Horizontal Accountability and Signals Intelligence: Lesson Drawing from Annual Electronic Surveillance Reports

By Christopher Parsons[*] and Adam Molnar[**]

Abstract:
This paper argues that Canada's foreign signals intelligence agency's public accountability reporting might be enhanced by drawing on lessons from existing statutory electronic surveillance reporting. Focusing exclusively on Canada's signals intelligence agency, the Communications Security Establishment (CSE), we first outline the relationships between accountability of government agencies to their respective Ministers and Members of Parliament, the role of transparency in enabling governmental accountability to the public, and the link between robust accountability regimes and democratic legitimacy of government action. Next, we feature a contemporary bulk data surveillance practice undertaken by Canada's signals intelligence agency and the deficiencies in how CSE's existing review body makes the Establishment's practices publicly accountable to Parliamentarians and the public alike. We then discuss how proposed changes to CSE oversight and review mechanisms will not clearly rectify the existing public accountability deficits. We conclude by proposing a principle-based framework towards a robust public accountability process that is linked to those underlying domestic and foreign statutory electronic surveillance reports.

Keywords: accountability, transparency, national security, signals intelligence, Canadian politics

Version: 1.0.2
Prepared for: Security Intelligence & Surveillance in the Big Data Age (University of Ottawa)

[*] Christopher Parsons is a Research Associate and Managing Director of the Telecommunications Transparency Project at the Citizen Lab, Munk School of Global Affairs at the University of Toronto. Corresponding Author: Christopher@Christopher-Parsons.com

[**] Adam Molnar is a Lecturer in Criminology at Deakin University (Australia) and is a member of the Alfred Deakin Institute of Citizenship and Globalisation.

> *One of my biggest takeaways from the past 16 months is that we need to be more transparent. And, if we're going to profess transparency, we need to produce transparency, wherever we can.*
> - James Clapper (2014, "Remarks as Delivered at the AFCEA/INSA National Security and Intelligence Summit)

The Communications Security Establishment (CSE) is Canada's foremost signals intelligence (SIGINT) agency. Historically it has collected foreign signals intelligence, provided security and defensive information technology services to the government of Canada and systems critical to the government of Canada, and assisted domestic federal law enforcement and security agencies (LESAs) (National Defence Act 1985, at ss. 273.64(1)(a)-(c)). The CSE's activities are guided in accordance with parliamentary legislation and by the Minister of National Defense vis-a-vis Ministerial Authorizations and Directives. The former can authorize the CSE to engage in practices that would otherwise violate Canadian law without criminal liability and the latter principally establish conditions or limitations on the kinds of lawful activities the CSE may conduct (OCSEC 2017). All of the CSE's activities are subject to review by the Office of the Communications Security Establishment Commissioner (OCSEC).

The CSE's activities are routinely concealed from the public eye, with legislators and the public principally reliant on the principles of Ministerial responsibility, OCSEC reviews, rare unauthorized discloses for classified activities, and (marginal) judicial oversight to ensure that the CSE's activities comport with law. This present system of accountability that governs CSE activities has often been questioned as insufficient in the media and amongst some analysts (Robinson 2015, Deibert 2015, Westin 2014). And while legislation that was tabled in 2017 in the Canadian Parliament may significantly restructure this historical relationship between the CSE, their Minister, and the OCSEC, and thus how the CSE is rendered accountable to its Minister and the public alike, we argue that both the current and proposed review and oversight of the CSE are insufficient to provide public accountability. We address these shortcomings by offering principle-based suggestions for how to facilitate such accountability.

In Section One, we unpack the concepts of accountability, transparency, and democratic legitimacy as linked to lawful government surveillance activities. In Section Two, we describe some of the CSE's more controversial activities to reveal deficiencies in how CSE's activities have historically been framed through legislation and publicly reviewed by their Commissioner. The combined effect of this legislative framing and reviews has been to undermine assurances that CSE's activities could be democratically legitimated. In Section Three we briefly argue that currently tabled legislative reforms that would affect the CSE's accountability structures would be

insufficient to rectify the public accountability deficits facing the CSE. We conclude in Section Four by sketching a principle-based framework that could ensure that the CSE's activities are both made accountable to their Minister and select Parliamentarians, as well as transparent as possible to Canadians and, as a result, democratically legitimated.

Section 1: Conceptual Terminology

When organizations act transparently they collate and present data to those outside the organization (Bushman et al., 2004, p. 207; Eigffinger & Geraats, 2006). This disclosure of information can sometimes present data that is useful for the public (Cotterrell, 1999). Often, organizations act transparently in situations when they are compelled to present information in a delimited format (Fung et al, 2007) or through their own methodologies to collate and disclose information (Fung et al, 2007; Parsons, 2017). In either case, organizations that 'behave transparently' may be attempting to engender greater trust in their practices (Wayland, Armengol, & Johnson, 2012). On this basis, scholars are advised to pay "careful attention to the human and material operations that go into the production of transparency" (Hansen et al., 2015) because the revelatory character of transparency practices may be overemphasized absent critique.

