Canadian Journal of Law and Technology

Volume 16 | Number 1 Article 16

1-1-2018

Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports

Christopher Parsons

Adam Molnar

Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports

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

Abstract

Real time electronic government surveillance is recognized as amongst the most intrusive types of government activity upon private citizens' lives. There are usually stringent warranting practices that must be met prior to law enforcement or security agencies engaging in such domestic surveillance. In Canada, federal and provincial governments must report annually on these practices when they are conducted by law enforcement or the Canadian Security Intelligence Service, disclosing how often such warrants are sought and granted, the types of crimes such surveillance is directed towards, and the efficacy of such surveillance in being used as evidence and securing convictions.

This article draws on an empirical examination of federal and provincial electronic surveillance reports in Canada to examine the usefulness of Canadian governments' annual electronic surveillance reports for legislators and external stakeholders alike to hold the government to account. It explores whether there are primary gaps in accountability, such as where there are no legislative requirements to produce records to legislators or external stakeholders. It also examines the extent to which secondary gaps exist, such as where there is a failure of legislative compliance or ambiguity related to that compliance.

We find that extensive secondary gaps undermine legislators' abilities to hold government to account and weaken capacities for external stakeholders to understand and demand justification for government surveillance activities. In particular, these gaps arise from the failure to annually table reports, in divergent

---

[*] 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.

The authors would like to thank Christopher Prince and Lex Gill for their feedback, as well Micheal Vonn, Tamir Israel, Joshua Segrave, Erik Zouave, and members of the Citizen Lab for comments received throughout this research project. We would also like to thank the anonymous reviewers who invested their time to suggest helpful ways of improving the article

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

The author 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.

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

formatting of reports between jurisdictions, and in the deficient narrative explanations accompanying the tabled electronic surveillance reports. The chronic nature of these gaps leads us to argue that there are policy failures emergent from the discretion granted to government Ministers and failures to deliberately establish conditions that would ensure governmental accountability. Unless these deficiencies are corrected, accountability reporting as a public policy instrument threatens to advance a veneer of political legitimacy at the expense of maintaining fulsome democratic safeguards to secure the freedoms associated with liberal democratic political systems. We ultimately make a series of policy proposals which, if adopted, should ensure that government accountability reporting is both substantial and effective as a policy instrument to monitor and review the efficacy of real-time electronic surveillance in Canada.

INTRODUCTION

Government agencies have conducted telecommunications surveillance since the inception of the telegraph, and each new means of communication has been accompanied by new surveillance capabilities.[1] Following concerns in the 1960s and 1970s about the computerization of personal information and new kinds of electronic surveillance methods the Government of Canada passed the *Protection of Privacy Act*.[2] The Act, amongst other things, required federal and provincial governments to present annual reports that detailed the number of electronic surveillance requests and approvals, how they were carried out, and their utility in securing convictions against alleged criminal offenders. The Act was amended in 1977 to "require [law enforcement agencies] to provide notification to investigative subjects within 90 days of the date upon which the authorization was issued and to comply with strict court restrictions on how, what, and where suspects may be monitored."[3] The intended effects of these reports (along with notification requirements) were to publicize how often government agencies used their interception powers which, in turn, would make them more accountable to their respective legislative assemblies.

Previous scholars have examined the extent to which electronic surveillance reports accurately account for government surveillance activities and the extent to which they enable legislators to meaningfully hold agencies accountable for intrusions into private citizens' lives. Kennedy and Swire found differences between how American federal and state agencies obtain interception orders and

---

1 Serena Chan & L. Jean Camp, "Law Enforcement Surveillance in the Network Society", *IEEE Technology and Society Magazine* 21:2 (2002); Susan Landau, *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies* (London: MIT Press, 2010) [Landau, *Surveillance or Security?*]; Stanley M. Beck, "Electronic Surveillance and the Administration of Criminal Justice" (1968) 46:4 Can Bar Rev 643.

2 *Protection of Privacy Act*, S.C. 1973-74, c. 50.

3 Nicholas Koutros and Julien Demers, "Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement" (2013) 11:1 CJLT 79 [Koutros and Demers, "Big Brother's Shadow"].

were held to account for their operation.[4] Nuun examined the extent to which American interception orders were used to secure arrests and convictions, finding that the "productivity" of interception orders varied considerably based on whether interceptions were used to arrest suspects or to secure convictions. [5] Koutros and Demers examined Canadian federal government interception reports and found that there had been a decline in the annual number of reported federal wiretaps.[6] Other work has examined the extent to which existing surveillance reporting in Canada and the United States inadequately accounts for contemporary modes of government surveillance techniques and proposes ways of correcting existing reporting mechanisms.[7]

To date, however, no research has systematically examined Canadian federal and provincial/territorial statutory electronic surveillance reports to determine whether they promote accountability between the government and legislature, and the government and public more broadly. This article finds deficiencies in how governments tabulate data for these reports, as well as in how governments present the information to legislative assemblies and the public, leading to accountability gaps concerning how governments report on electronic surveillance. Existing limitations of statutory surveillance reporting requirements call into question the efficacy of civil society and scholarly proposals to expand surveillance accountability by adopting templates that are currently used for electronic surveillance reports.

---

4 Charles H. Kennedy and Peter P. Swire, "State Wiretaps and Electronic Surveillance After September 11" (2003) 54:4 Hastings LJ 971.

5 Samuel Nunn, "Measuring Criminal Justice Technology Outputs: The Case of Title III Wiretap Productivity" (2008) 36:4 Journal of Criminal Justice 293.

6 Koutros and Demers, "Big Brother's Shadow", *supra* note 3.

7 Christopher Parsons, "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians", *Citizen Lab* (2015), online: < http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf > [Parsons, "The Governance of Telecommunications Surveillance"]; Christopher Soghoian, "The Law Enforcement Surveillance Reporting Gap", online: (2011) SSRN Electronic Journal < https://papers.ssrn.com/sol3/papers.cfm?abstract_id = 1806628 > [Soghoian, "Surveillance Reporting Gap"]; Paul M. Schwartz, "Reviving Telecommunications Surveillance Law" (2008) 75:1 U Chicago L Rev 287 [Schwartz, "Reviving Telecommunications"]; Devon Ombres, "NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History, Constitutional Basis, and the Efforts at Reform" (2015) 39:1 Seton Hall Legis J 27; Tyler C. Anderson, "Toward Institutional Reform of Intelligence Surveillance: A Proposal to Amend the Foreign Intelligence Surveillance Act" (2014) 8 Harvard Law & Policy Review 413; Craig Forcese, "Law, Logarithms and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives" in Michael Geist, ed., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: University of Ottawa Press, 2015) at 103; James Losey, "Surveillance of Communications: A Legitimation Crisis and the Need for Transparency" (2015) 9 International Journal of Communications 3450; Andrew Clement & Jonathan Obar, "Keeping Internet Users in the Know or in the Dark" (2016) 6:1 Journal of Information Policy 294, online: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id = 2996173 > .

Part I introduces a two-part conceptual framework for better understanding government accountability in the context of electronic surveillance. First, we discuss how "vertical" accountability between different government institutions and branches of government enable or constrain possibilities for the legislature to hold the government to account. Second, we explore how "horizontal" accountability between government institutions and the public strengthen public engagement into government policy, which fosters relationships that can promote trust and accountability in government activities. Third, we link vertical and horizontal accountability to annual electronic surveillance reports in Canada and discuss the value of these modes of accountability to monitor government interference into private life.

Part II discusses how interception reports for Canadian jurisdictions were collected and how data was collated for analysis. Part III discusses the major findings from the data, namely, deficiencies associated with the tabling, accessibility, and formatting of annual electronic surveillance reports. Part IV critically assesses whether the analyzed interception reports successfully promote governments' accountability to legislative assemblies and the public. Part V summarizes our argument and identifies areas of future work.

