Do Transparency Reports Matter for Public Policy?

Evaluating the effectiveness of telecommunications transparency reports

By Christopher Parsons[1]
Postdoctoral Fellow and Managing Director of the Telecom Transparency Project
Citizen Lab, Munk School of Global Affairs at the University of Toronto

Draft Version 1.5 :: January 13, 2015

Abstract:
Telecommunications companies across Canada have begun to release transparency reports to explain what data the companies collect, what data they retain and for how long, and to whom that data is, or has been, disclosed to. This article evaluates the extent to which Canadian telecommunications companies' transparency reports respond to a set of public policy goals set by civil society advocates, academics, and corporations, namely: of contextualizing information about government surveillance actions, of legitimizing the corporate disclosure of data about government-mandated surveillance actions, and of deflecting or responding to telecommunications subscribers' concerns about how their data is shared between companies and the government. In effect, have the reports been effective in achieving the aforementioned goals or have they just had the effect of generating press attention?

After discussing the importance of transparency reports generally, and the specificities of the Canadian reports released in 2014, I argue that companies must standardize their reports across the industry and must also publish their lawful intercept handbooks for the reports to be more effective. Ultimately, citizens will only understand the full significance of the data published in telecommunications companies' transparency when the current data contained in transparency reports is contextualized by the amount of data that each type of request can provide to government agencies and the corporate policies dictating the terms under which such requests are made and complied with.

---

[1] I can be contacted at Christopher@Christopher-Parsons.com, and welcome any feedback you may have on this draft paper. My work is funded by the Social Science and Human Research Council (SSHRC) as well as by the Canadian Internet Registration Authority (CIRA), and supported by the Munk School of Global Affairs at the University of Toronto.

We're building something here detective, we're building it from scratch. All the pieces matter.
- Lester Freamon, The Wire

Pressure has built on Canadian telecommunications companies to release 'transparency reports' which detail how often the companies disclose information about their subscribers to government agencies. The pressure has been created as a result of reports issued by independent officers of parliament, formal questions raised by parliamentarians, and public letters written by academic researchers and civil society organizations. And these efforts compounded the pressures placed on these companies following Edward Snowden's revelations that Canadians' telecommunications data were being monitored by signals intelligence agencies.[2] As a result of these pressures Canadian companies have begun publicly explaining what data they collect, their reasons for the collection, their rationale for storing it, and the terms and regularity at which data is disclosed to government.

This article examines the effectiveness of Canadian telecommunications companies' 2014 transparency reports in achieving a set of public policy goals. These goals include enhancing Canadians' understanding of existing government surveillance practices, legitimizing the corporate disclosure of data about government-mandated surveillance, and deflecting or responding to telecommunications subscribers' concerns about how data is shared between companies and government agencies. Though the reports may be sufficient to deflect some subscribers' concerns about the activities undertaken by telecommunications companies, meeting the other goals require that transparency reports include information about how long data is retained and terms or processes under which it is accessed, and that the presentations of data must be consistent across the industry. I ultimately argue that transparency reports largely add uncontextualized data to a nuance- and data-hungry public debate on the topic of domestic state surveillance without these additional data elements and industry-wide data reporting standardization.

The Potentials and Limits of Transparency Reporting

Transparency reporting refers to the public disclosure of data that pertains to a public interest. Such interests can include environmental issues, food safety, transportation safety, electrical standards compliance, and (increasingly) state access to data collected and stored by private businesses. Reporting can vary in its design and intended consequences. Warning systems are designed to sway individuals towards particular actions; the warning labels on cigarette packages are meant to dissuade people from smoking. Right to know reporting, in contrast, generally informs the public discourse without directing any particular action. Such reporting includes the release of structured 'open' datasets by governments without any accompanying assertions as to why, or whether, the data is significant to specific public policy debates. Targeted transparency reporting, in comparison, strikes a middle position and "provides information that is complex and factual" and "encourages users to make reasoned judgements of their own". Such reports are designed to "influence specific choices."[3]

---

[2] Government of Canada. (2014). "Memorandum for the Deputy Minister: Meeting with TELUS Corporation to Discuss Transparency Reporting for Electronic Surveillance," April 16, 2014, obtained under access to information and privacy legislation.

