House of Commons and in the media, the revelations were insufficient to force the government to deprioritize the issue on the policy agenda.

Opponents to the legislation had already prepared for its eventual passage; in 2012 a comprehensive legal analysis of proposed lawful access powers was developed to explain why elements of the lawful access bills were on questionable constitutional footing.[61] And courts, including the Supreme Court of Canada, have asserted that government agencies need a judicially authorized order to access subscriber data;[62] companies likely cannot disclose such data without running afoul of the law, nor can authorities request it absent exigent circumstances. A constitutional challenge was also launched to overturn parts of Canadian federal privacy legislation that prevents TSPs from informing their customers when specific customers' information is disclosed to government institutions.[63] The result is that next steps that are largely outside of the legislative agenda-setting process can be, and are being, taken up by critics of the lawful access powers.

Drawing Lessons

After examining how lawful access became stuck on the Canada policy agenda, we can identify some basic and additive conditions that might precede successful political oppositions to expansions or solidifications of government surveillance powers, be they targeted toward domestic surveillance operations or signals intelligence operations. We can also identify how opposition to one form of government surveillance, such as domestic lawful access legislation, can establish a common network of actors who are well-coordinated to oppose to other state surveillance activities.

Basic requirements begin with governments being responsive and reactive to the public and media agendas. If the government can unilaterally pass highly controversial legislation and is willing to spend its political capital in doing so, then even if opponents are

successful in negatively framing surveillance issues on the public or media agendas, the framing might not affect the passage of the legislation. The likelihood of a government being responsive to changes on the media and public agendas will correspond with the importance the government places on the surveillance powers and the extent to which the government's proposals can be taken up in political forums. If the proposed legislative action is at the bottom or towards the middle of the government's policy agenda and can be effectively challenged in legislative arenas, then opponents are more likely to be able to force the issue down or off the agenda, as compared to highly important issues that the government is willing to invest with large sums of its political capital or that operate in opaque or secretive corners of government.

When it comes to deeply secretive practices, such as the CSE's signals intelligence activities, there is heightened difficulty in opposing government policy because ministerial directives and other kinds of policy guidance that authorize and direct the CSE's activities are largely inaccessible to the public. As a result, there are evidentiary and policy difficulties in negatively framing the signals intelligence activities because the precise nature of the CSE's activities and rationales for them are off the public record. Absent whistle-blowers, it is almost impossible to develop enough understanding of the intelligence agencies and their practices to identify what should even be negatively framed in the first place.

Whereas controversial surveillance legislation such as lawful access will open up space to debate the legislation's merits or flaws in the legislative assemblies, committees, and so forth, there is not an equivalent space that is necessarily opened when debating signals intelligence-related directives, which are developed within, and authorized by, the executive branch of government. The result is that finding a legislative space to even frame signals intelligence activities on an ongoing basis can be difficult without a permanent legislative-based intelligence committee. Compounding the difficulties is the secrecy concerning how signals intelligence organizations interpret their authorizing legislation and the classification of their internal policy guidance documents. Even when privacy and civil liberties groups force discussions of signals intelligence activities onto the political agenda, the effectiveness of subsequent framing may be unclear insofar as the actual consequence of the government's proposed amendments, or those accepted by the opposition parties,

may not be understood by anyone other than members of the intelligence community who already enjoy privileged interpretations of existing legislative and policy frameworks. In effect, there is no clear way for opponents of government surveillance practices to be certain their efforts to restrain or modify signals intelligence agencies' practices will be successful. In fact, experience in the United States, where attempts to restrict access to business records actually led the National Security Agency to expand its domestic surveillance operations, make it clear that passing laws meant to delimit such surveillance may be interpreted around by the executive branch and members of the intelligence community.[64]

Two other basic requirements must be met for opponents to successfully set the agenda: there must be sufficiently empty (and interested) media and public agendas. In the case of the former agenda, the media is restricted in how many items are important enough to be covered in any depth at a given time. For an issue to be successfully framed, opponents must be able to either place a handful of stories that are sufficiently explosive to capture the media's and public's attention (and lead to shaping the policy agenda) or else enjoy ongoing access to the media in order to provide negative framings for weeks or months. In effect, the media must not be so entranced with other issues that opponents cannot successfully capture the attention of the press. With regards to the public agenda, it is typically capable of handling no more than nine items at a time. As a result, opponents of expanded surveillance legislation must enjoy either a suitably empty public agenda that is receptive to paying attention to lawful access or, alternately, opponents must reveal information that captures the public's attention away from other issues it is already attentive to. The media, effective appropriation of culturally resonant symbols, or narratives that capture the public imagination can all enhance the chances of opponents successfully placing their framing of surveillance issues on the public's agenda.