I. ACCOUNTABILITY AND LEGITIMIZATION

Legislators in democratic countries have created mechanisms to promote the accountability of public officials towards citizens. Such mechanisms are intended to impose binding rules on the powers and authority of public officials to ensure accountability.[8] Accountability exists "when there is a relationship where an individual or institution, and the performance of tasks or 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."[9] As such, an institution must both be obligated to answer questions regarding its decisions or actions and there must be a means for enforcing consequences for failing to be accountable.[10]

---

[8] David Brinkerhoff, "Taking Account of Accountability: A Conceptual Overview and Strategic Options", *US Agency for International Development Center for Democracy and Governance Implementing Policy Change Project Phase 2* (Washington, D.C.: March 2001), online: < http://www.msiworldwide.com/wp-content/uploads/2011/07/IPC_Taking_Account_of_Accountability.pdf >.

[9] Riccardo Pelizzo & Frederick Stapenhurst, *Government Accountability and Legislative Oversight* (New York: Routledge, 2013) at 2.

[10] Andreas Schedler, "Conceptualizing Accountability" in Andreas Schedler, Larry Diamond & Marc Plattner, eds., *The Self-Restraining State: Power and Accountability in New Democracies* (Boulder: Lynne Rienner, 1999) 13; Andrew Blick & Edward Hedger, "Literature Review of Factors Contributing to Commonwealth Public Accounts Committees Effectively Holding Government to Account for the Use of Public Resources", *Overseas Development Institute* (2008).

The accountability literature in political science and public policy has often focused on a hierarchical model, such as the responsibility of Ministers or members of the executive to their respective legislative bodies. This model involves an actor that is accountable to a forum, for particular activities or actions, where the forum could discipline the actor should they fall short of expected activities or actions.[11] As discussed by Mulgan, an extensive literature has developed to critique, supplement, or contextualize this traditional approach.[12] Accountability is sometimes now understood as establishing unnecessary adversarial processes,[13] as a concept needing to take on board how actors are sanctioned by their professional organizations,[14] as addressing how institutions control official behaviours through internal organizational processes,[15] as concerning how officials are accountable to the public directly[16] and to legislators through parliamentary appearances,[17] and how democratic dialogue disciplines institutions.[18] These changes to how accountability is conceptualized are based, in part, on the fact that private actors now assume roles and responsibilities that were carried out solely under the authority of state agencies.[19]

(a) Vertical and Horizontal Accountability

An open debate exists about whether the extensions of the concept of accountability are "more the creations of academics pursuing their own intellectual agendas" as opposed to "the result of shifts in everyday usage" of the term within government.[20] For this article, we examine accountability

---

[11] Richard Mulgan, "The Processes of Public Accountability" (1997) 56:1 Australian Journal of Public Accountability 25; Jonathan Anderson, "Illusions of Accountability: Credit and Blame Sensemaking in Public Administration" (2009) 31:3 Administrative Theory & Praxis 322 [Anderson, "Illusions of Accountability"].

[12] Richard Mulgan, "'Accountability': An Ever-Expanding Concept?" (2000) 78:3 Public Administration 555 [Mulgan, "Accountability"].

[13] Anderson, "Illusions of Accountability", *supra* note 11.

[14] Linda Deleon, "Accountability in A 'Reinvented' Government" (1998) 76:3 Public Administration 539.

[15] Amanda Sinclair, "The Chameleon of Accountability: Forms and Discourses" (1995) 20:2-3 *Accounting, Organizations and Society* 219; David C. Corbett, *Australian Public Sector Management*, 2nd ed. (St. Leonards, NSW: Allen & Unwin, 1996).

[16] Owen E. Hughes, *Public Management and Administration*, 2nd ed. (London: Macmillan, 1998).

[17] Bruce Stone, "Administrative Accountability in the 'Westminster' Democracies: Towards a New Conceptual Framework" (1995) 8:4 Governance 505 [Stone, "Administrative Accountability"].

[18] James G. March & Johan P. Olsen, *Democratic Governance* (New York: Free Press, 1995).

[19] Colin Scott, "Accountability in the Regulatory State" (2000) 27:1 JL & Soc'y 38.

[20] Mulgan, "Accountability", *supra* note 12 at 571.

exclusively through two lenses. First, through the lens of parliamentary Ministers being formally compelled to account for their departments' activities to legislative assemblies.[21] Second, through the lens of informal accountability measures which arise as public and policy communities hold government to account based upon the information publicly provided to legislatures.[22]

Ministerial reporting is characterized as being "vertical" because it takes place in a formal context involving a relationship between an actor (the Minister) and a forum (the legislature), where the actor is obligated to explain and justify their actions, and the forum is empowered to receive the explanation and justification, as well as to issue sanctions as needed. This type of accountability includes agreements between the actor and forum about which explanations are owed, the terms according to which the explanations are to be provided, and the consequences that might follow.[23] Our focus is on the extent to which processes and policies associated with Ministerial accountability operate when actually put into practice.

Informal reporting, in contrast, is referred to as "horizontal accountability" and is characterized as building accountability through civil engagement. This mode of accountability is meant to complement and enhance government accountability processes.[24] The parties involved in horizontal accountability lack a direct ability to impose sanction or exercise coercion and there is no formal requirement for an actor to provide an account to that forum.[25] Instead, horizontal accountability involves an actor voluntarily choosing to present information to a forum and receiving feedback or facing moral suasion based on the forum's evaluation of the presented information. If the media amplifies these debates, horizontal processes of accountability through civic engagement may be strengthened.[26]

Regimes of government accountability are designed to monitor and control government conduct. Such control is enforced during a government's tenure in office by the legislature and, during the electoral period, by "citizens, who pass judgement on the conduct of the government and who indicate their displeasure

---

[21] Dale Smith, *The Unbroken Machine: Canada's Democracy in Action* (Toronto: Dundurn, 2017); Bruce Stone, "Administrative Accountability", *supra* note 17.

[22] Carmen Malena et al., "Social Accountability: An Introduction to the Concept and Emerging Practice" (2004) The World Bank Working Paper No. 31042 at 76 [Malena et al., "Social Accountability"].

[23] Deborah G. Johnson, "Accountability in a House of Mirrors" in Deborah G. Johnson & Priscilla M. Regan, eds., *Transparency and Surveillance as Sociotechnical Accountability: A House of Mirrors* (New York: Routledge, 2014) 131 at 136 [Johnson, "Accountability in a House of Mirrors"].

[24] Malena et al., "Social Accountability", *supra* note 22 at 76.

[25] Mark Bovens, "Analysing and Assessing Accountability: A Conceptual Framework" (2007) 13:4 Eur LJ 447 [Bovens, "Analysing and Assessing Accountability"].

[26] Malena et al., "Social Accountability", *supra* note 22 at 76; Maxwell McCombs, *Setting the Agenda: Mass Media and Public Opinion* (Cambridge: John Wiley & Sons, 2014).

by voting for other popular representatives."[27] Where a legislature is slow or deficient in holding the government to account, then processes of accountability can be assisted by measures of horizontal accountability. Horizontal accountability practices can help to identify problems in government as external stakeholders evaluate government practices so that legislators can subsequently raise the problems (and possible solutions) with government. External experts can also be called to testify before committees or provide direct briefings to specific legislators or government departments. However, to be effective, those external to government require access to information and capacity to take on horizontal accountability tasks. There must also be state willingness and capacity to implement changes proposed by civil society, and active and meaningful interfaces between civil society and the state.[28] Absent these characteristics, external stakeholders will lack the material they need to hold the government to account, and legislators will lack required resources to effect change when issues are brought onto the policy agenda.

(b) Accountability Gaps

Accountability gaps can arise between actors and the forums to which they are responsible when "reviewers or overseers do not have adequate powers or resources to match the conduct that is being reviewed."[29] There may be either primary or secondary-types of accountability gaps. Primary gaps arise when there are no legislative requirements to produce government data, which is itself required to exercise accountability functions in the first place. Such primary gaps stymie both vertical and horizontal accountability. Secondary gaps arise when legislative requirements compel a certain degree of government accountability but the required information is either not provided or there are insufficient resources or capacity to analyze the data in question. For example, when a forum lacks expertise or capacity to understand the information provided by an actor they may be unaware that sanctions constitute an appropriate response. A lack of capacity can also be linked to an absence of long-serving legislators who have developed subject matter expertise concerning the actor's activities or obligations or to limits in external stakeholders' attention to the reporting or ability to act on disclosed information.[30] Another example of a secondary gap might emerge when the information that is provided by the actor may be sufficiently unclear

---

[27] Bovens, "Analysing and Assessing Accountability", *supra* note 25 at 463.

