Law Enforcement and Security Agency Surveillance in Canada:

The Growth of Digitally-Enabled Surveillance and Atrophy of Accountability

By Christopher Parsons[1]

[1] 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. This research was funded by the John D. and Catherine T. McArthur Foundation. Corresponding Author: Christopher@Christopher-Parsons.com

Governments have engaged in telecommunications surveillance since the earliest inception of publicly available communications tools. Letter mail, telegraphs, phone calls, text messages, and Internet communications have all been subject to surveillance.[2] Throughout the 20th century most Western governments have passed laws to restrict the state's ability to intrude into citizens' private lives and this tendency is as true in Canada as it is elsewhere. Perhaps most notably, following concerns in the 1960s and 1970s about the computerization of information and new ways of conducting electronic surveillance, the Government of Canada passed the *Protection of Privacy Act*.[3] The *Act*, as amended in 1977, established safeguards designed to protect Canadians' privacy by, in part, imposing mandatory reporting requirements on government agencies that engage in real-time electronic surveillance.[4] The intent of such laws was, and remains, to hold government agencies to account before their legislative assemblies and the citizenry more broadly for how such agencies intrude into the private sphere.

Fast forward to 2018, and state agencies have assumed and developed a wide range of new surveillance capabilities and been endowed with additional lawful powers. Vast volumes of information are stored as business records by private companies,[5] mobile device communications can be intercepted and select pieces of information extracted using a device capable of fitting inside a backpack or being mounted on the underbelly of airplanes,[6] Internet communications can be collected en mass for retroactive searching,[7] and more. Much of this surveillance constitutes 'bulk' surveillance, insofar a mass of digital data is collected by state agencies and is subject to analysis afterwards to understand the data's value. Despite the rise of these new technologies and creation of lawful powers to collect information for policing and security purposes there have been few accompanying reporting mechanisms. In effect, as ostensibly lawful state surveillance activities in Canada have expanded the requirements imposed on governments to account for their behaviour have atrophied.[8]

This chapter begins with a discussion of real-time electronic surveillance that has historically been conducted in Canada and the importance of government accountability for how law enforcement and security agencies (LESAs) conduct surveillance, as well as why such

---

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

[3] Stanley M Beck, "Electronic Surveillance and the Administration of Criminal Justice" (1968) 46:4 The Canadian Bar Review; Protection of Privacy Act, 1974.

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

[5] Daniel Solove. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.

[6] Parsons, Christopher; Israel, Tamir. (2016). "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," Citizen Lab – Telecom Transparency Project // CIPPIC. Available at: https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf

[7] See: Canadian SIGINT Summaries at https://christopher-parsons.com/writings/cse-summaries/

[8] Parsons, Christopher. (2016). "Transparency in Surveillance: Role of various intermediaries in facilitating state surveillance transparency," Centre for Law and Democracy. Available at: http://responsible-tech.org/wp-content/uploads/2016/06/Parsons.pdf

accountability is essential to the stability of democratic governance. It then proceeds to examine how such surveillance has been transformed in an era of digitization, and how contemporary surveillance simultaneously enables state actors to massively intrude upon Canadians' charter rights. It specifically notes how the atrophy of accountability regimes raise serious concerns for the democratic legitimacy of government surveillance activities. The chapter concludes by briefly outlining how surveillance accountability regimes might be rehabilitated and what such habilitation would mean for rendering government bulk surveillance activities more accountable to legislative assemblies and citizens alike.

1. The Threat of Real-Time Surveillance

Real-time government surveillance is perhaps most commonly thought of as a wiretap, with agents of the state listening intently on what the targets of the surveillance are saying and with whom the targets are communicating. Western governments tend to regard real-time surveillance more broadly, however, and in Canada it can assume many different forms, including audio and visual recordings, interception of communications, and planting of equipment designed to conduct surveillance in vehicles, homes, or businesses.[9] These kinds of surveillance tend to be regarded as deeply intrusive of private life on the basis that individuals reveal sensitive aspects of their lives while communicating with other persons, such as information about their sexuality, financial situation, medical issues, religious beliefs, or political leanings. Given these sensitivities, and the fact that there is a historical legal presumption that content is more revelatory than the metadata surrounding content (e.g. phone number dialed, place to which a letter is mailed, etc), criminal codes have tended to restrict government agencies' ability to engage in such intrusive surveillance.[10] 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."[11] This logic was adopted by the Canadian government when it established its own accountability and oversight regimes concerning electronic surveillance in the 1970s[12] with the passage and amendment of the *Protection of Privacy Act* during that decade.[13]

---

[9] Christopher Parsons and Adam Molnar. (Forthcoming). "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports," *Canadian Journal of Law and Technology*.

[10] As an example, the standards to obtain non-content information such as Internet routing information, or metadata associated with communications, tends to be lower as compared to the legal standard government agencies must meet to obtain interception orders or access to the content of communications. For an American perspective, see: John Villasenor. (2013). "What You Need To Know About The Third Party Doctrine," *The Atlantic*, https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/.