[3] Archon Fung, Mary Graham, and David Weil. (2007). *Full Disclosure: The Perils and Promise of Transparency*. New York: Cambridge University Press. Pp. 39.

Effective targeted transparency reports should "reduce specific risk or performance problems through selective disclosure by corporations and other organization."[4] In the financial sector, quarterly financial reports reduce investor risks and reveal organizational practices that enhance or weaken profitability. To reduce risk or performance problems that are otherwise incurred by less-knowledgable parties, reports must be: publicly disclosed; issued by organizations that hold a monopoly on relevant data; consist of standardized and comparable information; concern specific products or practices or policies; and further a defined public purpose.[5] Moreover, reports should be included within a defined feedback process; individuals must be able to access the information, make choices based on it, convey those choices (and rationales) to organizations responsible for the practices being evaluated, and organizations subsequently able to modify practice in response to individuals' actions or feedback.[6] Absent this full loop a transparency policy can have an *effect* without being *effective* in achieving its public policy ends.

There are disputes about the usefulness of transparency reports to publicize private information so that individuals and governments can make informed choices linked to the information. For Etzioni, regulations that compel the disclosure of privately-held information or knowledge of actions are needed for effective transparency reporting. Moreover, the public is generally forced to depend on intermediaries to 'translate' the complex data in transparency reports, thus causing decisions to be based on intermediaries conclusions.[7] The result of these translations, per de Fine Licht, is that the effectiveness — to say nothing of the effects — of transparency reports can be linked to third-party translators of technical facts as much as to the actions of the final decision makers themselves.[8]

To date, telecommunications transparency reports have largely focused on policing and security issues. Topics covered include how often data is disclosed to policing and security services, and the rationales for such disclosures. Telecommunications transparency reports differ from other transparency reports, such as those by health or food companies, because telecommunications companies must try to find a balance between between providing information about state activities to the public and not impeding the state's ability to protect its citizens.[9] The practice of trying to disclose information about government behaviours, while avoiding undermining the state's ability to protect citizens, can cause companies to engage in 'indirect' disclosures. Indirect disclosures often involve highly technical explanations of corporate practices that constrain analysis to handfuls of subject matter experts; such a limitation inherently prevents the public from making reasoned judgements independent of such experts' analyses and commentaries.[10]

---

[4] Archon Fung, Mary Graham, and David Weil. (2007). *Full Disclosure: The Perils and Promise of Transparency*. New York: Cambridge University Press. Pp. 5.
[5] Archon Fung, Mary Graham, and David Weil. (2007). *Full Disclosure: The Perils and Promise of Transparency*. New York: Cambridge University Press. Pp. 6.
[6] Archon Fung, Mary Graham, and David Weil. (2007). *Full Disclosure: The Perils and Promise of Transparency*. New York: Cambridge University Press. Pp. 6.
[7] Amitai Etzioni. (2010). "Is Transparency the Best Disinfectant?" *Journal of Political Philosophy* 18(4): 389-404.
[8] Jenny de Fine Licht. (2014). "Transparency actually: how transparency affects public perception of political decision making," *European Political Science Review* 6(2): 309-330.
[9] Alasdair Roberts. (2007). "Transparency in the Security Sector," Ann Florini (Ed.). *The Right to Know: Transparency for an Open World*. New York: Cambridge University Press.
[10] Christopher Hood. (2007). "What Happens When Transparency Meets Blame Avoidance?" *Public Management Review* 9(2). pp. 194.