[28] Malena et al., "Social Accountability", *supra* note 22 at 76.

[29] Kent Roach, "Permanent Accountability Gaps and Partial Remedies" in Michael Geist, ed., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: University of Ottawa Press, 2015) 163 at 169.

[30] Rod B. Byers, "Perceptions of Parliamentary Surveillance of the Executive: The Case of Canadian Defence Policy" (1972) 5:2 Canadian Journal of Political Science 234; Brent Rathgeber, *Irresponsible Government: The Decline of Parliamentary Democracy in Canada* (Toronto: Dundurn, 2014); Malena et al., "Social Accountability", *supra* note 22 at 76; Johnson, "Accountability in a House of Mirrors", *supra* note 23 at 136.

that the forum cannot interpret what is provided.[31] Accountability gaps run the risk of turning into accountability failures when either primary or secondary gaps become the norm, as opposed to the exception.

Accountability gaps pose dangers to democratic governance. On the one hand, if elected representatives do not, or cannot, hold government to account, then there is a breakdown in the representative democratic system insofar as the electorate's intentions of being well represented are not met.[32] Breakdown can prompt cynicism or doubt concerning legislators' competency in representing the electorate and, as such, inhibit electors from seeing themselves in the actions of legislators.[33] Moreover, accountability serves to "help to ensure the legitimacy of governance remains intact or is increased" by providing administrators "the opportunity to explain and justify their intentions" and enabling citizens and interest groups to "pose questions and offer their opinion". Such questioning, or horizontal accountability, "can promote acceptance of government authority and the citizens' confidence in the government's administration."[34] Thus, a failure by government to meet its obligations to disclose information can diminish the democratic bonds between citizens and their government and weaken the faith that lawful activities are undertaken with the approval, or democratic consent, of the citizenry.[35]

(c) Government Surveillance Accountability

Real-time government electronic surveillance can take many forms, including recording audio or visual activities, intercepting communications, or planting surveillance equipment in individuals' homes, vehicles, or workplaces. Such surveillance activities capture data in real-time and employ techniques that intrude into private spaces or capture the contents of private communications. These modes of surveillance stand in contradistinction to government powers that empower agencies to retrieve data in "stored" format, after it has been saved in either a digital or physical form. Criminal Codes have historically established the highest degrees of privacy protection around live real-time electronic

---

31 Archon Fung et al., *Full Disclosure: The Perils and Promise of Transparency* (New York: Cambridge University Press, 2007) [Fung et al., *Full Disclosure*].

32 Kevin D. Haggerty & Mina Samatas, "Introduction: Surveillance and Democracy: An Unsettled Relationship" in Kevin D. Haggerty & Minas Samatas, eds., *Surveillance and Democracy* (Canada: Routledge-Cavendish, 2010).

33 Jürgen Habermas, "On the Internal Relation between the Rule of Law and Democracy" in Jürgen Habermas, ed., *The Inclusion of the Other: Studies in Political Theory* (Cambridge: The MIT Press, 1998) 253 [Habermas, "Internal Relation"]; Christopher Parsons, "Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance" (2015) 3:3 Media and Communication 1.

34 Bovens, "Analysing and Assessing Accountability", *supra* note 25 at 464.

35 Habermas, "Internal Relation", *supra* note 33 at 253; Jürgen Habermas, "Three Normative Models of Democracy" in Jürgen Habermas, ed., *The Inclusion of the Other: Studies in Political Theory* (Cambridge: The MIT Press, 1998) 239.

surveillance, on the basis that secretive monitoring of live communications or activities is deeply revealing of private life.[36] In contrast, other ways of collecting data about a person or their communications are regularly afforded lower privacy protections, and include the collection of technical details surrounding those communications such as routing information, times of communications, or identifiers of the tools used to communicate (so-called "metadata"), or accessing data that is stored by third-parties such as email on a private companies' computer servers.[37] In the United States, the National Commission argued in 1976 that "wiretaps and eavesdrops are potentially more penetrating, less discriminating, and less visible than ordinary searches" and thus recommended a stringent process for prior judicial authorization be met before law enforcement or security agencies be allowed to engage in such surveillance.[38] This logic was adopted by the Canadian government when it established its own accountability and oversight regimes concerning electronic surveillance.[39]

Warrants are typically required before a Canadian government agency may conduct real-time electronic interception of communications.[40] Electronic surveillance warrants provide a control-based mode of accountability by adding a check to the government's actions. Before authorities can take action,

---

[36] Landau, *Surveillance or Security?*, *supra* note 1; Christopher Parsons and Tamir Israel, "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada", *Citizen Lab — Telecom Transparency Project // CIPPIC* (August 2016), online: <https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf> [Parsons and Israel, "Gone Opaque?"].

[37] The diminished expectations of privacy associated with stored data and metadata are highly contentious in academic literature and have been successfully challenged in Canadian courts (see *R. v. TELUS Communications Co.*, 2013 SCC 16, 2013 CarswellOnt 3216, 2013 CarswellOnt 3217; *R. v. Spencer*, 2014 SCC 43, 2014 CarswellSask 342, 2014 CarswellSask 343). See Government of Canada, "Guidelines for Agents and Peace Officers Designated by the Minister of Public Safety Canada (PS)" *Public Safety Canada* (December 2015), online: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/gdlns-gnts-pc-ffcrs/index-en.aspx> [Government of Canada, "Guidelines for Agents and Peace Officers"]; Parsons, "The Governance of Telecommunications Surveillance", *supra* note 7; Parsons & Israel, "Gone Opaque?", *supra* note 36; Schwartz, "Reviving Telecommunications", *supra* note 7; Soghoian, "Surveillance Reporting Gap", *supra* note 7.

[38] United States, National Commission for the Review of Federal and State Laws relating to Wiretapping and Electronic Surveillance, *Electronic Surveillance* (Washington: United States Government, 1976).

[39] Koutros and Demers, "Big Brother's Shadow", *supra* note 3; Canada, Law Reform Commission of Canada, "Electronic Surveillance" (1986) Working Paper No. 47; Morris Manning, *Wiretap Law in Canada: A Supplement to the Protection of Privacy Act, Bill C-176: An Analysis and Commentary* (Toronto: Butterworths, 1978).

[40] Government agencies can sometimes use emergency provisions to quickly initiate a real-time interception. Agencies that use these powers must provide notice to those targeted by such interceptions within 90 days, annually report on the regularity at which such emergency interceptions are conducted, and only use these emergency powers in relation to investigating criminal activities in s. 183 of Canada's *Criminal Code*.

the operation must be approved by a forum. Specifically, in the case of real-time electronic surveillance government agencies must typically convince a judge as well as a Minister that they have reasonable and probable grounds to believe that the real-time surveillance is necessary to conduct an investigation, that affected persons are identified as best as possible, and that all places in which the interception will take place have been disclosed.[41] Affiants requesting the warrant must also include whether surreptitious entry to a private space is required (e.g., to place a bug or video camera in a residence) as well as describe how they will limit their activities to protect the privacy of uninvolved persons.[42] Only once the judge is satisfied with the information provided, and authorities have clarified any questions posed or ambiguity detected by the judge, is the requesting authority authorized to initiate the surveillance.