One way that governments, in particular, demonstrate transparency is through the release of statutorily required reports. Electronic surveillance reports are an attempt to address social inequity in the social contract between governments and their citizens. By disclosing the regularity at which government surveillance practices occur, the disproportionate degree of power over the state into the private lives of citizens is thought to be safeguarded. In contrast, no requirement to disclose these activities, or a failure to release such reports, can hinder legislatures and the citizenry from holding the government to account (Korff, Wagner, Powles, Avila, & Buermeyer, 2017). Without information about secretive government practices, the public, Parliamentarians, and other stakeholders cannot evaluate whether government agencies are appropriately using their exceptional powers (Parsons & Israel 2016), and in ways that cohere with public interpretations and expectations of how the law ought to legitimize such activities (Molnar, Parsons, & Zouave, 2017).

Transparency in government activities is needed to ensure that civic agencies are held accountable to their Minister, the Parliament, and the public more broadly. A system of accountability exists "when there is a relationship where an individual or institution, and the performance of tasks of functions by that individual or institution, are subject to another's oversight, direction or request that the individual or institution provide information of justification for its actions" (Pelizzo and Stapenhurst, 2013, p. 2). In effect,

an institution must be obligated to answer questions and there must also be means to enforce consequences should the institution refuse, or fail, to provide satisfactory responses (Schedler 1999; Blick and Hedger 2008; Mulgan 1997; Anderson 2009). In the context of a parliamentary democracy, such as Canada, accountability can manifest vis-a-vis Ministerial responsibility or other formalized methods that empower the legislature to scrutinize an agency's practices (Smith 2017; Stone 1995). However, accountability also exists through more informal measures, such as when non-governmental stakeholders hold government to account based on information tabled by government Ministers or the government's independent officers (Malena, Forster, and Singh 2004).

There are several ways to understand accountability (see as examples: Mulgan 2000, Deleon 1998, Sinclair 1995, Corbett 1996, March and Olsen 1995). In this paper, we focus exclusively on informal, or horizontal, modes of accountability between government and non-government stakeholders. This mode can be contrasted with vertical accountability, which often involves Ministers being formally compelled to account for their departments activities to their respective legislatures (Smith 2017; Stone 1995). Whereas Ministers are obligated to explain their departments' activities and policies to their legislature, and the legislature is empowered to receive explanation and justification, and subsequently issue sanctions as appropriate (Edwards 1980; Savoie 2003), the same is not true with regards to the government's relationship with external stakeholders. Horizontal accountability institutes accountability through civil engagement, as a way to complement and enhance government accountability processes (Malena, Forster, and Singh 2004). External stakeholders, however, cannot necessarily impose sanctions and governments are not always required to provide an account to these stakeholders (Bovens 2007). In place of formal legal tools, moral suasion is routinely used to sanction government behaviours. And while the disclosure of ethical impropriety and accompanying use of moral suasion may be amplified by the media, it is rarely premised on stakeholders having formal powers to compel the government to provide an account or modify its behaviours (Malena, Forster, and Singh 2004; McCombs 2014).

The practice of holding governments to account is intended to control government conduct. Citizens can exert control through the ballot box (Bovens 2007) as well as outside of electoral periods. Stakeholders engaged in horizontal accountability can work to identify problems so that legislators, or the government itself, can take up and attempt to solve challenging issues (Roberts 2007). Moreover, through a proactive civil culture that proposes solutions to problems, government and legislators may realize previously unconsidered ways to correct them. External stakeholders can also testify or present information to government committees or members of the legislature. But for

any of these means to exercise horizontal accountability to work, external stakeholders must have access to government information, a capacity to take on the work of ingesting and processing the information in question, and recognize that the state is capable, willing, and competent to receive external actors' concerns and the potential ability to act on them (Malena, Forster, and Singh 2004). Absent information provided by government, citizens may be inhibited from participating in political processes; such secrecy "compels the public to defer to the judgement of a narrow elite" (Roberts 2007, 317).

By remaining open to external stakeholder analysis, critique, and problem solving a government combats cynicism or doubts that it is not 'of the people, for the people'. An inability to respond to civil society interests fosters cynicism and doubts about whether legislators can, or desire to, represent the citizenry. While most citizens may not be actively involved in holding their government to account, broader perceptions of accountability may be shaped by the government's receptiveness to civil society interventions (Scholte 2002; Fisher 1998). If the electorate fails to see its representatives respond on policy issues raised by stakeholders, they may lose faith in legislators, and by extension, in the representative democratic process of lawmaking itself (Habermas, 1998a, 1998b; Parsons 2015). Even if a government and its departments act based on laws passed within a legislative assembly, without adequate horizontal accountability, laws may be seen as severed from the legitimizing power of the citizenry itself. Such disconnection threatens to transform a democratic process bound through rule of law into a narrow and disconnected process that might be better understood as rule-with law (Bowling and Sheptycki 2014; Molnar, Parsons, and Zouave 2017). Severing 'lawful activities' from democratic legitimation processes have been recognized as a core challenge that the second generation of intelligence oversight must overcome. Whereas in the past, such oversight and review was concerned with detecting and preventing abuse and mischief, the second generation must reconcile economic, diplomatic, and strategic goals as well as secure the "consent of the governed" where public concerns are linked with the need for secrecy (Goldman & Rascoff 2016; see also: CSIS 2015).