Signals intelligence-related surveillance issues can quickly rise on a media agenda when and if a clear and explosive scandal is revealed, and so long as the scandals do not routinely appear. Since Edward Snowden's revelations began to appear, some media organizations have become weary of reporting on the stories, to the point where even leading national security journalists may not read or report on revelations that are part of their normal coverage area. Similarly, the public can pay an incredible amount of attention to

signals intelligence-related agenda items but are more likely to prioritize the general issue of signals intelligence when what is revealed is new and shocking. The constant outpouring of Five Eyes documents, and the technical and legal and policy knowledge required to fully understand them, can make it challenging to explain the significance of each document, which, in turn, reduces the likelihood that revelations will surface on the public agenda. Moreover, a weariness takes hold as stories are constantly written by the media and civil society, such that they blend together. While each Snowden document may reveal a new program, for the public the issue becomes less about any one program and instead about broader kinds of questions: Are the intelligence services accountable? Are the services overreaching? Are they behaving inappropriately? After one to three months, the public will have largely reached its conclusion about any given issue on the agenda. As a result, while the ongoing revelations may influence a minority of people who are attentive or sensitive to intelligence-related issues, the public agenda writ large will likely only shift following major new revelations with explosive discoveries that would challenge the public's conclusions concerning the intelligence services.

Beyond these basic conditions, at least two separate conditions can enhance the likelihood of successfully opposing proposed surveillance expansions. First, by revealing information or being prepared to exploit an explosive event, opponents can either create or (try to) control a focusing event. Governments often enjoy routine opportunities to introduce, debate, and pass legislation. Focusing events, either in the form of a minister's poor choice of words (i.e., breaking news) or reports and findings prepared by opponents, but not revealed, in advance of the introduction of legislation (i.e., *Access to Information* documents that are kept in reserve, or legal findings that are not disclosed until media attention is high) can provide opponents with a way of reframing surveillance-authorizing legislation as a problem in itself, instead of as a solution to a problem. Similarly, planning to release op-eds or engage in public action following the release of an explosive signals intelligence revelation can be an attempt to create, and use, a focusing event to the framers' own ends. Second, a diversified set of experts can enhance the likelihood that proposed surveillance power is opposed. A blend of activists, advocates, lawyers, scholars, and interested journalists are helpful in registering repeated critiques of lawful access powers, mustering

public support, and ensuring that editors or others media owners can publish a wide range of critical articles about the powers. This blend is especially important when analyzing highly technical or nuanced documents, such as those released by Edward Snowden, as few individuals will have a total understanding or awareness of public information pertaining to signals intelligence practices, law, or policy.

The presence of a diversified group of activists, advocates, lawyers, scholars, and journalists is also essential for continually highlighting and opposing the legitimization of surveillance activities as they (re)arise over the course of successive legislative sessions. In Canada, a group formed organically out of opposition to lawful access. Though its attention was swayed from lawful access through the course of C-13 as national security revelations linked to Edward Snowden's disclosures become public, the group as a whole was swayed; its membership did not fragment and attend to unrelated issues. And many of the actors of the group have played normal roles and assumed typical positions in their advocacy, which is the result of having worked together throughout the contests over lawful access. Some of this collaboration has been demonstrated in public coverage of Canada-related Snowden disclosures, with lawyers providing legal analysis of documents, technologists providing analyses of how the surveillance practices are designed and operated, policy analysts noting how the CSE's activities either fit into or seemingly run counter to the *National Defence Act* or *Charter* rights, and civil liberties groups launching challenges to the government's domestic surveillance practices.

Whereas opposition to lawful access revolved around demystifying and critiquing the legislation — to prevent the law from coming into being — opposition to signals intelligence practices involved ascertaining what activities were being conducted, how they were carried out, who they affected, and how the activities fit with publicly available legislation and policy documents. The opposition to signals intelligence activities had at least two goals: to understand the state of practices and to subsequently push back against practices that were seen as inappropriately intruding upon the rights of those affected. As of early 2015, there were few legislative victories beyond a handful of members of the Canadian Parliament and Senate critiquing existing practices, and it remained to be seen whether the courts or the legislature would (or could) operate as a way to effectively challenge

the CSE's practices. Nevertheless, the opposition that was mustered depended on previously established close working relationships born of critiquing domestic lawful access legislation and the experiences of how to work in concert with one another. The actual effectiveness of that opposition, however, remained to be seen.