Indirect transparency practices arise for a series of reasons. First, corporate officers might make the report hard to understand to avoid any blame or negative attention that might be linked to the report. Second, without common reporting standards across an industry it can be hard to compare between highly transparent reports. Even expert analysts may be unable to parse non-standardized data across an industry. Third, where transparency reporting would disclose government behaviours the government would rather remain suppressed, such as the extent of state surveillance, there may be little governmental appetite to regulate industry to produce direct transparency reports. Thus, governments may be less interested in regulating the structure of telecommunications transparency reports than food safety or medication reports.

Notwithstanding the limitations of transparency reporting there are numerous benefits when such reporting is done well. Transparency makes "processes of governance and lawmaking as accessible and as comprehensible as possible — to simplify them so they are more easily understood by the public."[11] By disclosing how often government agencies exercise their surveillance capabilities the public and legislators alike can see the emergence of new forms of surveillance and also understand the breadth and extent of information disclosures between private organizations and government. And, while de Fine Licht notes that the role of intermediaries impedes strong claims that transparency is linked to democratic theory, she does not go so far as to say there is no impact: transparency in governance and decision making increases public beliefs concerning the legitimacy of organizations' practice even where there is some intermediary analysis.[12] Thus the development and production of effective telecommunications transparency reports can lead the public to confirm or deny the legitimacy of otherwise secretive state surveillance practices. Finally, many of the limitations of transparency reports are alleviated when organizations genuinely commit to reporting. Such commitments entail not using the reports to foster blame avoidance, ensuring the reports have testable public policy impacts, and buttressing the reports with either hard (politically-legislated) or soft (binding corporate promises) regulations concerning the regularity and cross-industry consistency of reports.

In the past, scholars of transparency reporting often focused on reports where there is, or has been, some government support for the reporting. The effects and effectiveness of government supported reporting vary, as do the structures of the associated transparency reports. But how do companies structure transparency reports in response to government-mandated activity like state surveillance? And how effective are such reports in achieving public policy goals often meant to expose the actions of government?

Telecommunications Transparency in Canada

Telecommunications transparency reports are a relatively new phenomenon. The earliest reports were produced by Google (2010), Twitter (2012), and SpiderOak (2012) with other reports beginning to be issued following Edward Snowden's revelations concerning the extent to which telecommunications data is accessed by signals intelligence and domestic policing and security agencies. As of January 2015 there were thirty-nine reports that span industry categories such as Internet service companies (e.g. Yahoo!, AOL, Cloudflare, Dropbox),

---

[11] Patrick Birkinshow. (2006). "Freedom of Information and Openness: Fundamental Human Rights?" *Administrative Law Review* 58(1): 177-218. Pp. 189-90.

[12] Jenny de Fine Licht. (2014). "Transparency actually: how transparency affects public perception of political decision making," *European Political Science Review* 6(2): 309-330.

hardware/cloud companies (e.g. Microsoft, Apple), social media companies (e.g. LinkedIn, Pinterest, Facebook), and Internet access providers (e.g. Verizon, Rogers Communications, Vodafone).[13]

In Canada, academics and public advocacy organizations have called for increased transparency into how often, and for what reasons, government organizations request information from telecommunications companies which provide Internet access, telephone, and mobile telephony services. These call have been spurred by a decade-long public policy debate about the merits of 'lawful access' legislation. Such legislation is crafted to enhance and expand public officers' capabilities to conduct surveillance for investigative- and intelligence-related ends.[14] Those critical of successive governments' lawful access proposals have demanded that the federal government prove the legislation would resolve a set of problems facing government officers. Despite having stalled the passage of the legislation, the critics did not prompt the government to release data which strongly supports the legislation's need. Concerns that lawful access legislation was driven to extend or to legitimize existing intelligence and security practices[15] have been buttressed by growing evidence that government agencies are secretly accessing telecommunications data 'in bulk', as has been the case in the United Kingdom and United States.[16]

While demanding that the government produce evidence that the new powers are needed, Canadian academics and civil society organizations have also called for telecommunications companies to release transparency reports. Pressure for companies to release these built during 2014, and involved sending public letters to telecommunications companies, placing pressure on the federal government by opposition members of parliament, releasing aggregate historical information concerning government access to some subscriber information, and developing and deploying a tool that let Canadians easily request their personal information from their telecommunications provider and whether any of that information had been disclosed to third parties, including government agencies.[17] The transparency reports, from the perspective of academics and members of civil society, were driven with two public policy goals in mind:

---

[13] Peter Micek. (2014). "Transparency Reporting Index," *Access*, revised January 8, 2014, accessed January 15, 2014, https://www.accessnow.org/pages/transparency-reporting-index.