While judicial authorization functions as a control-based means of accountability, insofar as a judge can refuse to grant an interception order, the *Protection of Privacy Act* also requires provincial and federal governments to prepare and table annual reports concerning their agencies' use of electronic surveillance. As a review-based mechanism, these reports include information such as the total number of requests for interceptions made, and granted, the type of investigative method used, such as telephonic versus microphonic versus video interceptions, and the regularity at which interception-derived evidence is introduced into courts and used to secure convictions.[43]

These reports facilitate vertical accountability within the government, and between the government and legislators, in at least two ways. First, in preparing these reports the different federal or provincial agencies demonstrate accountability to their respective Minister in the Westminster tradition. Ministers assume responsibility for what their agencies do and also provide direction and control over their behaviours.[44] Second, when these reports are presented to the appropriate legislative assembly, legislators are subsequently expected to be able to answer basic questions such as whether surveillance capabilities were being used effectively and whether they were affecting disproportionate numbers of people.[45] If such questions cannot be answered with the provided information then legislators can challenge the government to answer those queries. Ultimately, the information in these annual reports is needed for legislators to determine "whether the government is judiciously

---

[41] Koutros and Demers, "Big Brother's Shadow", *supra* note 3; *Criminal Code*, R.S.C. 1985, c. C-46, ss. 184-186 [*Criminal Code*].

[42] Government of Canada, "Guidelines for Agents and Peace Officers", *supra* note 37.

[43] *Criminal Code*, *supra* note 41, s. 195.

[44] Adam Przeworski and Susan C. Stokes, *Democracy, Accountability, and Representation* (Cambridge: Cambridge University Press, 1999); Kaare Strm, "Parliamentary Democracy and Delegation" in Kaare Strm, Wolfgang C. Müller and Torbj—rn Bergman, eds., *Delegation and Accountability in Parliamentary Democracies* (New York: Oxford University Press, 2003) 55.

[45] Schwartz, "Reviving Telecommunications", *supra* note 7.

exercising its surveillance powers, whether the exercised powers are effectively addressing social ills, or whether the powers and their associated practices represent a good investment of taxpayer money."[46]

Thus, on the one hand legislators can exercise their vertical accountability by holding the government to account for any impropriety in how the reports have been provided or to raise questions about anomalous statistics. On the other hand, parties external to government can engage in horizontal accountability measures if they find the reported information deficient, either in explaining the statistical reporting provided by government or because there are other anomalies in how the information is presented. Horizontal accountability, however, lacks the formal mechanisms to sanction governments for issuing deficient, incorrect, or tardy reports. The degree of "accountability" imposed on the government, then, tends to be normative as opposed to lawfully compelled because it relies solely on critical evaluation of government activities as represented in the reports, as well as the activities that underpin the reports, within a voluntary forum of public debate. The disciplining activities undertaken when engaging in horizontal accountability bear a strong resemblance to the disciplining activities which are taken towards both public and private organizations which release data in the service of being "transparent" around an issue of public concern. Such transparency efforts collate and disclose information to create a "flow of information" to those outside the organization that generates it.[47] Such projects are designed to either operate as "a form of verifiability" or a kind of performance[48] to provide "information on matters of public concern."[49]

The mere act of issuing an annual report constitutes a first-step towards accountability given that published reports can potentially be scrutinized by a social forum. While a requirement exists to submit annual electronic surveillance reports to Canadian legislative assemblies, there is no obligation to provide these reports to civil society in an accessible format. Documents tabled or presented in legislative assemblies may be challenging or impossible to access without physically travelling to legislative libraries. The result is that while such documents may be "public", they are not always accessible to parties external to the government itself. Furthermore, there is no absolute requirement for civil society to take up, evaluate, scrutinize, or question reports provided by the government, which parallels how such stakeholders may be inattentive to

---

[46] Parsons, "The Governance of Telecommunications Surveillance", *supra* note 7.

[47] Sylvester C. W. Eigffinger and Petra M. Geraats, *Government Transparency: Impacts and Unintended Consequences* (New York: Palgrave Macmillan, 2006); Robert M. Bushman et al., "What Determines Corporate Transparency?" (2004) 42:2 Journal of Accounting Research 207.

[48] Oana B. Albu & Mikkel Flyverbom, "Organizational Transparency: Conceptualizations, Conditions, and Consequences", *Business & Society* (13 July 2016).

[49] Roger Cotterrell, "Transparency, Mass Media, Ideology and Community" (1999) 3:4 Journal for Cultural Research 414.

information released through transparency projects by either private firms or government.[50] Specifically, "the crowdsourcing enabled by transparency is not evenhanded, unbiased, consistent, or itself accountable. The "crowd" that watches consist of those who are intensely interested in whatever is being watched and often shares a certain perspective. The crowd also tends to be episodic in its coverage."[51] This does not mean that civil society's horizontal accountability or its attention to transparency projects are without merit. Experience has shown that applying either moral or political suasion to an organization can subsequently modify its behaviour.[52] Ultimately however, absent an ability to legally challenge a government's accountability reporting or release of public data, civil society is limited in its ability to informally compel changes in government activity.

II. METHODOLOGY

To analyze the annual electronic surveillance reports tabled by Canada's federal and provincial governments, we first attempted to access the reports from governmental websites in July 2015. We found publicly available reports online from the federal government, as well as the governments of Alberta, Nova Scotia, and Quebec. When unable to find such publicly available reports we sent a standard form request (Appendix 1) to all other provinces' and territories' respective Justice departments, when there was a public method of contacting them, or to a general government inquiry email or communications email address when there was no clear way to directly contact the relevant government's Justice department. The standard form request asked for all electronic surveillance reports, prepared by the respective governments' solicitor general, for the years 2005-2014. Given that requests were sent in mid-2015, the most current reports that were available at the time were expected to be from 2014. The governments of British Columbia, Manitoba, New Brunswick, and Ontario provided copies of reports following these requests. Non-responsive provinces and territories included: Prince Edward Island, Newfoundland, Saskatchewan, Yukon, Northwest Territories, and Nunavut. It was only following an inquiry from a colleague in the media in late 2017 that Newfoundland, Saskatchewan, Nunavut and Yukon replied. The two provinces provided links into their online-accessible Hansards, from which we were able to find many of their annual electronic

---

[50] Christopher Parsons, "The (In)effectiveness of Voluntarily Produced Transparency Reports", *Business & Society* (17 July 2017) [Parsons, "Voluntarily Produced Transparency Reports"].

[51] Priscilla M. Regan and Deborah G. Johnson, "Policy Options for Reconfiguring the Mirrors" in Deborah G. Johnson and Priscilla M. Regan, eds., *Transparency and Surveillance as Sociotechnical Accountability: A House of Mirrors* (New York: Routledge, 2014) 162 at 166.

[52] Jill A. Brown et al., "Board Socio-cognitive Decision-making and Task Performance Under Heightened Expectations of Accountability", *Business & Society* (7 November 2016).

surveillance reports. Nunavut and Yukon, in contrast, asserted that its electronic surveillance statistics are included in the federal government's reports and thus the respective governments do not produce territory-specific reports.

All documents were provided in .pdf format. A spreadsheet was created to tabulate data contained in the reports. A generic spreadsheet format was created per the requirements for reporting that are established in the *Criminal Code*, with modifications to the template made on a per-province basis if there was deviation from the mandated format. Baseline categories included:

- total number of authorizations and numbers of times they were renewed;
- general description of the ways in which communications are intercepted;
- type of offences related to surveillance authorizations;
- the number of times evidence from interceptions was adduced in criminal proceedings;
- the number of times evidence from interceptions resulted in convictions;
- the number of notifications issued to targets of surveillance.

Our data set represents the most recently available data from the reports we gathered. Alberta, Nova Scotia, New Brunswick, Newfoundland, Manitoba, Quebec, and Saskatchewan release information specific to each year of the document (*i.e.* all information pertaining to interceptions in a given year are captured in the following year's report). All other governments similarly release data on an annual basis, but include updates to previously published annual reports (*i.e.* a report tabled in 2014 about interception activities undertaken in 2013 might also update statistics concerning interceptions carried out in 2007). As we will discuss, these updates raise questions about how reports should be evaluated by legislators and stakeholders external to government alike.

III. DATA

(a) Tabling of Reports

Governments must annually table their electronic surveillance reports to their respective legislative assemblies.[53] The reports we obtained for British Columbia, New Brunswick, and Ontario lacked publication dates, thus preventing us from determining when they were tabled.