Ultimately, for opponents of surveillance powers to successfully frame the issue according to their interests, a government must be responsive to competing agendas, not highly prioritize the surveillance authorizations amongst its broader legislative agenda, and public and media agendas must be receptive to, and capable of receiving, negative framings of surveillance. If these basic conditions are not met, then focusing events or effective uses of symbols or narratives on the parts of diversified expert opponents might be insufficient to dissuade strong governments from legislating expanded lawful access powers. And all of these efforts are even more challenging when opposing signals intelligence-related issues given the secrecy of the practices, the secret interpretations of law, and the challenge in maintaining media and public interest in the kind of technically and politically complicated processes that signals intelligence agencies are involved in.

The diversity of groups opposing state surveillance practices is perhaps most important when the groups are unsuccessful in framing a proposed surveillance authorization as inappropriate or unneeded. Efforts to prevent the passage of legislation or inhibit newly revealed signals intelligence operations can represent just the first step of a much longer campaign, as legal challenges against the newly authorized surveillance powers are mounted, as new political parties with different priorities enter office, or as new technologies that operate outside the expanded powers are created and deployed to counter government-authorized surveillance capabilities. Policy problems, solutions, and framings will continue to circulate even as court proceedings are ongoing, thus giving perpetual hope to opponents of government surveillance activities that their interpretations of these activities will eventually be taken up by either the courts or in one policy forum or another.

Notes

1. Andreas Busch, "Privacy, Technology, and Regulation: Why One Size is Unlikely to Fit All," in *The Social Dimensions of Privacy: Interdisciplinary*

Perspectives, eds. Beate Roessler & Dorota Mokrosinksa (Cambridge: Cambridge University Press, June 2015).

2. Chas Critcher, "Media, Government and Moral Panic: The Politics of Paedophilia in Britain 2000–1," (2002) 3:4 *Journalism Studies* 521 at 530.
3. Maxwell E. McCombs, *Setting the Agenda: The Mass Media and Public Opinion* (Cambridge: Polity Press, 2004) at 38.
4. Thomas A. Birkland, *After Disaster: Agenda Setting, Public Policy, and Focusing Events* (Washington, DC: Georgetown University Press, 2007) at 22.
5. Hans Mathias Kepplinger & Johanna Habermeier, "The Impact of Key Events on the Presentation of Reality," (1995) 10:3 *European Journal of Communication* 371 at 373 [emphasis in original].
6. Thomas A. Birkland, "The World Changed Today: Agenda-Setting and Policy Changes in the Wake of the September 11 Terrorist Attacks," (2004) 21:2 *Review of Policy Research* 179 at 180.
7. Jarol B. Manheim, "A Model of Agenda Dynamics," in *Communication Yearbook*, ed. Margaret L. McLaughlin (London: Sage, 1987) 499 at 510.
8. Hannah Murphy & Aynsley Kellow, "Forum Shopping Global Governance: Understanding States, Business and NGOs in Multiple Areas," (2013) 4:3 *Global Policy* 139–49; Mary Garvey Algero, "In Defence of Forum Shopping: A Realistic Look at Selecting a Venue," (1999) 78 *Nebraska Law Review* 79; Christopher Parsons, "The Politics of Deep Packet Inspection: What Drives Surveillance By Internet Service Providers?" PhD dissertation, University of Victoria, Victoria, 2013, 192–228.
9. Daphne Gilbert, Ian Kerr & Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers," (2006) 51:4 *Criminal Law Quarterly* 569 at 480.
10. Canada, Department of Justice, "Lawful Access – Consultation Document," (Ottawa: DOJ, 25 January 2002). For historical overview of successive legislative efforts, see also Philippa Lawson, *Moving towards a Surveillance Society: Proposals to Expand "Lawful Access" in Canada* (Vancouver: British Columbia, Civil Liberties Association, 2012); Kevin McArthur & Christopher Parsons, "Understanding the Lawful Access Decryption Requirement," *Social Sciences Research Network* (2012) (unpublished paper), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2148060>; Christopher Parsons, "Canadian Cyberbullying Legislation Threatens to Further Legitimize Malware Sales," *Technology, Thoughts, and Trinkets* (blog), 4 June 2014, <http://www.christopher-parsons.com/canadian-cyberbullying-legislation-threatens-to-further-legitimize-malware-sales/>.
11. Reg Whitaker, "The Curious Tale of the Dog That Hasn't Barked (Yet)," (2012) 10:3/4 *Surveillance & Society* 103 at 340.