[14] Christopher Parsons. (Forthcoming). "Stuck on the Agenda: Drawing lessons from the stagnation of 'lawful access' legislation in Canada," in Michael Geist and Wesley Wark (Eds.).*Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: Ottawa University Press.

[15] Christopher Parsons. (2013). "The Canadian Experience" in *The Politics of Deep Packet Inspection: What Drives Surveillance by Internet Service Providers?* Doctoral Dissertation. University of Victoria, Victoria.

[16] Several documents from the Edward Snowden archive have indicated there is one or many 'special sources' of domestic Canadian telecommunications data that is accessed by Canada's foreign signals intelligence agency. See: Communications Security Establishment. (Date Unknown). "TLS Trends: A roundtable discussion on current usage and future directions," accessed December 30, https://www.christopher-parsons.com/Main/wp-content/uploads/2014/12/csec-tls-trends.pdf and; Communications Security Establishment. (2012). "IP Profiling Analytics & Mission Impacts," accessed December 30, 2014, https://www.christopher-parsons.com/writings/cse-summaries/.

[17] Andrew Hilts and Christopher Parsons. (2014). "Enabling Citizens' Right to Information in the 21st Century," *The Winston Report*, Fall 2014; Christopher Parsons (Forthcoming). "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).

1. To expand upon and contextualize the information concerning the extent of government surveillance of telecommunications systems.
2. To legitimize and make routine the disclosure of data relating to surveillance in excess of what municipal, provincial, and federal government agencies are required to make public because of legislative statutes.

In addition, corporations arguably have their own goal when releasing their reports:

3. To deflect or respond to telecommunications subscribers' concerns about how their data is shared between ISPs and government agencies.

This third goal, in particular, focuses on dampening public calls for mandatory transparency reporting, which could involve regulations that impose costs on companies and that would require particular kinds of disclosure instead of disclosures that are made (and decided upon) based on corporate generosity. Though these companies' reports add to the aggregate base of information concerning government surveillance the effectiveness of the reports in meeting the first two goals remains partial at best.

Fragmentary Knowledge of Government Surveillance

Transparency efforts by Canadian academics and civil society organizations have been linked to resistance to proposed expansions of state surveillance powers, with a focus on the impacts of the new powers for federal agencies. These critics learned about fragments of government surveillance practices over the course of a decade, but these fragments did not form a mosaic that revealed the full extent of telecommunications surveillance in Canada.

Canadian domestic authorities are statutorily required to produce annual reports about how often they conduct telecommunications interceptions. As part of their reporting, these authorities must disclose the number of individuals affected, the average duration of the surveillance, type of crimes investigated, number of cases brought to court, and number of individuals notified that the surveillance had taken place.[18] When the federal government's reports are juxtaposed the number of requests for surveillance have decreased (from almost 1,200 in 1975 to under 200 in 2010) with a fifty-percent increase in the number of individuals notified (roughly 800 in 1977 to approximately 1,200 in 2010). These figures indicate that though fewer interception orders are issued they now encompass the communications of more individuals than when the reports were initially tabled in the 1970s.[19] However, the federal governments reports tell a partial story at best: data contained in a 2012 access to information and privacy (ATIP) request revealed that all telecommunications carriers had received at least 6,000 orders applying to the interception of wireline, wireless, and internet communications.[20] The bulk of surveillance was not conducted by federal agencies, but by their provincial and municipal counterparts. Regardless of the

---

[18] Criminal Code of Canada, s.195

[19] Nicholas Koutros and Julien Demers. (2013). "In Big Brother's Shadow: Historical Decline of Electronic surveillance by Canadian Federal Law Enforcement," *Social Sciences Research Networking*, last revised March 15, 2013, accessed December 2, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2220740.