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

[12] Nicholas Koutros & Julien Demers, "Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement" (2013) 11:1 *Canadian Journal of Law and Technology*; Law Reform

Canadian LESAs must typically obtain a judicially authorized warrant before they can engage in real-time interception activities.[14] Such warrants operate as a control-based means of accountability, insofar as judges are situated to approve, approve with conditions, or deny the authorization request. Judges must be satisfied that the LESA officer in question has reasonable and probable grounds to believe that the real-time surveillance is necessary to advance an investigation, that affected persons have been identified, that all places the interception will take place have been disclosed, and that no other less intrusive mode of surveillance is available.[15] Furthermore, the *Protection of Privacy Act* also requires provincial and federal governments of Canada to prepare and table annual electronic surveillance reports that detail the frequency, reasons, and efficacy of real-time electronic surveillance. These reports provide accountability in the form of reviews which take place after the surveillance activities have been authorized by a judge and undertaken by the relevant LESA. A range of statistics are included in the reports, including the total number of requests for interceptions, how many such requests are granted, types of investigative methods employed, the regularity at which collected information is introduced as evidence, and number of times that the information is used in securing a conviction. Also included are the types of crimes for which real-time electronic surveillance warrants are authorized to investigate. There reports are tabled annually in the provincial and federal legislatures. Whereas control-based modes of accountability are concerned with the reasonableness and proportionality and necessity of electronic surveillance at the time of the request, review-based modes of accountability such as the annual electronic surveillance reports, are concerned with how the government more generally is undertaking such intrusive surveillance. The annual reviews do not focus on specific cases but, instead, on the efficacy of the surveillance in advancing investigations and ultimately securing convictions for different kinds of serious crimes.

Annual electronic surveillance reports are designed to ensure that the government minister responsible for agencies conducting such surveillance can be held accountable to legislators and, also, to the citizenry writ large. Accountability exists when "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

---

Commission of Canada, "Electronic Surveillance" *Department of Justice* (1986) online: <http://trove.nla.gov.au/work/18626452?versionId=45109635>; Morris Manning, *Wiretap Law in Canada: A Supplement to the Protection of Privacy Act, Bill C-176: An Analysis and Commentary* (Toronto: Butterworths, 1978).

[13] Stanley M Beck, "Electronic Surveillance and the Administration of Criminal Justice" (1968) 46:4 The Canadian Bar Review; Protection of Privacy Act, 1974.

[14] The exception to the rule is in the case of an emergency electronic surveillance operation; in such cases, the target(s) must be notified of the surveillance after the fact and a justice may authorize the surveillance for up to thirty-six hours without the LESA officer(s) having to prepare a completed warrant.

[15] Nicholas Koutros & Julien Demers, "Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement" (2013) 11:1 *Canadian Journal of Law and Technology*; *Criminal Code*, RSC 1985, s. 184-186.

or institution provide information of justification for its actions."[16] In effect, this means that when a government agency or Minister is compelled to provide information to another body, and that body can sanction the agency or Minister based on its provision of information, then an accountability framework exists. This kind of directed accountability conforms to a traditional understanding of accountability, where an actor that is accountable to a forum, for particular activities or actions, and where the forum could discipline the actor if they fall short of expected activities or actions.[17] This traditional approach to understanding accountability regimes stands in contrast to the broader literature on accountability which is focused on understanding how governmental accountability more broadly operates in an era where private actors assume roles and responsibilities that have historically been undertaken by states.[18] In the case of real-time electronic surveillance it is ultimately a governmental LESA which obtains the warrant for the activity and, thus, even should there be assistance from a non-government party, that assistance is the direct result of being judicially compelled to cooperate with the government agency in question.

Annual electronic surveillance reports facilitate traditional modes of accountability in at least two ways. First, in preparing the reports the relevant ministers who will table the reports will become aware of what their agencies have done and, in the process, be better able to direct and control their behaviours.[19] Receiving this information is essential for Canadian ministers to assume responsibility for their agencies and be able to correct deficient or problematic behaviours. Second, legislative assemblies can ask questions of the minister when the reports are tabled as required each year. Questions might be raised concerning whether the surveillance capabilities are useful in collecting evidence to secure convictions or why there were significant increases or decreases in the numbers of affected persons from one year to the next. Using information in the annual reports, legislators can try and determine "whether the government is judiciously 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."[20]

There are significant limitations associated with the accountability reporting concerning real-time electronic surveillance in Canada. Reports are often not tabled on a regular basis, the actual formatting of those reports can be so variable as to frustrate comparative analyses (both within and across jurisdictions), statistics can be irregularly updated and call into question the