Section 2: Making the Past Clear?

The CSE was formally established as part of the National Defense Act (NDA 1985), though its origin dates back to the end the Second World War where it secretly existed in different government departments (Robinson 2000). The NDA imposed three mandates on the CSE: mandate A, to "acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence"; mandate B, to "provide advice, guidance and services to help ensure the protection of electronic

information and of information infrastructures of importance to the Government of Canada"; and mandate C, to "provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties" (National Defence Act 1985, at ss. 273.64(1)(a)-(c)). The breadth of these mandates only became truly apparent following Edward Snowden's disclosure of classified national security documents to journalists who subsequently selectively published from what they were given.

One of the most prominent Canadian-focused Snowden disclosures were about a program covernamed CASCADE. CASCADE was operated on non-government of Canada networks and designed to analyze network traffic. The analysis involved discovering and tracking targets, as well as isolating content or metadata from traffic exposed to the network probes (CSE Undated). Within the CASCADE program were a series of differently-classified and covernamed network sensors. Some could capture metadata and content alike (EONBLUE and INDUCTION) whereas others could solely collect and analyze metadata (THIRD-EYE and CRUCIBLE) (CSE 2011). All of these sensors relied on deep packet inspection technology, which enables operators to analyze the metadata and contents of unencrypted communications and take actions on it, such as blocking certain traffic or modifying other traffic (CSE Undated, Parsons 2008).

INDUCTION operated at "SSO sites", or within the premises of private Canadian organizations which had consented to CSE's activities. CRUCIBLE sensors, similar to INDUCTION sensors, were located in the pathways of networks that were designated 'systems of importance' to Canada (CSE 2011). Such systems might belong to defense contractors, extractive resource companies, banks, or equivalent organizations whose compromise could detrimentally affect the governance of Canada. These sensors could also collect the metadata of communications that Canadians, and persons communicating with Canadians, were engaged in, as well as the metadata of devices which transmitted information into or out of Canada. Other aspects of CASCADE involved monitoring satellite communications as well as microwave towers that transmitted data (CSE 2011).

The purpose of CASCADE, when combined with an equivalent sensor network designed to protect the Government of Canada's own networks (covernamed PHOTONIC PRISM (CSE 2010) and which was expected to be replaced by EONBLUE (CSE 2011)), was to use the entirety of the global information infrastructure as a means of defense. By tracking threat actors, and their activities, the CSE intended to "affect changes at the CORE of the Internet on detection" in collaboration with its Five Eyes partners. Such changes included modifying traffic routes, silently discarding malicious

traffic, or inserting payloads into communications traffic to disrupt adversaries (CSE Undated). To achieve these ends, CASCADE would, in essence, be situated to grant fulsome awareness of domestic and foreign Internet activity throughout the world. The most controversial aspects of this program in Canada were principally linked to the extensive surveillance of Canadian-source, Canadian-bound, and Canadian-domestic traffic, as well as the CSE's efforts to work alongside private partners to conduct this global surveillance activity.

Fuzzy Mandates, Clarified?

The different mandates that the CSE operates under authorize a broad spectrum of activities, including: network discovery, exploitation, and attack, defensive cyber operations, the creation of information profiles useful for other agencies that engage in physical operations, as well as other activities intended to further or advance the missions of other government agencies (Deibert 2015). The program discussed, above, reveals how seemingly restrictive mandates can be interpreted as authorizing mass surveillance practices in excess of imagined restrictions.

The CASCADE program goes beyond the concept of erecting a network perimeter and defending it in depth by envisioning that the entirely of the domestic and international Internet be monitored so that the CSE can track all data emissions which might be harmful to Canadian interests. If Mandate B was principally considered to be instructing the CSE to shield certain systems, the Snowden documents revealed that CSE took shielding domestic institutions to mean engaging in global mass surveillance as a prerequisite for such defensive policies. While monitoring data traffic internationally arguably falls under Mandate A, the identification of domestic networks of interest and subsequent generation of domestic content and metadata from these networks runs counter to Canadians' perceptions that the CSE was not authorized to routinely monitor Canadians' activities (Westin, Greenwald, and Gallagher 2014). Indeed, in internal slides the CSE recognizes that providing 'defense' using CASCADE engages all three of their mandates: A, B, and C (CSE Undated).

Though the CSE is formally prohibited from deliberately collecting the personal communications content of Canadians, or of persons residing in Canada, the agency operates with a Ministerial Authorization that permits the agency to collect such data incidentally in the course of its operations. That is to say: CSE cannot direct its surveillance apparatus in a deliberate way towards specific or named Canadians or

Canadian targets unless it is providing assistance to a foreign agency under warrant.[†] But these restrictions are not interpreted by the Canadian government nor the OCSEC to preclude the CSE from monitoring all metadata emanations from persons within Canada (CTV 2014, OCSEC 2017; see also: Forcese 2014) even though the Establishment, its Minister, and its review body know that the CSE has the capability to re-identify the persons to whom the emanations are associated with. The OCSEC's conclusion that the CSE behaved lawfully in the collection of metadata pertaining to Canadians' communications and devices was unsurprising: independent analysts have found that it is almost impossible for any activity conducted by the CSE to be found unlawful given the nature of the OCSEC's role and interpretations of national security law (Robinson 2015).