Federal government reports were generally tabled in Parliament annually, though the 2014 and 2015 reports were both released in 2016 and the 2008 report was tabled after the 2009 report. Alberta generally published its reports each year, save for the 2012 and 2013 years, which were published in 2014 and 2015, respectively. Manitoba's annual reports are irregularly published; the 2005 and 2006 reports were both tabled in 2007, the 2008 and 2009 reports both in 2010, and the 2012 and 2013 reports both in 2014. We were not able to obtain a report for 2011. We were unable to find several of Newfoundland's reports, inclusive of

---

[53] *Criminal Code*, *supra* note 41, s. 195.

2010-2012, though otherwise the province issued annual reports. Nova Scotia's reports were tabled annually for 2005-2008, whereas there was a bulk publication of annual reports for 2009-2013 on March 18, 2015. Quebec's reports were the least regularly tabled, with the 2005 and 2006 reports being tabled in 2006, the 2006-2007 reports tabled in 2014, and 2008-2014 reports all being tabled in June 2016 following the Quebec government calling an inquiry into police surveillance of journalists.[54] Saskatchewan's reports were generally tabled each year, though we were unable to locate the report for 2010.

(b) Accessibility of Reports to the Public

Some governments made their annual reports accessible to the public online, which meant that we could easily access and download reports from the governments of Canada, Alberta, and Nova Scotia. While Quebec's reports were online as well, reports tended to be published in batches; when we first collected reports in mid-2015 we could only download reports until 2005. Reports from Newfoundland and Saskatchewan were available online through their respective Gazettes, but the available public search functions on the governments' own websites were unable to find the reports. Moreover, the Saskatchewan reports do not cite the law which requires the province to issue these annual reports and title these sections of their Gazette as "Criminal Code (Canada)". Combined, these limitations significantly impeded the accessibility of the reports from Newfoundland and Saskatchewan.

We did not receive the same responses from all provinces when we requested copies of their annual reports. A government official in Quebec informed us that reports from 2005-2014 would be provided once the individual responsible for them returned from vacation. No reports were ever provided by that individual, though reports for 2005-2015 were published online in February 2017 following scandals that Quebec police had been conducting electronic surveillance of journalists.[55] In contrast, the governments of British Columbia, Manitoba, New Brunswick, and Ontario responded to our requests for copies of their annual reports. The government official in British Columbia initially stated they did not produce annual reports and only found and provided them upon further questioning.[56] The Manitoba Queen's Printer was able to provide reports for 2005-2012, with the exception of 2011, as a copy could not be found. The New Brunswick government compiled and provided copies of its annual reports within five days. The Ontario government provided the reports two months after the initial request. There were no responses to our requests from the governments of Newfoundland, Prince Edward Island, Saskatchewan, Yukon, Northwest

---

[54] See Sidhartha Banerjee, "Quebec Provincial Police Admits to Monitoring Six Reporters' Phones in 2013" *The Star* (2 November 2016), online: < https://www.thestar.com/news/canada/2016/11/02/quebec-provincial-police-had-reporters-under-surveillance-too-media-outlets-say.html > [Banerjee, "Monitoring Reporters' Phones"].

[55] Banerjee, "Monitoring Reporters' Phones", *ibid.*

[56] Communications between author and government.

Territories, or Nunavut. Information we collected concerning Newfoundland, Saskatchewan, Yukon, and Nunavut only came after a media colleague contacted the respective governments in late 2017.

(c) Formatting of Reports

After collating the reports, we evaluated them for similarities and differences in the categories used to report practices of electronic surveillance.

(i) Variations in "Interception by Method" Across Jurisdiction

Provinces and the federal government of Canada report on the methods of interception differently. Some, such as the Federal government, Alberta, Manitoba, and Nova Scotia, report on the modes of interception as involving "Telecommunications", "Microphone", "Video", or "Other". British Columbia included these same four categories, as well as three additional categories: "tracking", "cellular/payphone", and "Internet". However, these supplemental categories in the BC reports appeared in different years. Ontario listed "Telecommunications and Other" and "Room Probes and Body Pack" (each for years 2005-2011), and included a further breakdown in methods for certain years, noting a difference between "Telephone" (only for years 2008-2011) and "Cell Phone" (only for years 2008-2011). Saskatchewan has added and subtracted from its list of interception methods; while "telecommunications" and "microphone" are present in many reports, other categories are added and sometimes removed from reports, including "video", "cell phone", "other", "tracking device", and "body pack". Newfoundland did not report on the number of times that different kinds of electronic surveillance methods were used, but updated its kinds of methods of surveillance during the years we examined. "Telecommunications" and "oral communications" remained a constant kind of interception method across reports, with "video" and "Internet" added in the 2007 report.

Quebec is noteworthy for the number of classifications of interception it provides in reports over the years. The province's reports list "telecommunications" and then uniquely display methods of "video", "microphone", and "other" compared with other jurisdictions. For instance, Quebec includes categories such as "audio device installed in a place" (for years 2004-2014), "video device installed in a place" (for years 2004-2014), "audio device installed on person" (for years 2004-2014), "video device installed on person" (for years 2004-2014), "computer data" (2008-2014), and "other" (appearing in 2013-2014, but showing zero). Faxes were also included as categories in 2013 and 2014. Quebec also included categories for "audio video device installed on person" (2001-2003) and "audio video device installed in place" (2001-2003). "Other (fax machine)" (2001-2003), and "Other (computer data)" (2001-2004) also appeared.

New Brunswick does not include a section for data on interception methods. Instead, Section K of the report includes "A general description of the methods

of interception involved in each interception under an authorization". This section lists "Electromagnetic, Acoustic, Mechanical, or Other Devices ("bugs" in dwellings or other locations, and telephone interceptions)" each year.

(ii) Variations in Reporting Historical Information

While some jurisdictions provide information about prior years' interception reports in each new report, not all do so and not all report on historical data in the same way. While the Federal government and government of British Columbia include historical information, their reports showcase inconsistencies between years, including around the regularity with which interception-related information is adduced as evidence and is used to lead to convictions. For instance, some federal reports indicate that while evidence was adduced in one year, later years showcase a reduction in the number of times in which interception data is adduced into evidence. As an example, the 2012 annual report tabled by the Federal government stated that interception-related evidence was adduced in 659 times, but the government's 2014 annual report revealed that the 2012 numbers were revised downward to 537. Similarly, British Columbia's reports also had downward revisions. The province's annual report issued in 2011 showed that there were only two convictions in 2010, but the 2014 report shows that there were in fact no convictions in 2010. Moreover, in the 2013 report, the number of convictions in 2005 states nine, but the 2014 report revised these convictions downwards.

In comparison to the British Columbia and Federal governments, the governments of Alberta, Quebec, Manitoba, Newfoundland, New Brunswick, Nova Scotia, Ontario, and Saskatchewan only offer statistics from that single year of the report. Consequently, they do not provide revisions to the frequency at which the evidence is adduced, or conviction rates. Nova Scotia, in particular, does not include a separate category of "adduced as evidence" or "resulting in conviction". Instead, they include a section termed "adduced and resulted in conviction". Similarly, Newfoundland's reports did not indicate whether interception-related information was used as evidence or used to secure a conviction. And lastly, while Ontario offers an update in the data for authorizations, they do not do so for convictions.

(iii) Other Conflations in Categories

A small number of other discrepancies emerged in the formatting of the documents. In Ontario and Newfoundland, the number of authorizations specific to the type of warrant was unavailable. Instead, these provinces only provide the number of authorizations, leaving a reader uncertain as to whether a report refers to overall total authorizations or authorizations specific to video-warrants. Compared with other jurisdictions such as Alberta, which break down the figures specific to other warrants such as "audio", "video", "emergency audio", and "emergency video", it is difficult to derive accuracy from the Ontario or Newfoundland figures. There were also discrepancies in how provinces

displayed their backdated data. For instance, the Federal government reports show previous years in consecutive fashion (*i.e.* the 2010 report included information pertaining to 2009, 2008, 2007 and 2006). However, British Columbia did not always display previous year's data in a linear format (*i.e.* British Columbia's 2010 report displayed data for the years 2010, 2009, and 2002, while their 2014 report showed data for the years 2014, 2013, and 2007). The rationale for these differences is not indicated in the report. Furthermore, while New Brunswick (in years 2012, 2013, and 2014) stated that "there have been no authorizations issued in New Brunswick as a result of application", the government did not display any data on how many *applications* were made or what type of applications they were, which would otherwise be available at that time. Information on number and type of application was reflected in other jurisdictions. And lastly, federal reports were the only ones that visualized the data in graphs.