---

[16] Riccardo Pelizzo & Frederick Stapenhurst, Government Accountability and Legislative Oversight (New York: Routledge, 2013) at 2.
[17] Richard Mulgan, "The Processes of Public Accountability" (1997) 56:1 Australian Journal of Public Accountability; Jonathan Anderson, "Illusions of Accountability" (2009) 31:3 *Administrative Theory & Praxis*.
[18] Colin Scott, "Accountability in the Regulatory State" (2000) 27:1 *Journal of Law and Society*.
[19] Adam Przeworski & Susan C Stokes, *Democracy, Accountability, and Representation* (Cambridge: Cambridge University Press, 1999); Kaare Strøm, "Parliamentary Democracy and Delegation" in Kaare Storm, Woldgang C Muller and Torbjorn Bergman, eds, *Delegation and Accountability in Parliamentary Democracies* (New York: Oxford University Press, 2003) 55.
[20] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Citizen Lab*, http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

veracity of any information which is presented to legislative assemblies, and the narrative sections of the reports which explain and contextualize the reported year's activities are sometimes missing or are simply copies of the same statement year over year.[21] Moreover, it isn't self-evident that legislators, independent members of government, civil society organizations, or academics have comprehensively examined the reports on any kind of regular basis.[22] Nevertheless, these annual electronic surveillance reports represent the most comprehensive kinds of review of government surveillance activities. As discussed in the subsequent sections, despite all of their flaws, these rarely-read reports constitute the gold standard of government surveillance accountability in Canada.

2. The Digitization of Surveillance

As we have embraced the digital era in our personal and professional lives, LESAs have also developed new techniques and gained additional powers in order to keep pace as our memories have shifted from personal journals and filing cabinets to blogs, social media, and cloud hosting providers. LESAs now subscribe to services designed to monitor social media services for intelligence purposes,[23] they collect bulk data from telecommunications providers in so-called 'tower dumps' of all the information stored by cellular towers,[24] establish their own fake cellular towers to collect data from all parties proximate to such devices,[25] use malware to intrude into either personal endpoint devices (e.g. mobile phones or laptops) or networking equipment (e.g. routers),[26] and can even retroactively re-create our daily online activities with assistance from Canada's signals intelligence agency.[27] In the past, each of these kinds of

---

[21] Christopher Parsons and Adam Molnar. (Forthcoming). "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports", *Canadian Journal of Law and Technology*.
[22] Christopher Parsons and Adam Molnar. (Forthcoming). "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports", *Canadian Journal of Law and Technology*.
[23] Patrick McGuire. (2015). "Toronto Police Chief Bragged About Monitoring Protesters and Anonymous Is Pissed", *Vice*, March 19, 2015, https://www.vice.com/en_ca/article/dpk5am/watch-torontos-police-chief-brag-about-spying-on-political-protesters-263.
[24] R. v. Rogers Communications, 2016, ONSC 70; see also: Shannon Kari. (2017). "The new surveillance state," *Canadian Lawyer*, October 2, 2017, http://www.canadianlawyermag.com/author/shannon-kari/the-new-surveillance-state-13735/.
[25] Christopher Parsons and Tamir Israel. (2016). "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," *Citizen Lab // CIPPIC*, https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf. See also: 2017 FC 1047.
[26] Based on conversations between author and members of Canada's federal and provincial governments. See also: Adam Molnar, Christopher Parsons, and Erik Zouave. (2017). "Computer network operations and 'rule-with-law' in Australia," *Internet Policy Review* 6(1).
[27] This involves a federal LESA obtaining stored content or metadata from the Communication Security Establishment's (CSE) bulk content and metadata stores under part C of the CSE's mandate under the *National Defence Act* or the Technical and Operational Assistance part of the CSE's mandate should Bill C-59 (An Act respecting national security matters) pass into law without significant modifications to its text after being introduced for first reading in mid-2017. For more, see: Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert. (2017). "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading (December 18, 2017)," *Citizen Lab // CIPPIC*, https://citizenlab.ca/wp-content/uploads/2017/12/C-59-Analysis-1.0.pdf, p 32-35.

activities would have required dozens or hundreds or thousands of government officials to painstakingly follow persons -- many of whom might not be specifically suspected of engaging in a criminal activity or activity detrimental to the national security of Canada -- and gain lawful entry to their personal safes, install cameras in their homes and offices, access and copy the contents of filing cabinets, and listen in on conversations that would otherwise have been private. So much of our lives have become digital that entirely new investigative opportunities have arisen which were previously restricted to the imaginations of science fiction authors both insofar as it is easier to access information but, also, because we generate and leave behind more information about our activities vis-a-vis our digital exhaust than was even possible in a world dominated by analog technologies.