12. Canada, Department of Justice, "Summary of Submissions to the Lawful Access Consultation," (Ottawa: DOJ, last modified 7 January 2015, <http://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html>.
13. Jesse Kline, "Vic Toews Draws Line on Lawful Access: You're with Us, or the Child Pornographers," National Post, 14 February 2012, <fullcomment.nationalpost.com/2012/02/14/vic-toews-draws-line-on-lawful-access-youre-with-us-or-the-child-pornographers/>.
14. Daniel Proussalidis, "Magnotta to Be Charged with Criminal Harassment of PM," *Toronto Sun*, 1 June 2012, <www.torontosun.com/2012/06/01/internet-snooping-bill-would-be-helpful-in-lin-case-toews>.
15. Tabatha Southey, "Bill C-13 Is about a Lot More than Cyberbullying," *Globe and Mail*, 6 December 2013, <www.theglobeandmail.com/globe-debate/columnists/maybe-one-day-revenge-porn-will-be-have-no-power/article15804000/>.
16. Michael Vonn, "How Will the Reduction in EU Privacy Affect Canadians' Right to Access Information?" (Lecture delivered at the Sunshine Summit, Victoria, BC, 27 September 2013) [unpublished]; see also Lisa Austin, "Getting Past Privacy? Surveillance, the Charter, and the Rule of Law" (2012) 27:3 *Canadian Journal of Law and Society* 381.
17. Canada, "Response to the Government of Canada's 'Lawful Access' Consultations," Office of the Privacy Commissioner of Canada, May 2005, <http://www.priv.gc.ca/information/research-recherche/sub/sub_la_050505_e.asp>; Jennifer Stoddart et al., "Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the Current 'Lawful Access' proposals," Office of the Privacy Commissioner of Canada, 9 March 2011, <http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.asp>; Privacy Commissioner of Canada, "Statement from the Privacy Commissioner of Canada regarding Bill C-13," Office of the Privacy Commissioner of Canada, 28 November 2013, <http://www.priv.gc.ca/media/nr-c/2013/s-d_131128_e.asp>.
18. Lindsey Pinto, "NDP Leader Responds to StopSpying.ca Campaign," 25 May 2012, *OpenMedia*, <openmedia.ca/blog/ndp-leader-responds-stopspyingca-campaign>.
19. Dominique Valiquet, "Telecommunications and Lawful Access: I. The Legislative Situation in Canada," (Canada: Library of Parliament, 21 February 2006), <http://www.parl.gc.ca/Content/LOP/ResearchPublications/prb0565-e.html>.
20. Nestor Arellano, "Small ISPs Foresee Cost Burden In 'Lawful Access' Bills," 27 June 2011, *ITBusiness*, <www.itbusiness.ca/news/small-isps-foresee-cost-burden-in-lawful-access-bills/16419>; Christopher Parsons, "Unpacking the Potential Costs of Bill C-30" (2012) 9:6 *Canadian Privacy Law Review* 57.