(iv) Variations in Narrative Assessments

Narrative assessments are included in electronic surveillance reports to contextualize the activities undertaken in a given year, challenges that may have been experienced in conducting interceptions, or relative importance of electronic surveillance methods. Past research found that Federal government electronic surveillance reports did not meaningfully change the assessments on an annual basis; the reports used practically the same language each year and thus did not enhance a readers' understanding of the context in which electronic surveillance is conducted. [57] Based on analysis conducted by Koutros and Demers, the last substantive narrative assessment of the federal government's electronic surveillance appeared in the 1995 annual report.[58]

Using 2005 reports as a baseline, we examined the extent to which different provinces modified the text in their narrative assessments. Alberta used the same language from 2005 to 2009, and then ceased including narrative assessments from 2010-2013. British Columbia used the same narrative language from 2005-2014. Manitoba's reports revealed the number of charges, pleas, and times interception data was introduced into courts but did not provide a narrative assessment of the actual value, importance, or challenges linked with electronic surveillance. New Brunswick used the same language for 2005-2011, in which electronic surveillance interceptions were conducted. There were no assessments for 2012-2014, nor were there interceptions conducted in those years. Nova Scotia did not include a narrative assessment of the value of, or challenges facing, electronic assessments in the 2005-2014 reports. Ontario showed small updates – in 2008 a paragraph was added about the importance of interceptions – but the narrative assessment text was largely reused each year, to the point where the 2010 electronic surveillance report did not change the date from 2009 to 2010 in

---

[57] Koutros and Demers, "Big Brothers' Shadow", *supra* note 3.

[58] *Ibid*, at 92.

the assessment paragraphs. Quebec's electronic surveillance reports showed two dominant templates – one from 2005 and the other from 2006 – that was incrementally updated and largely reused from one year to the next. Neither Newfoundland nor Saskatchewan included narrative assessments in their reports. Overall, reading these annual narrative assessments did not provide information concerning the specific importance of interceptions, or note that new communications technologies were impeding the efficacy of electronic surveillance, nor that additional interception capacity was needed for government agencies to conduct their investigations.

IV. DISCUSSION

The presentation of annual electronic surveillance reports is mandated by the *Criminal Code*, but despite requirements that annual reports be issued, our research has found that many governments are only intermittently compliant. Further, the law as written at the time of this article's publication does not require governments to make these annual reports easily accessible to the public. As a result, while there is no primary gap, as the law requires issuing reports to legislative assemblies, a gap nevertheless exists insofar as the law lacks any formal requirement to ensure that extra-governmental forums can access, analyze, and critique the information provided by government. To put it another way, the law as written establishes the basis upon which vertical accountability can be imposed upon ministers, but does not include an explicit process to facilitate horizontal accountability regimes.

Despite a legislative mandate to issue annual reports, there are numerous secondary accountability gaps that weaken or undercut both the vertical and horizontal accountability regimes associated with electronic surveillance in Canada. First and foremost, there are cases where governments have declined or failed to table the annual reports as required under the law. In doing so, legislative assemblies as well as external stakeholders have been prevented from examining the activities undertaken by the government, evaluating the efficacy of the activities undertaken, and understanding the rationale for such activities in the investigation of serious criminal offences in Canada.

Second, tabled reports showcase significant variations with regards to how different types of electronic surveillance are reported. While some provinces provided broad categories (*i.e.* telecommunications, video, audio, "other") others specifically described the target system as mobile phones, internet communications, body cameras, or facsimile communications. Reports that were more specific than others are likely to provide legislators with greater insight into the activities that were being undertaken, and thus allow them to better appreciate the ways in which electronic surveillance is being transformed by the application of old laws to new modes of surveillance. By contrast, categories such as telecommunications, video, audio, and "other" tend to mask how established laws are being used in modern practice.[59] Though governments are permitted under the law to provide non-standardized descriptions of the kinds of electronic

surveillance they are involved in, this lack of standardization makes it challenging to compare surveillance reports issued by one government against the reports of another. The result is that neither legislators nor external stakeholders, nor even the courts approving the surveillance, can confidently understand how government agencies exercise their lawful interception and electronic surveillance powers. Agencies can adopt new technologies for electronic surveillance practices and still not be required to disclose to members of Parliament or to the public the ways that laws have been interpreted to authorize new lines of technical investigation.

Moreover, the challenges in analyzing reports is difficult even within a single jurisdiction. Along with the federal government, some of the provincial governments provide periodic updates to their annual statistics. In some cases, this involves adjusting up or down the total number of times that there were authorizations for electronic surveillance (e.g. shifting from 421 times to 433 times) whereas in others there is only a number beside the "new" number of authorizations (e.g. in a 2013 report there might have been seven authorizations whereas the 2014 report indicates there was one additional authorization, but not the new total of having been eight authorizations). Further, when governments provide updates to past interception reports that were issued many years previously it gives rise to questions about the ability of law enforcement agencies to accurately count the number of authorizations they receive and lawfully monitor their effectiveness. In tandem, the inability of law enforcement bodies to carry out these reporting functions negatively affects the abilities of legislators and external stakeholders to evaluate and trust information submitted by government. Updating statistics years after the required tabling of the annual report undermines informed debate by raising doubt over the veracity of the tabled reports.

The aforementioned secondary gaps – namely in the regularity at which reports are tabled, the differences in how provinces categorize surveillance methods, and updates to past reports – could be at least somewhat remedied if governments included meaningful narratives alongside reported data. For instance, those narratives should include information about why the kinds of surveillance undertaken are important. They should also describe how such surveillance activities are used to advance investigations and prosecutions, explain failures to annually table reports, and clarify to readers why particular models were adopted to update past reports. Moreover, given the regularity with which government agencies discuss the limitations of being able to intercept communications,[60] decry the extent to which encryption stymies investigations as a justification for new interception,[61] and call for other lawful access powers,[62]

---

[59] Adam Molnar, "Technology, Law, and the Formation of (Il)liberal Democracy?" (2017) 15:3/4 Surveillance & Society 318 [Molnar, "(Il)liberal Democracy?"].

[60] Government of Canada, "Guidelines for Agents and Peace Officers", *supra* note 37; Christopher Parsons, "Stuck on the Agenda: Drawing Lessons from the Stagnation of 'Lawful Access' Legislation in Canada" in Michael Geist, ed., *Law, Privacy and*

the narrative sections of reports could place evidence regarding these stated issues before the legislative assembly and to the citizenry itself more widely. But this is not how reports are tabled. Instead, when narrative descriptions are included at all, they largely recycle the text of past years, thus providing no meaningful information to legislators tasked with holding agencies vis-à-vis their Ministers to account, nor to external stakeholders who might also hold the government to account in the public sphere.

Vertical accountability is predicated on the presence of clear laws which establish how an actor presents information to a forum, along with a clear set of sanctions in place should the actor fail to render themselves accountable in the manner prescribed by law. Such information is used to correct an information asymmetry between the government and legislators, so that legislators can subsequently issue sanctions as appropriate. But when actors can retroactively update reports intended to demonstrate their accountability to legislative assemblies without explanations, when no apparent consequences exist for failing to provide more than a general explanation of how invasive powers are used, or where boilerplate language is deployed to justify the necessity of electronic surveillance for criminal investigations, then the ability for legislators to hold the government to account is limited. The information provided grants only a partial correction to the information asymmetry. In parliamentary government systems, there are dedicated critics of different government departments, but the delayed, retroactively-updated, and boiler-plated language in the reports suggests that either governments are non-responsive to critics or that critics lack a capacity to identify and call attention to limitations in the electronic surveillance reports which, in turn, facilitates inconsistent and unhelpful reporting.