Each of the aforementioned kinds of digital surveillance open novel investigative lines for LESAs. In the case of monitoring social media services, LESAs can track protests to understand who is central to creating or amplifying messages, develop a social networking map of persons who are directly involved (e.g. marching in a protest or participating digitally) as well as those who are affiliated (e.g. sharing or amplifying messages in support of the protest, while not being directly involved in it), as well as those who respond positively or negative to the messaging. What once would have required placing officers in a crowd and taking photos of participants to subsequently identify them can be done by paying a third-party to harvest the data and deliver it in real-time or in after-action reports at a fraction of the cost associated with deploying masses of officers. In collecting bulk data from telecommunications providers' cellular towers, LESAs can identify which mobile devices were proximate to the towers during the times requested. Quite often this data is released on a relatively low standard of reason to suspect, is for data stored by multiple towers, and can compel telecommunications companies to disclose data on tens or hundreds of thousands of customers with each request. To engage in a similar kind of retroactive surveillance in an analogue era, the government would have to install cameras or other recording devices throughout every room, public space, and vehicle and subsequently task hundreds or thousands of officers to determine who was in what location, at what time. Using tower dump orders, they can compel telecommunications providers to provide similar kinds of data at a fraction of the cost. And where the government decides to collect mobile device identifiers without the assistance of a mobile telecommunications provider, it can do so using its own IMSI Catcher devices. Such devices compel all mobile devices within range to connect to the given IMSI Catcher and, subsequently, provide a series of unique identifiers that the LESA can then bring to telecommunications carriers to identify the persons who have registered the devices. Such surveillance devices are sometimes used in cases where government agents believe that a suspect, or suspects, are using mobile devices but lack the identifiers associated with them; these devices can also potentially be used to identify all persons at a protest, those proximate to a VIP such as a government dignitary, or even to deliver malware to mobile devices which connect to the IMSI catcher in order to subsequently access content on their devices. Each of these kinds of activities would be time consuming -- and likely quite

obvious to those affected -- were officers required to manually inspect devices or request the identities of persons proximate to the area of surveillance.

There are also a range of ways in which LESAs can retroactively acquire information about communications, activities, and engagements that are communicated using digital technologies. First, LESAs can obtain a production order and serve it on private companies which are in the business of retaining this information for their own commercial purposes. Sometimes data is retained because such retention is part of why citizens use the service in question: email services, as an example, have made a business of keeping our mail for us. The same is true of cloud storage providers, such as Apple, Amazon, Dropbox, or Google, all of which can provide LESAs with access to their customers' stored records after receiving a lawful request from a LESA. But this is only the most obvious source of retroactive records. In the second category, Western intelligence agencies such as the National Security Agency and Canada's own Communications Security Establishment (CSE) collect vast quantities of data about foreign persons as well as citizens of their own countries and residents of those countries. Such data can potentially be accessed by non-intelligence parties, such as security agencies like the Canadian Security Intelligence Service (CSIS), or law enforcement agencies, such as the Royal Canadian Mounted Police (RCMP), should those parties make formal and lawful requests for some of the bulk data which is collected by the CSE. In Canada, the CSE has capabilities that far exceed those of any other federal agency insofar as it is lawfully authorized to engage in surveillance activities that no other LESA can engage in. Moreover, the CSE can develop systems of surveillance that no other agency is competent, let alone legally permitted, to create. Such systems include, as examples, those which monitor the Internet writ large for file downloads, monitor metadata associated with our digital movements to populate vast databases which can subsequently be queried to understand every place we've been online and many of the people we've communicated with, or track a vast swathe of the data which is sent into, and exits from, all Canadian networks. Once these systems collect data and store them in the CSE's databases, the RCMP or CSIS can obtain a warrant to compel the CSE to disclose data pertaining to its suspects or activities named in the warrant. And, depending on the warrant, the CSE can even delve into its partner intelligence agencies' databases in Australia, New Zealand, the United Kingdom, or the United States and query those foreign systems for information which is relevant to the warrant. This is a kind of surveillance that is grossly in excess of what any LESA in Canada could do in the past, let alone today with its own independent surveillance capabilities.

LESAs have a range of legal instruments which provide the requesting agency a right to attempt to obtain the data they want to further their investigation. There are, however, a set of instruments which are more commonly used in the course of their investigations. Preservation demands can be issued on companies which process information and, upon receipt, compel the companies to store the identified data for 21 days for domestic offences and 90 days for international offences. LESAs must subsequently obtain and serve a production order on the company to gain access to whatever has been preserved. Where the data is normally retained in the course of business, such as subscriber data records pertaining to a user of a company's

services or the email or other documents the customer stores with the company in question, then a LESA might only obtain and serve a production order to obtain all of the historical documents denoted in the court order. The produced data can be deeply revealing given that it may include the content of digital communications and activities, yet the production order can be obtained after meeting a reasonable ground to suspect standard. Number dialer orders can also be obtained on grounds to suspect that the collected information will assist in the investigation of an offence that is suspected will be, or has been, committed. Such orders are used to collect the numbers which are dialed from, and to, specified devices and can reveal more than just phone numbers: where a mobile phone is used for banking to input account numbers, or to enter passwords to enter conference calls, or to otherwise interact with a phone-based computer system, the number dialer warrant will authorize the collection of such information.