[20] Matt Braga. (2014). "New Documents Show Thousands of Unreported Wiretaps by Canadian Cops," Motherboard, November 20, 14, accessed November 26, 2014, http://motherboard.vice.com/en_ca/read/new-documents-show-thousands-of-unreported-wiretaps-by-canadian-cops.

organization which conducts the interception, individuals who have been subjected to an interception are later notified that they were monitored by the government.

In addition to interception warrants, there are also warrants that authorize federal authorities to install number dialler recorders. These are issued on the standard of "reasonable grounds to suspect that an offence under this or any of other Act of Parliament has been or will be committed".[21] Such recorders keep logs of numbers dialled to and from targeted phone numbers or devices. 'Grounds to suspect' is a diminished standard to receive a warrant; the standard is based on the belief that an individual's dialling habits enjoy reduced privacy protections because they reveal less information about a person's private life than an interception.[22] The government is not required by statute to record or report the number of number recorder orders they receive each year, nor an aggregate summary of the number of persons affected by these recorders. However, an ATIP document that was rereleased in 2014 revealed that there had been approximately 12, 000 number recorders issued to telecommunications companies in 2011.[23]

The lawful access debates have routinely focused on the relative ease at which government agencies can access 'subscriber data'. Such data has been defined differently in past pieces of lawful access legislation and has, in aggregate, included the following data items: name, address, telephone number, email address of the subscriber, as well as Internet protocol number, mobile identification numbers, electronic serial numbers, local service provider identifiers, international mobile equipment identity numbers, and subscriber identity module cards associated with the account.[24] Several versions of the legislation would have forced telecommunications companies to warrantlessly disclose subscriber data at the request of a public officer.[25] Some versions also included a reporting function that would compel government agencies to record the number of requests they made for this data. Though the federal government maintained that access to this information was critical for contemporary policing it did not disprove that authorities were already accessing subscriber data in bulk without court orders.[26]

Scholars found that authorities routinely gained access to subscriber data without the powers included in lawful access legislation. The Royal Canadian Mounted Police (RCMP), Canada's

---

[21] Criminal Code, s.492(1).
[22] Tim Quigley. "The Impact of the Charter on the Law of Search and Seizure." *Supreme Court Law Review* 40 (2008). Pp. 131.
[23] Matt Braga. (2014). "New Documents Show Thousands of Unreported Wiretaps by Canadian Cops," Motherboard, November 20, 14, accessed November 26, 2014, http://motherboard.vice.com/en_ca/read/new-documents-show-thousands-of-unreported-wiretaps-by-canadian-cops.
[24] Christopher Parsons. "The Anatomy of Lawful Access Phone Records," *Technology, Thoughts, and Trinkets*, published November 21, 2011. Accessed December 2, 2014. https://www.christopher-parsons.com/the-anatomy-of-lawful-access-phone-records/.
[25] Philippa Lawson. (2012). *Moving Towards a Surveillance Society: Proposals to Expand "Lawful Access" in Canada*. Vancouver. Pp. 33.
[26] Michael Geist. (2012). "Everything You Always Wanted to Know About Lawful Access, But Were (Undertandably) Afraid To Ask," *Michael Geist,* published February 13, 12012, accessed December 2, 2014, http://www.michaelgeist.ca/2012/02/lawful-access-faq/; Jameson Berkow. (2012). "Police 'scrambling' to justify lawful access laws," *Financial Post*, January 18, 2012, accessed December 2, 2014, http://business.financialpost.com/2012/01/18/police-scrambling-to-justify-lawful-access-laws/?__lsa=b365-ec43; David Fraser. (2011). "What's the justification for warrantless access to customer data in "lawful access"," *Canadian Privacy Law Blog*, published November 4, 2011, accessed December 2, 2014, http://blog.privacylawyer.ca/2011/11/justification-for-warrantless-access-to.html.