Horizontal accountability practices, where external stakeholders examine information released by the government for the purposes of providing normative

---

Surveillance in Canada in the Post-Snowden Era (Ottawa: Ottawa University Press, 2015) 257 [Parsons, "Stuck on the Agenda"].

[61] Philippa Lawson, "Moving Toward a Surveillance Society: Proposals to Expand 'Lawful Access' in Canada", *British Columbia Civil Liberties Association* (2012), online: < https://bccla.org/wp-content/uploads/2012/03/2012-BCCLA-REPORT-Moving-toward-a-surveillance-society.pdf > ; Canada, Public Safety and Emergency Preparedness Canada, "Legislation to Modernize Investigative Techniques Introduced Today" (November 2005), online: < https://www.canada.ca/en/news/archive/2005/11/legislation-modernize-investigative-techniques-introduced-today.html?=undefined&wbdisable=true > ; Office of the Privacy Commissioner of Canada, "Response to the Government of Canada's 'Lawful Access' Consultations" (Ottawa: OPCC, May 2005), online: < https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_la_050505/ > ; Office of the Privacy Commissioner of Canada, , "Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the Current 'Lawful Access' Proposals", by Jennifer Stoddart et al. (Ottawa: OPCC, March 2011), online: < https://www.priv.gc.ca/en/opc-news/news-and-announcements/2011/let_110309/ > .

[62] Parsons, "Stuck on the Agenda", *supra* note 60 at 257.

feedback concerning the information's contents, similarly depend on the release of reliable information in the first place. Without a formal mechanism for external stakeholders to sanction the government, and with a dependence on other stakeholders (such as the media or sympathetic members of a legislative assembly) to place pressure on the government, any failure to release information exacerbates a profound information asymmetry.[63] External stakeholders often "crowdsource" analysis and critique, insofar as different stakeholders will focus on different governments' reports, often based on their geographic interests (e.g. British Columbia actors focus on reports pursuant to the provincial government's reports, whereas Ontario actors focus on the Ontario-related information). However, these stakeholders may not find it worthwhile to examine released information that is produced by either corporate or government actors if that information is insufficiently useful to be taken up into organizational practices. Without regularly issued reports, which adhere to standardized data requirements, being released with the intention of furthering particular policy goals, and which hold value for external stakeholders, there is a reduced likelihood that external parties will devote limited resources to ingest, analyze, and use data provided by the government.[64] Without this kind of use, the parties invested in horizontal accountability can neither serve to legitimize government practices or actively work to improve upon deficient or questionable ones.[65]

Over time, a combined inability or difficulty for legislators to engage in vertical accountability and for external stakeholders to engage in horizontal accountability raises the prospect of an accountability failure. Policy programs can be said to "fail" when they do not achieve what they were originally designed to do.[66] Given that the objective of annual electronic surveillance reports is to establish internal-to-government accountability through agency reporting to Ministers, as well as Ministerial accountability to their respective legislatures, accountability is not possible when there are chronic failures in data collection, tabulation, and issuance to the legislative bodies. These chronic issues are expressed, in part, through failures to regularly table reports, to consistently format reports, or to clarify why reporting matters in the context of agencies' surveillance activities. Given these factors, the policy driving the release of these reports is ostensibly failing in its desired outcomes.

---

[63] The authors note that they experienced this asymmetry in the course of conducting this research, insofar as some governments were not responsive to inquiries concerning their annual electronic surveillance reports. This asymmetry was only partially corrected following a media colleague contacting non-responsive governments with questions pertaining to their respective electronic surveillance reports. We note that, as of early 2018, not all governments were responsive even to our colleague, let alone to us.

[64] Fung et al., *Full Disclosure*, *supra* note 31.

[65] *Ibid*; Malena et al., "Social Accountability", *supra* note 22.

[66] Allan McConnell, "Policy Success, Policy Failure and Grey Areas In-between" (2010) 30:3 Journal of Public Policy 345.

To compound this problem, program failure in surveillance accountability regimes can be masked by what might simultaneously appear as a political success. While our account of electronic surveillance reports indicates chronic gaps and breakdowns in establishing conditions for accountability, the mere existence of a lawful requirement for vertical accountability can enhance the reputations of officials tasked with ensuring legitimacy of the programs. The presence of laws, which compel annual reports, projects a symbolic veneer of 'formalised accountability'. One the one hand this veneer presents an authoritative view of government dutifully fulfilling their regulatory role under liberal democratic arrangements while, on the other, there is a failure to meaningfully provide information that is a pre-requisite for the forms of accountability discussed in this article. Even in the most thoroughly detailed and regularly issued reports amongst our sample, the Federal reports, the statistics include a compilation of electronic surveillance that is conducted in the Canadian territories as well as by federal agencies across Canada more broadly. None of the reports, however, reveal this aggregation. Given that these reports are intended to provide a meaningful reflection of the surveillance activities of authorities, their current presentation prevents Canadians and persons studying the reports from understanding specifically where surveillance geographically takes place and, as such, inhibits the ability of federal and territorial legislators to understand the actual targeting of federal surveillance measures. The current arrangement of reporting on electronic surveillance threatens to create a misguided belief that existing institutions are both the most appropriate parties to conduct surveillance oversight and review, and that they are actually *conducting* such oversight and review. Most problematically, it does so largely vis-à-vis a democratically passed law which establishes a process of review but does not mandate the substance which would actually ensure that the review is undertaken seriously. In short, it presents a veneer of review without supplementing it with the substance of review.

The production of the annual electronic surveillance reports demonstrates governmental commitment to lawfulness, but lawfulness itself can operate as a deceptive yardstick for evaluating state practices designed to review lawful surveillance activities. Compliance with review requirements can be taken by government as a way of appearing to safeguard democratic liberties while actually doing little to inhibit surveillance and instead supporting its exercise.[67] Accountability reporting may similarly suffer when it is used to symbolize accountability and oversight — and thus a demonstration of liberal democratic norms in practice — while failing to substantively provide the accountability and oversight which is practically required to hold government to account for its

---

[67] Adam Molnar and Christopher Parsons, "Unmanned Aerial Vehicles (UAVs) and Law Enforcement in Australia and Canada: Governance Through 'Privacy' in an Era of Counter-Law?" in Randy K. Lippert, Kevin Walby, Ian Warren, and Darren Palmer, eds., *National Security, Surveillance and Terror: Canada and Australia in Comparative Perspective* (Palgrave MacMillan, 2017) 225-248.

exercise of state surveillance within a liberal democratic structure of government.[68] If the conditions for accountability are not being met in surveillance reports, as demonstrated in this article, the legislatively mandated 'act of reporting' might be more accurately described as a superficial or incomplete gesture of democratic safeguarding at the expense of a program that might otherwise more deeply inform the democratic process.

The deficiencies we have identified in the course of this research are neither necessary nor inevitable. Members of the government, legislators, and external stakeholders could undertake deliberate and collaborative efforts to close existing gaps and preclude future failures. To begin, the annual electronic surveillance reports are intended to help legislators understand the types, reasons, and efficacy of government surveillance but, as it stands today, comparing reports across jurisdictions is challenging at best. The federal government, working with its provincial counterparts, could take the lead to reform its own reporting systems as well as create a central repository that collates all Canadian governments' statistics and presents them alongside one another. Doing so would assist legislators in each jurisdiction to better understand how the activities of their own policing forces operate as compared to those in other jurisdictions, while clarifying whether increases or decreases in annual electronic surveillance warrants and interceptions were in line with national fluctuations. Regardless of whether the federal government was so tasked with aggregating reports from across Canada, legislation pertaining to the reports might be amended to require all policing bodies to affirmatively state the number of interception authorizations they requested each year. This would compel bodies to state that they had or had not sought such an authorization, and could eliminate existing confusions that emerge from provinces and the federal government modifying old reports to indicate a greater or lesser number of authorizations having been sought in a given year.