In 2017, the Government of Canada introduced Bill C-59 which, among other things, was designed to clarify the CSE's mandate while simultaneously updating the control and review structure for Canada's intelligence agencies. Based on the Snowden revelations, it was apparent that the CSE was involved in a broader range of activities than many thought was already likely given the scope and perceived capabilities of the Establishment. While C-59 may retroactively authorise these already existing activities, it has made more explicit the expansive range of the CSE's activities, which include: the collection of foreign intelligence through the global information infrastructure; engaging in cybersecurity and information assurance; conducting defensive operations to broadly protect federal institutions' systems and those deemed of importance to Canada; performing active cyber operations that may involve degrading, disrupting, influencing, responding to or interfering with "the capabilities, intentions or activities" of non-Canadian parties; and providing technical and operational assistance to LESAs, the Canadian Forces, and the department of National Defense (C-59, Part 3 17-21). There are provisions within the CSE Act which also permits the CSE to collect information from any public source (C-59, Part 3 24(1)(a)), including perhaps grey market information brokers, as well as interfere with non-democratic foreign elections (C-59, Part 3 33(1)(b)), amongst other controversial measures.

The program that we have examined in this paper can be situated within this expanded mandate. CASCADE could operate simultaneously under the collection of foreign intelligence, cybersecurity and information assurance, as well as (potentially) assistance mandates. When viewed through each of these mandate areas, the CSE is permitted to acquire information as required, provide services to different government and non-government organizations that are meant to guarantee the respective organizations'

[†] Based on discussions between the authors and senior CSE staff, we understand that in such warranted cases, information is cordoned off from CSE's more general repositories and thus inaccessible to many, if not all, CSE staff and operations.

digital security, and use collected information as appropriate to assist domestic LESAs or foreign-operating Canadian Forces to act on parties threatening Canadian organizations' digital systems. If it obtains authorization, activities in Canada could extend to active defensive operations. Furthermore, C-59 explicitly authorizes the CSE to infiltrate any part of the global information infrastructure for the purposes of collecting information that would provide foreign intelligence. This includes the types of attacks being launched towards Canadian networks or systems of interest, and also permits private companies to cooperate with the CSE and, as such, operate as SSOs. Whereas the CSE's current legislation does not make explicitly explain the conditions under which it can engage with private organizations (as envisioned under the CASCADE program), the cybersecurity authorizations for non-federal infrastructures under Bill C-59 establishes the legislative framework for such cooperation. Notably, C-59 also includes emergency provisions for access to private organizations' infrastructure. These provisions might let the CSE to gain permission from either the operator of infrastructure, such as a party that is running software on, say, computer servers in a shared computing facility or, alternately, from the party that owns the servers and which leases them to the software-running party (C-59, Part 3 41(4)). This can occur without having to get the activity approved by anyone besides the CSE's minister. Such access might be needed, in some cases, to establish, expand, or re-establish the defensive perimeter envisioned as part of the CASCADE program.

Beyond providing a broader range of activities that the CSE might engage in, Bill C-59 also re-envisions how the CSE's activities are authorized, controlled, and reviewed. Ministers will continue to issue authorizations and directives that guide and delimit the types of activities that the CSE can engage in, with the Minister of Foreign Affairs generally being consulted prior to engaging in defensive cyber operations or active offensive cyber operations. The Intelligence Commissioner, a new control-type body that would be created as part of C-59, would be typically responsible for (amongst other things) approving foreign intelligence authorizations and cyber security authorizations, and also must be notified of (and approve) significant amendments or repeals of these kinds of authorizations.[‡] The Intelligence Commissioner is also expected to provide annual reports to the Minister. The CSE's activities would be subject to review by the National Security Intelligence Review Agency (NSIRA), and thus assume responsibilities for the CSE's reporting paralleling those held by the OCSEC. Neither the NSIRA nor any other body, including a committee of Parliamentarians which will report principally to the Prime Minister of Canada, is required to evaluate whether or not the activities of the CSE are normatively appropriate and that, even if they're 'lawful', focus extensively on whether they might still unnecessarily infringe upon Canadians' civil

[‡] The tabled bill does include a caveat: the Intelligence Commissions is not required to first approve emergency authorizations (C-59, Part 3 42 (2))

liberties. In the United States, the Privacy and Civil Liberties Oversight Board (PCLOB) provides this kind of external oversight of activities undertaken by the National Security Agency and produces classified reports for the government as well as reports which are accessible to the public.

While Bill C-59 requires both the CSE and NSIRA to produce annual reports, in the case of the NSIRA, its reports must include information about the CSE's compliance with law, ministerial authorizations, as well as the reasonableness and necessity of how the CSE has used its powers. It does not, however, require *or* authorize the NSIRA to produce annual reports similar to those produced about the United States' National Security Agency. These reports include statistics on the numbers of Americans targeted by the National Security Agency under FISA Title I and Title III warrants and the proportion of persons targeted who are non-US vs US persons, estimates of the number of non-US targets affected by Section 702 surveillance orders, the number of search terms that are used to query the Section 702 database that concern a known US person and aim to retrieve the unminimized contents of their communications, as well as the number of Section 702-based reports which contain American persons' identity information, amongst other statistics (see as example: ODNI 2017).