In 2014 the *Criminal Code* was amended to, in part, establish three different types of tracking. One type is used to track objects (e.g. motor vehicles or mobile devices) and another for tracking transmission data (e.g. data which is emitted from devices and which can be used to track the device(s) in question). Either of these types of tracking orders can be obtained on grounds that the LESA suspects that the privacy invasion will assist in the investigation of an offence. The third type of transmission order is used to track individuals and is obtainable on a higher standard, where the LESA has a belief that the privacy invasion will assist in the investigation of an offence. As noted, previously, interception orders are granted exclusively on reasonable grounds to believe that the overseeing justice has been satisfied that the real-time surveillance is necessary to advance an investigation, that affected persons have been identified, that all places the interception will take place have been disclosed, and that no less-intrusive mode of surveillance would produce evidence needed for the investigation. And finally, there is a broad category to catch many of the most controversial kinds of government surveillance, general warrants. Such warrants tend to be difficult to obtain, insofar as the LESA officers in question must demonstrate there are reasonable grounds to believe that an offence has been, or will be, committed and that relevant information can be obtained using the methods described in the general warrant application. Surveillance techniques such as IMSI Catchers, malware, and other activities which are not better captured by other powers denoted in the *Criminal Code* or other act of parliament have tended to rely on general warrants to authorize LESA activities.

Due to the relatively high standard which must be met before a LESA can obtain an interception order, agencies tend towards using alternate surveillance methods to conduct their operations. As an example, in 2014 the federal government and provincial governments obtained 250 court orders that authorized their respective agencies to engage in real-time surveillance.[28] By contrast, a subset of telecommunications providers which operate exclusively in Canada

[28] Based on the author's collection of Annual Electronic Surveillance Reports tabled by federal and provincial governments. Note that several provincial governments did not issue their statutory reports in 2014, or otherwise did not make the information available to the public, legislators, or the author.

reported receiving 81,443 court orders or warrants;[29] this number does not reflect orders issued to cloud service providers, social media companies, hotels, insurance companies, or even all telecommunications providers which operate in Canada. Nevertheless, the juxtaposition does indicate that real-time electronic surveillance accounts for a small fraction of the surveillance activities which are conducted by government agencies. Only real-time electronic surveillance must be tabulated in annual reviews to legislative assemblies, and federal and provincial agencies have historically been unwilling or unable to independently collate statistics on their use of other warranting methods,[30] even to advance their own arguments for increased surveillance powers.[31]

3. The Perils of Contemporary Canadian Surveillance Activities

While the public knows about many of the government's contemporary surveillance techniques and technologies, this knowledge has only followed from persistent, ongoing, and challenging research endeavors undertaken by academics, journalists, members of civil rights organizations, and as a result of whistleblowers. One of the most commonly used techniques by all of the aforementioned groups -- save for whistleblowers -- is reliance on freedom of information (FOI) laws to compel government agencies to disclose information pertaining to different surveillance devices and techniques. Unfortunately, many Canadian LESAs have adopted stances that any revelation of techniques which are not widely disclosed to the public would have deleterious impacts on the future use of those techniques and operation of associated devices. This has meant, as an example, that knowledge about the operation of IMSI Catcher devices in Canada was stymied for years as government agencies alternatively denied they had any knowledge of the devices (partially on the basis that the agencies referred to the technologies as Mobile Device Identifiers instead of IMSI Catchers[32]) or that any disclosure of whether they did or didn't use the devices would hinder investigative practices.[33] Indeed, given the challenges in learning about government surveillance capabilities and the regularity at which such capabilities are used, researchers have entered into collaborations with parliamentarians to compel agencies to explain their surveillance activities, brought legal challenges against federal

---

[29] Parsons, Christopher. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," Telecom Transparency Project. Available at: http://www.telecomtransparency.org/release-the-governance-of-telecommunications-surveillance/; p. 45-56.

[30] Minister of Public Safety and Emergency Preparedness's Responses to MP Charmane Borg's Q-233 Order Paper Questions, March 24, 2014, retrieved January 17, 2015, https://www.christopher- parsons.com/Main/wp-content/uploads/2014/03/8555-412-233.pdf.

[31] See Access to Information and Privacy document released by Public Safety Canada, A-2011-00220.

[32] Based on discussions between the author and Canadian investigative reporters.

[33] See: Israel, Tamir and Parsons, Christopher (for Open Media). (2016). "Written Inquiry Under Part 5 of the Freedom of Information & Protection of Privacy Act ("FIPPA) of British Columbia: In re: Vancouver Police Department," Office of the Information and Privacy Commissioner of British Columbia, March 2016.; Parsons, Christopher; Israel, Tamir. (2016). "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," Citizen Lab – Telecom Transparency Project // CIPPIC. Available at: https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf, pp. 31-49.

and provincial governments of Canada which have led to government agencies producing internal documents in the course of legal discovery processes, encouraged corporations to explain how they are compelled to provide information and assistance to LESAs, incited the public to try and learn about whether and if so how they have been subject to surveillance, and issued complaints to independent officers of parliament so that they will launch investigations and reveal information concerning LESA activities.[34]

One of the reasons that such a varied set of practices must be used to understand the breadth of LESA's surveillance activities stems from the ability of government prosecutors to invoke sections of the *Canada Evidence Act* in the course of criminal tries. Such successful invocations limit the defendant, their defense lawyers, and the public from understanding the methods and techniques that were used to collect evidence introduced in a case. Such an invocation follows when the Crown believes that the disclosure of specific information would either be injurious to the public interest[35] or to international relations, national defense, or national security.[36] If defense attorney's do not challenge such invocations, or if they are unsuccessful in their challenge to compel the Crown to disclose information it is attempting to suppress, then no court record of the technique or device(s) being used will be generated. As a result of the government's often aggressive efforts to mask its less-publicized methods of surveillance, this means that the aforementioned parties of academics, journalists, and civil rights advocates must use a range of atypical processes to ascertain what LESAs are doing in the course of exercising their lawful authorities.