As discussed, governments of Canada include differing degrees of detail about the kinds of electronic surveillance which are carried out in any given year. Though the granularity provided by some reports does shed some light on the ways that policing and security agencies are using their lawful powers, the unevenness in this granularity simultaneously makes it challenging for readers to effectively compare reports against one another. One path forward would be for the Federal/Provincial/Territorial Coordinating Committee of Senior Officials (Criminal Justice): Cybercrime Working Group (FPT CCSO CWG) to develop an updated standard for reporting electronic surveillance statistics in a way that is adopted uniformly across all reporting jurisdictions. The FTP CCSO CWG has previously worked to develop suggestions pertaining to legislation which could authorize lawful access to Basic Subscriber Information,[69] as well as recommending ways of combating cyberbullying and the non-consensual

[68] Molnar, "(Il)liberal Democracy?", *supra* note 59.

[69] Government of Canada, "Lawful Access Implications of the Supreme Court Decision in *R. v. Spencer*" Public Safety Canada (December 2015) online: <https://www.scribd.-

distribution of intimate images.[70] Given its expertise, as well as its ability to coordinate across all jurisdictions, the group is well situated to review and evaluate all previously published electronic surveillance reports and subsequently issue recommendations to the governments for how to amend existing legislation in order to improve upon current statistical reporting. Their recommendations could also clarify and establish the kinds of information that must (or should) be included in narratives accompanying the annual statistics. Narratives might, as an example, include the number of instances where encryption or other technical characteristics foiled an attempted method of electronic surveillance, or whether there are difficulties in compelling private companies to conduct warranted electronic surveillance when compelled to do so, or other challenges facing law enforcement and security agencies.

Regardless of whether the federal and provincial governments amend existing practices to enhance comparability across governments' annual reports, there is also an important role for external independent evaluators. For instance, independent evaluators could examine governments' past annual reports, and also be expected to evaluate future reports. Specifically, these independent evaluators could examine the reports in a very similar fashion as to our own study in this article, that is, to scrutinize government actions that have led to a failure to issue reports, or which backdated reports in opaque ways. Information and privacy commissioners or another independent government auditor, or private consulting company, could be tasked with undertaking these reviews in order to ultimately restore trust in the veracity of the reports which were, and are, tabled by governments.

And finally, regardless of whether annual electronic surveillance reports are reformed or reviewed by external examiners, the reports ought to be made easily accessible to the public. Given that electronic surveillance is recognized as amongst the most intrusive forms of surveillance and, as such, requiring the highest degrees of oversight, control, and review, it is essential that governments throughout Canada make these reports easily available to the public so that they can understand the regularity, rationales, and efficacy of such surveillance. Without enhancing the public availability of these reports it is dubious that stakeholders external to government, such as academics, civil society organizations, or journalists, will be able to regularly compare and write about the nature and impacts of annually occurring electronic surveillance activities. If the current status quo persists, the government will not benefit from the policy insights external stakeholders might offer, such as ways to improve upon existing

---

com/document/342931031/Public-Safety-memos-on-warrantless-access> (unpublished).

[70] Canada, Coordinating Committee of Senior Officials Cybercrime Working Group, *Report to the Federal/Provincial/Territorial Ministers Responsible for Justice and Public Safety: Cyberbullying and the Non-consensual Distribution of Intimate Images*, (Ottawa: Department of Justice, June 2013), online: <http://www.justice.gc.ca/eng/rp-pr/other-autre/cndii-cdncii/pdf/cndii-cdncii-eng.pdf>.

reporting functions or to evaluate the government's actions as being just and appropriate and, thus, whether (and what) surveillance activities are legitimately a public good. Such legitimization is particularly important if citizens are to recognize their laws as functioning to appropriately secure the safety and security of society without unduly interfering with basic rights.

V. CONCLUSION

This article examined the extent to which Canadian governments' annual electronic surveillance reports can be used by legislators and external stakeholders alike to hold the government to account. It found that though there was not a primary gap in vertical accountability, insofar as there are laws compelling government to release these reports, there were extensive secondary vertical gaps stemming from failures to issue reports on an annual basis as required, a lack of standardization across jurisdictions, and a neglect on the part of governments to provide a narrative justification for the value of interception and surveillance powers. The same secondary gaps apply where external parties are engaged in horizontal accountability and are made worse because external stakeholders have no legal expectation that they can or will receive information about government electronic surveillance activities in an accessible format, thus creating a primary gap in horizontal accountability. When these issues are chronic, a policy gap can become a policy failure, insofar as the exceptions to the rule threaten to swallow the rule itself. We argue that such failures are manifest in the tabling, presentation, and explanation of the electronic surveillance reports studied. Unless these deficiencies are corrected, accountability reporting as a public policy instrument threatens to advance a veneer of political legitimacy at the expense of maintaining fulsome democratic safeguards designed to secure the freedoms associated with liberal democratic political systems. By adopting a range of policies such as updated statistical reporting models, aggregated statistics to support comparisons, enhanced narrative discussions in reports, or even just making the reports easily accessible to external stakeholders, the existing reporting instruments can be strengthened and used to enhance democratic values. However, the ongoing unwillingness or failure to more meaningfully account for government's use of electronic surveillance, however, may indicate the triumph of veneer over substance.

Future work in this area can focus on whether governments that declined to respond to our inquiries for their annual reports simply failed to respond to us, or instead did not table the reports in their respective legislatures at all. This might involve visiting libraries that hold different provinces' and territories' Hansards, or other government archives. Work could also include small-scale interviews with current and past legislators to understand whether these reports have ever been sought internally or used to hold government to account. Such work would clarify whether ongoing weaknesses in the reports, which lead to vertical and horizontal accountability gaps, are the result of legislators failing to use the reports, or rather the government's failure to modify them in response to

comments from legislators. Similar types of interviews could be done with members of civil society and the media to understand whether they have relied on the annual reports in their efforts to hold governments to account for their use of electronic surveillance. Another line of research into government surveillance accountability mechanisms might follow our prior work that attempted to understand and encourage private companies to disclose how, how often, and on what basis they disclose information to law enforcement and domestic security organizations.[71] Specifically, by working with legislators, publishing public letters, issuing Access to Information and Privacy requests, as well as other methods, we could encourage governments to evaluate the ease of, or possibility of, reforms into how governments report on the shifting technological dynamics of electronic surveillance. This approach would test the extent to which horizontal accountability might prompt change in government surveillance reporting behaviours.

Where annual accountability reporting is done irregularly, when there are challenges that inhibit understanding of the reported information or comparison across jurisdictions, and where the value of intrusive government actions is not explained clearly, accountability reporting has the potential to distort, extend, and distend information.[72] Similar to corporate reports that are meant to correct information asymmetries between firms and external stakeholders, accountability reports issued by government are unlikely to "correct information asymmetries, promote intended policy changes, or lead to alterations of behavior."[73] Given the number of proposals, especially following the revelations of Edward Snowden, for reforming surveillance legislation to clarify what constitutes democratically legitimated surveillance activities and make more apparent how often, and for what reasons and to what effects, foreign and domestic surveillance is undertaken, it behooves the academic community to understand the existing mandatory reporting systems in order to ensure that any new systems improve upon what exists today, as opposed to repeating mistakes of yore.

---

[71] See Christopher Parsons, "Beyond the ATIP: New methods for interrogating state surveillance" in Jamie Brownlee and Kevin Walby, eds., *Access to Information and Social Justice: Critical Research Strategies for Journalists, Scholars, and Activists* (Winnipeg: Arbeiter Ring Publishing, 2015); Parsons, "Voluntarily Produced Transparency Reports", *supra* note 50.

[72] Johnson, "Accountability in a House of Mirrors", *supra* note 23 at 136.

[73] Parsons, "Voluntarily Produced Transparency Reports", *ibid.*

APPENDIX 1

Request for Provincial Electronic Surveillance Reports

SUBJECT: Request for Annual reports on use of electronic surveillance

To Whom It May Concern,

I am an academic researcher at the Citizen Lab, Munk School of Global Affairs at the University of Toronto.

I would like to request copies of your province's Annual reports on the use of electronic surveillance, for the years 2005 to 2014. These reports are produced annually per section 195 of the *Criminal Code*. More information about what these reports include is available at Public Safety Canada's website, here: < http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2012/index-eng.aspx >

Could you provide me with copies (preferably electronic versions) of your province's reports dating back to 2005?

Best Regards,
Chris