Section 3: The Performance of Legislative Legitimacy and Accountability

Bill C-59 is designed, in part, to reform how the CSE is controlled and reviewed, and Bill C-22 established a committee of parliamentarians to evaluate some of the CSE's activities and report on them to the Prime Minister's Office. Though judicial and other forms of evaluating the lawfulness of the CSE's activities are important, they are limited in notable ways. As Roach (2016) discusses "...even at its heroic best, judicial oversight will focus on issues of legality and propriety, not efficacy and effectiveness. Intelligence agencies will also have incentives -- and often the ability -- to take measures that avoid or limit any inconvenient judicial oversight." (181). Similarly, while the NSIRA is designed to limit the CSE and its partner agencies from avoiding or limiting review, members of the Canadian Intelligence Community have historically been willing to mislead judges and downplay questionable rationales of action to their reviewers (X (Re) 2009, X (Re) 2016). Furthermore, the very *structure* of accountability raises some critical problems when it comes to roles played by legislators. For instance, "[g]iving legislators access to secret information but no mechanism for revealing their concerns may only allow the government to claim legitimacy for illegal and improper conduct … Rather than relying on its members, much of the legitimacy of a legislative committee might come from constructive engagement with civil society." (Roach 2016, 187-88).

Parliamentarians, under Bill C-22, will be restricted in what they can examine, what they can report publicly, and who they can appoint as their chair and members (Guertin 2016, Newark 2016). So, while it is possible that the new control and review structures will improve accountability internal to formal government practices, nothing in Bill C-59 or the previously passed Bill C-22 necessarily establish enhanced *public* reporting of the CSE's activities and, as such, do not actively promote horizontal accountability of the CSE's activities.

Actively promoting horizontal accountability is vitally important to restore public trust in the CSE. Per Goldman and Rascoff (2016) trust "is, perhaps, the single most important determinant of how intelligence agencies will fare in liberal democracies." Goldman (2016) separately argues that "[t]he [Snowden] leaks really, then, revealed" a lack of social agreement about the proper contours of the rules "including about whether current interpretations of key constitutional provisions are consistent with society's expectations, rather than about significant illegal behaviour. Debates also revolved around policy choices by the [Intelligence Community] in areas where there is no direct legal authorization, such as whether the [National Security Agency] should stockpile zero-day exploits, or whether it should monitor communications of lawful foreign intelligence targets such as a foreign leader" (219). To promote horizontal accountability and restore the trust deficit between the population and the CSE's lawful activities, the government might amend C-59 or table new legislation that specifies certain statistical and narrative accounts of the CSE's activities, as well as establish an independent review body responsible for evaluating the proportionality of the CSE's activities.

Any efforts to ensure the CSE is subject to horizontal accountability could include the following modes of transparency:

- ***Legal transparency***: Decisions that are issued by the Federal Court should be made public and minimally redacted to assist external legal experts and scholars in understanding the development and shaping of law. As discussed by Renon (2016), "[m]aking the overarching legal framework of surveillance programs more visible and participatory may make these programs more resilient … the fundamental legal framework of intelligence programs belongs in the light" (135).[§]
- ***Statistical transparency***: The Office of the Director of National Intelligence in the United States voluntarily produces statistical reports concerning the National Security Agency's (NSA) annual operations. While statistics may leave much to be desired, they show that information concerning the annual activities of the

[§] Though beyond the scope of this argument, such proceedings could also include special advocates as much as possible to avoid *ex-parte* hearings that might lead to legal interpretations that unduly impact the civil liberties of those affected by the CSE's surveillance operations.

NSA can be disclosed without undue harm to national security. Reported information could also disclose the regularity at which the CSE provides assistance to domestic LESAs to assuage concerns that the CSE is routinely directing its activities towards Canadians or persons in Canada. A form of this reporting has been undertaken in Canada since the 1970s, and involves the federal and provincial governments of Canada issuing annual electronic surveillance reports which detail the regularity and efficacy of provincial and federal agencies' surveillance activities. To date, there is no evidence that such statistical transparency has negatively affected ongoing or concluded domestic LESA investigations.

- ***Narrative transparency:*** Legal or statistical transparency should be accompanied with narratives that help to clarify the rationales for the actions undertaken by the CSE. Such narratives should provide some information about the specific, annual, activities of the Establishment and not merely refer to authorizing legislation under which the CSE operates; though recent annual electronic surveillance reports in Canada generally fail to provide a useful narrative example to follow, federal reports pre-dating the mid-1990s that explain the situations associated with such surveillance may be a useful starting point for what such narrative explanations might include. Similarly, the narratives associated with the Office of the Director of National Intelligence's annual statistical reports indicate possible ways to explain how laws are interpreted and acted upon.
- ***Proportionality transparency:*** though the review structures under C-59 are expected to evaluate whether CSE's activities are reasonable or necessary for the CSE to exercise its powers (see: C-59, Part I 3(a) as well as Part II 13-21), review and control bodies are not expected to focus on whether the CSE's activities are proportionate to the impacts on civil liberties that result from those activities. The Minister is required to take the proportionality of a measure into consideration before issuing a Ministerial authorization, but this is an internal to government process (See: C-59, Part III 35(1)). An external civil liberties board, such as the PCLOB in the United States, could report on whether the specific activities undertaken by the CSE are reasonable and proportionate when viewed against their intrusion into citizens' and foreigners' private lives alike.