Citizens cannot appreciate the extent to which LESAs may be intruding into their private lives if they are unaware of the existence of government surveillance techniques and devices, let alone the regularity of their operation. Potentially thousands of persons have their information collected in the course of LESA social media analytics, police requests for tower dump information from cellular providers, IMSI Catchers being operated within a kilometer or two of a person's location, authorities' use malware to target routing equipment, or the CSE's mass, global, surveillance activities that capture Canadian and non-Canadian persons' information alike. All of the aforementioned modes of mass surveillance are conducted without accountability regimes which correspond with that linked to real-time electronic surveillance, and which is designed to make the LESAs accountable to legislative assemblies or to the public. The only time when an affected person is likely to realize their information has been collected using one of these contemporary means of surveillance is when they might be charged with an offence and subsequently has information entered into evidence. Outside of this situation they may never know that their life chances have been affected or are at risk as a result of the government's intrusion into their private lives. Contrasted against the accountability regimes which were created concerning real-time electronic surveillance, and which include annual reports to legislative assemblies and notifications to persons affected by the surveillance

[34] Parsons, Christopher. (2015). "Beyond the ATIP: New methods for interrogating state surveillance," in Jamie Brownlee and Kevin Walby (Eds.), Access to Information and Social Justice (Arbeiter Ring Publishing).
[35] *Canada Evidence Act*, S. 37.
[36] *Canada Evidence Act*, S. 38.

regardless of whether a criminal charge is laid, and the lack of equivalent regimes for today's dominant tools of surveillance reveal a significant shift in the treatment of Canadians' privacy rights.

There are significant risks associated with these new surveillance technologies and powers without a correspondingly robust accountability regime. Specifically, many of the aforementioned new power, such as the receipt of tower dump information, operation of IMSI Catchers, deployment of malware, or bulk collection of Canadians' digital activities vis-a-vis the CSE, are all highly secretive activities: evidence may be suppressed in court proceedings or, alternately, may be used to secretly influence targets' life chances by a security agency which does not have to disclose to persons it targets how it has received or used the acquired information. Furthermore, the very laws which authorize these investigative techniques are often unclear to lawyers, let alone parliamentarians or the general public: general warrants, tracking orders, and production orders can be used to exercise the aforementioned powers, but it is exceedingly rare that the debates surrounding the passage of those laws include reference to the specific techniques used by LESAs today.[37] In many cases the techniques didn't even exist at the time the legislation was debated and subsequently passed into law, and parliamentarians have no mechanism to understand how previously passed legislation is being used to intrude into private life. Without a mechanism to alert them of how old laws are being used in new ways, legislators remain unaware of whether debates are even required about how LESAs are (ab)using the old law in the course of their contemporary investigative efforts, or whether new laws are needed to authorize entirely new kinds of investigative techniques.

A key risk associated with the new techniques of surveillance, then, is associated with the fact that such techniques and corresponding activities rest on laws or interpretations of laws that parliamentarians and the public alike could not have been said to have legitimated. Without understanding the implications of law, citizens cannot be said to have reasonably approved a law through the activities of the political representatives. This is not to say that citizens must *agree* that the legislation in question should have been passed into law but, instead, that they should *understand* how a given law is associated with activities which intrude into their private lives. The opacity of secretive digital investigative techniques and their legal justifications effectively "function outside of the scope of citizen-authorization and separate the government's actions from the actions of citizens. Instead of citizens being at the center of democratic power, they become serfs who are protected by their government."[38] In effect, while the surveillance activities undertaken by government may be said to be lawful -- they are justified under the auspice of legislation passed by legislative assemblies -- they cannot be said to be legitimate, on

---

[37] During Committee hearings for *Bill C-13 (An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act)* parliamentarians reacted with open shock that aspects of the bill would authorize LESAs to target motor vehicles with malware. This was raised by the Canadian Civil Liberties Association; no member of government who was called to testify alerted committee members to this element of the legislation.