21. Nicholas Kyonka, "Telcos Object to Industry Department's 'Lawful Intercept' Proposal for 700 MHz Band," *Wire Report*, 9 July 2012, <www.thewirereport.ca/news/2012/07/09/telcos-object-to-industry-department's-'lawful-intercept'-proposal-for-700-mhz/25496>; Christopher Parsons, "Lawful Access is Dead; Long Live Lawful Intercept," *Technology, Thoughts, and Trinket*s (blog), 11 February 2013, <www.christopher-parsons.com/lawful-access-is-dead-long-live-lawful-intercept/>; Colin Freeze & Rita Trichur, "Wireless Firms Rejected Ottawa's Changes to Surveillance Rules over Cost Concerns," *Globe and Mail*, 16 September 2013, <www.theglobeandmail.com/technology/mobile/wireless-firms-reject-ottawas-changes-to-surveillance-rules-over-cost-concerns/article14363379/>.
22. Public Safety Canada, "Memorandum for the Minister: Proposed Consultation Strategy on Access to Customer Name and Address Information (For Decision)," (Canada: PSC, 11 July 2007) at 4.
23. *MITA* could be read as an attempt by the government of the day to appear "tough on crime" instead of constituting a genuine legislative attempt. For more, see "Liberals Try to Resuscitate Big Brother Plan for the Internet," *Ottawa Citizen*, 27 March 2007, <www.canada.com/ottawacitizen/news/business/story.html?id=b987660e-cf6d-432c-aafb-c39075caa972>.
24. "Harper Government Should Adopt Liberal Bill on Surveillance: MP," *CBC News*, March 29, 2007, <http://www.cbc.ca/m/touch/canada/story/1.635923>.
25. Public Safety and Emergency Preparedness Canada, "Legislation to Modernize Investigative Techniques Introduced Today," Government of Canada, 15 November 2005.
26. Lawson, *supra* note 10; David Christopher, "OpenMedia.ca Concerned 'Cyberbullying' Legislation Will Unnecessarily Erode the Privacy of Law-Abiding Canadians," 20 November 2013, *OpenMedia*, <openmedia.ca/news/openmediaca-concerned-%E2%80%9Ccyberbullying%E2%80%9D-legislation-will-unnecessarily-erode-privacy-law-abiding-canad>.
27. See Access To Information And Privacy document A-2012-00010, Public Safety Canada, pp.105–127/421.
28. Michael Geist, "Liberal MP Reintroduces Lawful Access as Private Members Bill," *Michael Geist* (blog), 2 February 2014, <www.michaelgeist.ca/content/view/1827/>.
29. Michael Geist, "Public Safety to Release Lawful Access Consultation," *Michael Geist* (blog), 13 September 2007, <www.michaelgeist.ca/content/view/2233/125/>.
30. Michael Geist, "Public Safety Canada Quietly Launches Lawful Access Consultation," *Michael Geist* (blog), 11 September 2007, <www.michaelgeist.ca/content/view/2228/99999/>.

31. Civil Liberties Groups Fear Erosion of Privacy Rights," *CanWest News Service*, 13 September 2007, <www.canada.com/nationalpost/news/story.html?id=378b169e-036d-4ea8-9aba-8f10d7a570d6&k=77186>; "Government Moving to Access Personal Info, Sparking Privacy Fears," *CBC News*, 12 September 2007, <www.cbc.ca/news/technology/government-moving-to-access-personal-info-sparking-privacy-fears-1.631075>.
32. "Warrant Needed to Pull Data on Internet Users: Day," *Ottawa Citizen*, 14 September 2007, <www.canada.com/ottawacitizen/news/story.html?id=af578ca9-0d7e-4785-b939-58364e4f5845>.
33. "Privacy Watchdog Reiterates Lawful Access Concerns," *CBC News*, 27 October 2011, <www.cbc.ca/news/technology/privacy-watchdog-reiterates-lawful-access-concerns-1.996304>.
34. Colin Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge, MA: MIT Press, 2008) at 96.
35. Sarah Schmidt, "Can You Spot the Difference on 'Lawful Access' Bill?," *Canada.com*, 15 February 2012, <http://o.canada.com/news/politics-and-the-nation/can-you-spot-the-difference-on-lawful-access-bill>.
36. "Online Surveillance Bill 'Will Put an Electronic Prisoner's Bracelet on Every Canadian'," *National Post*, 4 February 2012, <news.nationalpost.com/2012/02/14/online-surveillance-bill-will-put-electronic-prisoners-bracelet-on-every-canadian/>.
37. Laura Payton, "Toews Steps Back from Child Pornographers Comment," *CBC News*, 16 February 2012, <www.cbc.ca/news/politics/toews-steps-back-from-child-pornographers-comment-1.1127817>.
38. Laura Payton, "'Tell Vic Everything' Tweets Protest Online Surveillance," *CBC News*, 16 February 2012, <www.cbc.ca/news/politics/tell-vic-everything-tweets-protest-online-surveillance-1.1187721>.
39. "Stop Online Spying," *Open Media*, 2013, <https://openmedia.ca/StopSpying>.
40. "Don't let Harper read your e-mails," Liberal Party of Canada, 2013, <http://petition.liberal.ca/online-privacy-surveillance-lawful-access-bill-c30-liberal-amendment/>.
41. Steve Anderson, interview with the author, 2013.
42. Privacy Commissioners of Ontario, Alberta, British Columbia, "RE: Police Chiefs Speak out," *Information and Privacy Commissioner of Ontario* (first appeared in *Windsor Star*), 7 November 2012, <http://www.ipc.on.ca/english/About-Us/Whats-New/Whats-New-Summary/?id=263>.
43. Bennett, *supra* note 34 at 96.
44. Canadian Wireless Telecommunications Association (CWTA), "Re: Consultation on a Licensing Framework for Mobile Broadband Services (MBS) — 700 MHz Band," *Canadian Radio-television Telecommunications Commissioner*, 22 June 2012, <https://www.ic.gc.ca/eic/site/smt-gst.nsf/

vwapj/DGSO-002-12-comments-CWTA-submission.pdf/$FILE/DGSO-002-12-comments-CWTA-submission.pdf>; see also Parsons, *supra* note 21.