Three of these measures of transparency are born from accountability reporting the provincial and federal governments of Canada already conduct in their annual electronic surveillance reports. Such reports clarify the laws which authorize such surveillance, regularity at which such surveillance is conducted and its broad impacts, and they are supposed to provide some narrative explanation of those reports. The fourth measure we propose, focused on proportionality transparency, draws from measures established

by Canada's close allies. Admittedly the proposals we make extend beyond what the current annual electronic surveillance report include -- these current reports do not, as an example, include discussions or decisions linked to secret caselaw associated with wiretapping or other live forms of surveillance -- but importantly our proposals are not a radical adoption of entirely novel forms of government transparency and accountability.

Promoting transparency of government intelligence operations would result in important gains for horizontal accountability. Stakeholders could play a role in providing critical insights and analyses to parliamentary committees, legislatures, and regulatory bodies that routinely experience resource shortages or lack appropriate technical expertise. These stakeholders, who are often area experts, could play an important role by representing their communities' interests in debating the often thorny issues of secretive government surveillance activities that historically have 'touched' the information of far more Canadians and residents and visitors of Canada than previously suspected.

In general, emboldening horizontal accountability through meaningful public disclosure can inform the broader democratic process in an area of governance that is well known for its capacity to engender distrust and skepticism amongst the citizenry. Elsewhere, we've noted how even when legislation might exist to authorize a particular secret activity, information asymmetries between government lawyers and the public mean that the lawfulness of an activity may lack legitimation given the disconnect between legislation, law, and practice. In effect, by becoming more transparent in secret operations and, as such, better enabling horizontal accountability processes the lawful activities which are undertaken may be subject not *just* to critique, but also to approval of how a measure is authorized and the policies to safeguard against misconduct, overbreadth, or civil liberties infringements.

Conclusion

Walsh and Miller (2016) have argued that, "[t]he Snowden leaks now provide the opportunity for 'Five Eyes' governments to do a root and branch review of current organizational, ministerial, parliamentary and other standing oversight bodies to ensure they remain fit for purpose" (2016, p. 365-366). Goldman has separately insisted that "although the institutions designed to ensure compliance work well, these same institutions have difficulty with a broader role" (Goldman 2016, p. 220). We agree with these points of argument, and argue ourselves that a review of the Intelligence Community and its transparency and accountability structures must also consider how to empower external to government stakeholders to better engage in horizontal accountability. Indeed, in an environment that is characterised by rapid technological innovation, extensive legal ambiguities, and associated tensions with traditional liberal

democratic principles, horizontal accountability is an essential component for meaningful regulation.

In this article we have argued that horizontal accountability can help to legitimize secretive government activities which are authorized by legislation. We proposed four separate measures, focused around legal, statistical, narrative, and proportionality, to enhance the information available to external-to-government stakeholders. This information could then be taken up and used to understand and critique some activities, while also meaning that parties external to government could identify and propose solutions to thorny legal issues, could better explain the protections and safeguards established to protect civil liberties and human rights, and ensure that the stakeholders they represent are better informed about the actual, versus hypothetical or hyperbolic, issues linked to government surveillance activities.

A continuation of the status quo, where citizens are kept in the dark concerning the activities and laws which authorize secret intelligence activities, “undermines the capacity of citizens to determine whether a new balance of security concerns and basic rights has been struck” (Roberts 2007, 320). The status quo also threatens to magnify the already disturbing gap between legislation as it is written, as it is interpreted by Department of Justice and other government national security lawyers, and as it is acted upon by Communications Security Establishment staff. This gap fundamentally threatens the legitimacy, if not the lawfulness, of the CSE’s activities. Only once citizens, often facilitated through academic and civil society actors, can know what is being done in their name, why, and how those measures are linked to the activities authorized by their legislators can the gap be bridged. As Canada undertakes national security consultations and engages in legislative action, the time to start bridging the gap is now.

Acknowledgements

The authors would like to thank the participants of a national security roundtable that was held at the 2017 Annual Citizen Lab Summer Institute for their insights concerning the CSE Act and other relevant aspects of Bill C-59. They would also like to thank members of the CSE for providing numerous briefings about different aspects of the CSE’s mandate, challenges it seeks to overcome, and how Bill C-59 might affect the Establishment’s practices.

Declarations of Conflicting Interests

The authors declare no potential conflicts of interest with rest to the research, authorship, and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: the John D. and Catherine T. MacArthur Foundation.

References

Anderson, Jonathan. 2009. “Illusions of Accountability.” Administrative Theory & Praxis 31 (3): 322-39.

Blick, Andrew, and Edward Hedger. 2008. “Literature REview of FActors Contributing to Commonwealth Public Accounts Committees Effectively Holding Government to Account for the Use of Public Resources.” National Audit Office, Overseas Development Institute.