[38] Parsons, Christopher. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," Telecom Transparency Project. Available at: http://www.telecomtransparency.org/release-the-governance-of-telecommunications-surveillance/, p. 83.

the basis that neither the legislative assemblies which passed the legislation nor the citizens who are affected by the law can perceive the link between the law as passed and the activity as undertaken.[39] This gap between lawfulness and legitimacy threatens to separate the lawful from the legitimate activities of government and, in the process, promote distrust in governmental activities, the value of legislators and legislative assemblies, and potentially chill Charter rights of speech and association, amongst others, as citizens avoid engaging in activities that are lawful but fall outside of the norm.[40]

4. Rehabilitating Surveillance Accountability

The current impoverishment of surveillance accountability as it relates to the Government of Canada's investigative powers in a digital era is the direct result of successive governments introducing legislation that expands the state's capabilities to intrude into private life without the legislation also including corresponding robust accountability regimes. But the current state of affairs is also the result of how members of opposition parties and civil society organizations have sought to limit the government's ability to intrude. In the case of new powers introduced in *C-13 (An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act)*, civil society organizations fought a decade-long campaign to prevent the LESAs from obtaining powers which would authorize certain kinds of warrantless surveillance or compel private companies to develop surveillance-supportive communications infrastructures.[41] More recently, the same classes of parties have tried to delimit the abilities of the CSIS to use newly gained powers to violate Canadians' Charter rights[42] as well as argue against the CSE from obtaining powers which could be used to further collect information about Canadians and persons in Canada, amongst other classes of powers.[43] Only recently, in the case of legislation which may extend the CSE's capabilities, have there been strong calls for a robust accountability regime to be baked into the CSE's actual use

---

[39] Jürgen Habermas. (1998). "On the internal relation between the rule of law and democracy." In C. Cronin and P. De Greiff (Eds), *The Inclusion of the Other: Studies in Political Theory* (pp. 253-264). Cambridge, MA: MIT Press.
[40] Jonathon W. Penney. (2017). "Internet surveillance, regulation, and chilling effects online: a comparative case study," *Internet Policy Review* 6(2); Jonathon W. Penney. (2016). "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal* 31(1).
[41] Parsons, Christopher. (2015). "Stuck on the Agenda: Drawing lessons from the stagnation of 'lawful access' legislation in Canada," Michael Geist (ed.), Law, Privacy and Surveillance in Canada in the Post-Snowden Era (Ottawa University Press).
[42] Craig Forcese and Kent Roach. (2015). *False Security: The Radicalization of Canadian Anti-Terrorism*. Toronto: Irwin Law.
[43] Parsons, Christopher; Gill, Lex; Israel, Tamir; Robinson, Bill; and Deibert, Ron. (2017). "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading (December 18, 2017)," Citizen Lab // CIPPIC. Available at: https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf; British Columbia Civil Liberties Association. (2018). "Written Submissions of the British Columbia Civil Liberties Association ("BCCLA") to the Standing Committee on Public Safety and National Security regarding Bill C-59, *An Act respecting national security matters,*" Standing Committee on Public Safety and National Security; Canadian Civil Liberties Association. (2018). "Submission to the Standing Committee on Public Safety and National Security regarding Bill C-59, *An Act respecting national security matters*," Standing Committee on Public Safety and National Security.

of those powers;[44] this is, in part, based on the fact that the proposed legislation includes suggestions for accountability reform as well as a more prominent effort to include publicly accessible review-based accountability that parallel those of Canada's closest intelligence allies in the legislation as introduced at first reading.[45]

Broadly, surveillance accountability can be restored following study to understand the kinds of annual reporting that are appropriate to the different kinds of activities. Such reporting could subsequently be used to better appreciate the actual activities that are carried out to ensure the peace, order, and good government in Canada and, where appropriate, expand or curtail the activities in question by way of legislation. In the case of existing deficiencies with electronic real-time surveillance reporting, which include problems tabling reports annually as required under the law as well as reports not being comparable year-over-year or across jurisdiction, the reports themselves might be reviewed and updated to clarify how agencies are to compile and present statistics. The legislation which sets out what must be in these reports has not been updated since the mid-1970s and it is perhaps appropriate over forty years later to reflect on what is working well, what needs improvement, and whether additional granularity is required in the presented statistics. In the case of surveillance activities which are not currently subject to a dedicated annual review process, legislation might be passed which would require LESAs to provide details about the kinds of investigative activities they are involved in and the legislation which authorizes such activities. Such details need not specify specific models of equipment or versions of software being employed to conduct lawful surveillance but should, at a minimum, provide actionable and specific information concerning the activities. With this in mind, it likely would be appropriate to declare that the RCMP collected identifiers from mobile devices using IMSI Catchers and that the devices had an effective working range of five hundred meters to five kilometers, but not necessarily the parties from whom the RCMP purchased its devices, the versions of the devices used, and so forth. This revelation of capability would parallel that which already exists concerning real-time electronic surveillance: the *Criminal Code* is explicit in the different kinds of real-time surveillance which might be undertaken and the revelation of these capabilities has not caused them to lose their investigative value.