45. (CWTA), *supra* note 44.
46. See Access to Information and Privacy document A-2012-00457 released by Public Safety Canada, at 83–84.
47. *Ibid*., at 324
48. *Ibid*., at 30–31.
49. Colin Freeze & Rita Trichur, "Ottawa Sought Broader Access To Smartphone User Data, Records Show," *Globe and Mail*, 16 September 2013, <www.theglobeandmail.com/technology/mobile/ottawa-sought-broader-access-to-smartphone-user-data-records-show/article14343991/>.
50. Freeze & Trichur, *supra* note 21.
51. By this I mean that, while the 2012 *SGES* lacks the annotations found in previous iterations of the *Standards*, the wording of the *Standards* themselves has not changed. It remains possible that the annotations, which themselves explain how the *Standards* are to be implemented, may have changed.
52. Laura Payton, "Government Killing Online Surveillance Bill," *CBC News*, 11 February 2013, <www.cbc.ca/news/politics/government-killing-online-surveillance-bill-1.1336384>.
53. Southey, *supra* note 15.
54. Michael Geist, "Is C-13 Needed?: How Canadian Law Already Features Extensive Rules to Combat Cyberbullying," *Michael Geist* (blog), 13 January 2014, <www.michaelgeist.ca/content/view/7046/125/>.
55. Michael Geist, "The Privacy Threats in Bill C-13, Part One: Immunity for Personal Info Disclosures without a Warrant," *Michael Geist* (blog), 25 November 2013, <www.michaelgeist.ca/content/view/7006/125/>.
56. Canada, "Statement from the Privacy Commissioner of Canada regarding Bill C-13," Office of the Privacy Commissioner of Canada, 28 November 2013, <http://www.priv.gc.ca/media/nr-c/2013/s-d_131128_e.asp>.
57. Kathryn Blaze Carlson, "Bullying Victims' Families Split over Crime Bill," *Globe and Mail*, 13 May 2014, <http://www.theglobeandmail.com/news/politics/bullying-victims-families-split-over-crime-bill/article18653112/>; Evan Dyer, "Cyberbullying Bill Draws Fire from Diverse Mix of Critics," *CBC News*, 20 October 2014, <http://www.cbc.ca/news/politics/cyberbullying-bill-draws-fire-from-diverse-mix-of-critics-1.2803637>.
58. Colin Freeze, Christine Dobby & Josh Wingrove, "TekSavvy, Rogers Break Silence over Government Requests For Data," *Globe and Mail*, 5 June 2014, <http://www.theglobeandmail.com/technology/tech-news/

teksavvy-opens-books-on-government-data-requests/article18999107/>; David Paddon, "Telus Issues First 'Transparency' Report on Requests for Customer Information," *Canadian Press*, 18 September 2014, <http://www.thestar.com/business/2014/09/18/telus_issues_first_transparency_report_on_requests_for_customer_information.html>.

59. Ms. Borg (Terrebonne-Blainville), "Q-233," Notice Paper No. 36, Tuesday, 28 January 2014, <http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&Parl=41&Ses=2&DocId=6391359&File=11>.
60. Christopher Parsons, "Mapping the Canadian Government's Telecommunications Surveillance," *The Citizen Lab*, 27 March 2014, <https://citizenlab.org/2014/03/mapping-canadian-governments-telecommunications-surveillance/>.
61. Lawson, *supra* note 10.
62. *R. v. Spencer*, 2014, SCC 43.
63. *Corporation of the Canadian Civil Liberties Association et al. v. Canada (Attorney General)*, Court File No. CV-04-504139, Notice of Application, 13 May 2014, <http://ccla.org/wordpress/wp-content/uploads/2014/05/Notice-of-Application-re-PIPEDA-Issued.pdf>.
64. Jim Sensenbrenner, "How Obama Has Abused the Patriot Act," *LA Times*, 19 August 2013, <http://articles.latimes.com/2013/aug/19/opinion/la-oe-sensenbrenner-data-patriot-act-obama-20130819>.

Page left blank intentionally