Bovens, Mark. 2007. “Analyzing and Assessing Accountability: A Conceptual Framework.” European Law Journal 13 (4): 447-68.

Bowling, B. and Sheptycki, J., 2015. “Global policing and transnational rule with law.” Transnational Legal Theory, *6* (1):141-173.

Bushman, R., Piotroski, J., and Smith, A. 2004. “What determines corporate social transparency?” Journal of Accounting Research 42: 207-252.

Communications Security Establishment (CSE). Undated. CSEC Cyber Threat Capabilities: SIGINT and ITS: an end-to-end approach. Government of Canada. Available at: https://christopher-parsons.com/Main/wp-content/uploads/2015/03/doc-6-cyber-threat-capabilities-2.pdf.

Communications Security Establishment. 2010. Cyber Network Defence R&D Activities. Government of Canada. Available at: https://christopher-parsons.com/writings/cse-summaries/#cse-cyber-threat-capabilities.

Communications Security Establishment (CSE). 2011. CASCADE: Joint Cyber Sensor Architecture. Government of Canada. Available at: https://christopher-parsons.com/writings/cse-summaries/#cse-cascade-joint.

Corbett, D. 1996. Australian Public Sector Accountability. Second. Sydney: Allen and Unwin.

Cotterrell, R. 1999. “Transparency, mass media, ideology and community.” Journal for Cultural Research 3: 414-26.

Centre for Strategic & International Studies (CSIS). 2015. "Intelligence Reform in a Post Snowden World." CSIS. Available at: https://www.csis.org/events/intelligence-reform-post-snowden-world-0.

CTV. 2014. “Defence minister insists spy agency did not track Canadian travellers.” CTV. Available at: http://www.ctvnews.ca/canada/defence-minister-insists-spy-agency-did-not-track-canadian-travellers-1.1664333.

Deibert, Ronald. 2015. “Who Knows What Evils Lurk in the Shadows?” Open Canada. Available at: https://www.opencanada.org/features/c-51-who-knows-what-evils-lurk-in-the-shadows/.

Deleon, Linda. 1998. “Accountability In A ‘Reinvented’ Government.” Public Administration 76 (3): 539-58.

Edwards, J. LI. J. 1980. "Ministerial Responsibility for National Security as it relates to the Offices of the Prime Minister, Attorney General and Solicitor General of Canada," for The Commissioner of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. Ministry of Supply and Services Canada, Ottawa.

Eigffinger, S. C. W., and Geraats,P. M. 2006. *Government transparency: Impacts and unintended consequences*. New York, NY: Palgrave Macmillan.

Fisher, J. 1998. *Non governments: NGOs and the political development of the Third World*. West Hartford: Kumarian Press.

Forcese, Craig. 2014. “Faith-based Accountability: Metadata and CSEC Review,” National Security Law: Canadian Practice in Comparative Perspective. Available at: http://craigforcese.squarespace.com/national-security-law-blog/2014/2/13/faith-based-accountability-metadata-and-csec-review.html.

Fung, A., Graham, M., and Weil, D. 2007. *Full disclosure: The perils and promise of transparency*. New York: Cambridge University Press.

Goodman, Zachary K. 2016. “The Emergence of Intelligence Governance.” In *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, Zachary K. Goldman and Samuel J. Rascoff (ed). New York: Oxford University Press.

Goldman, Zachary K., and Rascoff, Samuel J. 2016. "The New Intelligence Oversight." In *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, Zachary K. Goldman and Samuel J. Rascoff (ed). New York: Oxford University Press.

Guertin, Anne Dagenais. 2016. “Our Analysis of C-22: An Inadequate and Worrisome Bill,” International Civil Liberties Monitoring Group. Available at: http://iclmg.ca/our-analysis-of-c-22-an-inadequate-and-worrisome-bill/.

Habermas, Jürgen. 1998a. “On the Internal Relation between the Rule of Law and Democracy.” In *The Inclusion of the Other: Studies in Political Theory*, 253-64. Cambridge, Mass.: The MIT Press.

Habermas, Jürgen. 1998b. “Three Normative Models of Democracy.” In *The Inclusion of the Other: Studies in Political Theory*, 253-64. Cambridge, Mass.: The MIT Press.

Hansen, H.K., Christensen, L.T., and Flyverbom, M. 2015. “Introduction: Logics of transparency in late modernity: Paradoxes, mediation and governance.” *European Journal of Social Theory* 18: 117-131.

Korff, D., Wagner, B., Powles, J., Avila, R., and Buermeyer, U. 2017. “Boundaries of law: Exploring transparency, accountability, and oversight of government surveillance regimes.” Social Science Research Network. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894490.

McCombs, Maxwell. 2014. *Setting the Agenda: Mass Media and Public Opinion*. John Wiley & Sons.

Malena, Carmen; Forster, Reigner; and Singh, Janmejay. 2004. “Social Accountability: An Introduction to the Concept and Emerging Practice.” World Bank.

March, J. G., and J.P. Olsen. 1995. Democratic Governance. New York: Free Press.

Molnar, Adam; Parsons, Christopher; Zoauve, Erik. (2017). “Computer network operations and ‘rule-with-law’ in Australia.” Internet Policy Review 6(1).