It may sometimes be challenging to establish an appropriate review format. In the case of production orders, as an example, which can be used to compel documents from any organization from a hotel to a gas station to an Internet company, it may be important to clarify

---

[44] Parsons, Christopher; Gill, Lex; Israel, Tamir; Robinson, Bill; and Deibert, Ron. (2017). "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading (December 18, 2017)," Citizen Lab // CIPPIC. Available at: https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf; Christopher Parsons and Adam Molnar. (2017). "Horizontal Accountability and Signals Intelligence: Lesson Drawing from Annual Electronic Surveillance Reports," *SSRN*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047272; Communciations Security Establishment Commissioner. (2018). "Substantial Proposals Regarding the Intelligence Commissioner's Role," Standing Committee on Public Safety and National Security; Pierre Blais and Chantelle Bowers. (2018). "Speech for Bill C-59: Presented to the Standing Committee on Public Safety and National Security (SECU)," Standing Committee on Public Safety and National Security.

[45] Cat Barker, Claire Petrie, Joanna Dawson, Samantha Godec, Holly Porteous, and Pleasance Purser. (2017). "Oversight of Intelligence Agencies: A Comparison of the 'Five Eyes' Nations," *Library of Parliament*.

the kinds of businesses or organizations which receive such orders, the volume(s) of records requested, and the kinds of records requested. But each of the aforementioned categories would admittedly be challenging to establish given the wide breadth of possible records that might be sought by a LESA in the course of its investigation. Such difficulty, however, should not prevent legislators and external to government stakeholders from engaging in the hard work of rebuilding Canada's accountability frameworks pertaining to government surveillance activities.

5. Potential of Surveillance Accountability

But perhaps what is most important is that there are clear assertions of which laws are being used to engage in what kinds of activities. Such explanations are important for at least two reasons. First, they would help to close the gap between the lawfulness of activities and the legislative branch's legitimization of the activities in question: should it become apparent that general warrants are being heavily relied on for a given type of surveillance it would be better understood how there was a link between law and intrusive government practices. Second, where the government adopted an interpretation of legislation that varied significantly from that of the parties who drafted the legislation, a political contest could arise surrounding the appropriateness (and, correspondingly, lawfulness) of the interpretation in question. In the United States, a legislative effort to restrict how the National Security Agency could obtain business records in the course of engaging in intelligence activities was ultimately interpreted by government lawyers to *expand* the numbers of business records which the Agency could collect.[46] The government's (mis)interpretation of Congress' will only came to light following revelations associated with Edward Snowden's disclosures about intelligence activities undertaken by the National Security Agency and its closest national and international partners. By compelling the government to explain how it is interpreting law a bridge can be built between lawful activity and legitimate activity, thus better empowering LESAs in Canada to act with the broader consent of the public.

As an added advantage to government, external parties can evaluate the appropriateness of the exercise of lawful power (in terms of activities conducted) as well as the legal soundness linked with using certain techniques and devices under particular parts of the *Criminal Code* and other Canadian laws. These evaluations can lead government agencies to realize that there are more appropriate techniques to conduct investigations or legal avenues which would better ground the techniques being used. In the former case, if external parties can identify less intrusive measures to conduct the same kinds of investigations then LESAs could carry out their activities in even more rights-protective manners and, in the process, better secure citizens' rights by intruding upon them in a more restricted manner. In the latter case, if external parties identify more appropriate laws which should be used to authorize LESA activities this can have a

[46] F. James Sensenbrenner, Jr. (2013). "Brief Amicus Curiae Of Congressman F. James Sensenbrenner, Jr. in Support of Plaintiffs," ECF Case No. 13 Civ. 3994 (WHP), https://www.eff.org/document/aclu-v-clapper-amicus-brief.

direct impact on the strength of the investigations and criminal cases which emerge from these investigations. In effect, by identifying the best laws to rest different techniques on, LESAs can adopt stronger legal arguments that they are, indeed, authorized to carry out different techniques and thus reduce the likelihood that an investigation is for naught when evidence or information collected is thrown out of court or ordered deleted on the basis that it was collected under an inappropriate legal standard or based on a flawed legal theory.

The rehabilitation of surveillance accountability can thus better ground the lawfulness of LESAs' surveillance activities while, at the same time, more firmly establishing the democratic legitimacy of the activities in question. Bridging the gap between lawfulness and legitimization would not necessarily restrict the actual kinds of surveillance which are being undertaken: it may simply reassure legislators and the public of the appropriateness of existing activities and operations. Admittedly, any accountability regime will impose an additional fiscal and operational burden on agencies interested in conducting surveillance operations, especially those which have the potential to massively intrude into the private lives of Canadians and persons in Canada. But such accountability requirements were imposed on government agencies in the 1970s when they used what was, at the time, the most intrusive form of activity: real-time electronic surveillance. The principles of the 1970s are as applicable today as they were then. All that is lacking is the political will to apply these principles in the service of expanding Canada's surveillance accountability regime. Should this political will not manifest, and should LESAs continue to expand the scope of their digital surveillance activities without providing clarity as to how often they exercise their powers, for what reasons, to what effect, and at what economic and Charter-rights cost, then the gap between lawfulness and legitimization will only continue to widen to the detriment of Canada's democracy.