Mulgan, Richard. 1997. “The Process of Public Accountability.” Australian Journal of Public Accountability 56 (1): 26-36.

Mulgan, Richard. 2000. “‘Accountability’: An Ever-Expanding Concept?” Public Administration 78(3): 555-73.

Newark, Scott. 2016. “Ensuring Independence for the Parliamentary National Security Committee: A Review of Bill C-22,” Macdonald-Laurier Institute. Available at: http://www.macdonaldlaurier.ca/files/pdf/MLICommentaryNewark11-16-webV2.pdf.

Office of the Communications Security Establishment Commissioner. 2017. “Frequently Asked Questions,” Office of the Communications Security Establishment Commissioner, https://www.ocsec-bccst.gc.ca/s56/eng/frequently-asked-questions.

Office of the Director of National Intelligence (ODNI). 2017. “Statistical Transparency Report Regarding Use Of National Security Authorities For Calendar Year 2016,” United States Government. Available at: https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf.

Parsons, Christopher. 2008. “Working Paper: Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials.” The New Transparency Projects. Available at: http://www.sscqueens.org/sites/default/files/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf.

Parsons, Christopher. 2015. “Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance.” Media and Communication 3(3).

Parsons, Christopher. 2017. “The (In)effectiveness of Voluntarily Produced Transparency Reports.” Business & Society.

Parsons, Christopher, and Tamir Israel. 2016. “Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada.” Citizen Lab. Available at: https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf.

Pelizzo, Riccardo, and Stapenhurst, Frederick. 2013. *Government Accountability and Legislative Oversight*. Routledge.

Renan, Daphna. 2016. "The FISC's Stealth Administrative Laws." In *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, Zachary K. Goldman and Samuel J. Rascoff (ed). New York: Oxford University Press.

Roach, Kent. 2016. “Review and Oversight of Intelligence in Canada: Expanding Accountability Gaps.” In *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, Zachary K. Goldman and Samuel J. Rascoff (ed). New York: Oxford University Press.

Roberts, Alisdar. 2007. "Transparency in the Security Sector." In The Right to Know: Transparency For An Open World, Ann Florini (Ed.). Columbia University Press. Pp. 309-336.

Robinson, Bill. 2000. “An unofficial look inside the Communications Security Establishment, Canada’s signals intelligence agency,” Lux Ex Umbra. Available at: http://circ.jmellon.com/docs/html/communications_security_establishment_unofficial_webpage_020623.html.

Robinson, Bill. 2015. “Does CSE comply with the law?”, Lux Ex Umbra. Available at: https://luxexumbra.blogspot.ca/2015/03/does-cse-comply-with-law.html.

Savoie, Donald J. (2003). Breaking the Bargain: Public Servants, Ministers, and Parliament. University of Toronto Press: Toronto.

Schedler, Andreas. 1999. “Conceptualizing Accountability.” In *The Self-Restraining State: Power and Accountability in New Democracies*, edited by Andrew Schelder, Larry Diamond, and Marc Plattner. Boulder, CO: Lynne Rienner.

Scholte, Jan Aart. 2002. “Civil Society and Democracy in Global Governance,” Global Governance 8(3): 281-304.

Sinclair, Amanda. 1995. “The Chameleon of Accountability: Forms and Discourses.” Accounting, Organizations and Society 20 (2-3): 219-37.

Smith, Dale. 2017. *The Unbroken Machine: Canada’s Democracy in Action*. Dundurn.

Stone, Bruce. 1995. “Administrative Accountability in the ‘Westminster’ Democracies: Towards a New Conceptual Framework.” Governance 8 (4): 502-25.

Walsh, Patrick F., and Miller, Seumas. 2016. “Rethinking the ‘Five Eyes’ Security Intelligence Collection Policies and Practice Post-Snowden.” Intelligence and National Security 31(3): 345-368.

Wayland, K., Armengol, R., and Johnson, D. 2012. “When transparency isn’t transparent: Campaign finance disclosure and internet surveillance.” In *Internet and surveillance: The challenges of Web 2.0 and social media*, C. Fuchs, K. Boersma, A. Albrechtslund, and M. Sandoval (eds.). New York: Routledge.

Westin, Greg; Greenwald, Glenn; and Ryan Gallagher. 2014. CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents. CBC News. Available at: http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881.

Legisation

National Defence Act, RSC 1985, c N-5.

Bill C-22: An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts. 2017. Royal Assent September 22, 2017, 42 Parliament, 1st Session. Retrieved from the Parliament of Canada website http://www.parl.ca/DocumentViewer/en/42-1/bill/C-22/royal-assent.

Bill C-59: An Act respecting national security matters. 2017. 1st Reading June 20, 2017, 42 Parliament, 1st Session. Retrieved from the Parliament of Canada website http://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/first-reading.

Federal Court

X (Re), [2010] 1 FCR 460, 2009 FC 1058 (CanLII), <http://canlii.ca/t/2669z>, retrieved on 2017-09-25

X (Re), 2016 FC 1105 (CanLII), <http://canlii.ca/t/gw01x>, retrieved on 2017-09-25