federal policing agency, made at least 28,143 requests for subscriber records in 2010.[27] Based on an industry-association that collated data for its members, at least 1,193,630 requests for subscriber data were made in 2011 across Canada which affected 784,756 accounts at a minimum.[28] The number of persons affected by the requests, however, was unclear because customer requests that were not about customer name information but "may cover many accounts/customers."[29]

Further documents, disclosed following a parliamentarian's questions, revealed that in 2013 the RCMP had abandoned its ability to track its number of requests for subscriber data and stated that individuals were not notified that their records were requested unless "through the Crown's obligation to disclose when the investigation results in a prosecution."[30] Responses to the same parliamentarian's questions revealed that the Canadian Border Services Agency (CBSA) had made 18,729 requests for basic subscriber information. It made 0 requests for interception orders. Like the RCMP, CBSA does not notify subscribers that it has requested their information though such requests may be revealed if the data is used as evidence against the subscriber in a court proceeding. Ultimately, the data that was provided by industry associations and by federal agencies was limited because the data had not been released on an annual basis and because what was provided merely indicates the lower number of subscribers or accounts that have been affected by government requests for subscriber data. In the wake of a Supreme Court of Canada decision, *R. v. Spencer*, subscriber data will be granted a higher degree of protection[31] — public agencies must now serve a court order to companies or rely on statutory powers to receive subscriber records in non-exigent circumstances — and as a result federal agencies are abandoning some investigations. Instead of taking five minutes to request information pre-*Spencer* it now (allegedly) takes up to ten hours to ensure that a request will meet judicial scrutiny.[32] However, despite ascribing stronger privacy protections to subscriber data the Supreme Court of Canada ruling did not establish statutory requirements on any level of government to either record or report the regularity at which it requests, and receives copies of, subscriber data records that are retained by telecommunications providers.

The actions of select members of parliament and an independent officer of parliament, as well as the efforts of academics and investigative journalists notwithstanding, their contributions

---

[27] Christopher Parsons. (2012). "Canadian Social Media Surveillance: Today and Tomorrow," *Technology, Thoughts, and Trinkets*, May 12, 2012, accessed November 26, 2014, https://www.christopher-parsons.com/canadian-social-media-surveillance-today-and-tomorrow/. The RCMP's data is incomplete and did not include information on how provincial deployments of the policing agency requested subscriber records.

[28] Gowlings, for the Canadian Wireless Telecommunications Association. (2011). "Re: Response to Request for General Information From Canadian Wireless Telecommunications Association (the "CWTA") Members," *Gowlings*. December 11, 2011.

[29] Gowlings, for the Canadian Wireless Telecommunications Association. (2011). "Re: Response to Request for General Information From Canadian Wireless Telecommunications Association (the "CWTA") Members," *Gowlings*. December 11, 2011. Pp. 1.

[30] Minister of Public Safety and Emergency Preparedness. (2014). "Response to Q-233," *Government of Canada*.

[31] *R. v Spencer*, 2014 SCC 43.

[32] Jim Bronskill. (2014). "RCMP has dropped Internet-related probes following high court decision: memo," *The Canadian Press*, last revised November 20, 2014, accessed December 2, 2014, http://www.winnipegfreepress.com/canada/rcmp-has-dropped-internet-related-probes-following-high-court-decision-memo-283393061.html.

have only suggested the contours of contemporary government surveillance. They have not mapped the specific dimensions of what governments are requesting, the regularity at which such request are made on a yearly basis, or the value of such requests in resolving offences under the Criminal Code or other Acts of Parliament. Their efforts do, however, demonstrate that that data provided in statutory reports on the use of interceptions falls short of accounting for the full extent of federal, provincial, and municipal agencies' surveillance activities.

Transparency reports may be a last and best hope to understand the extent to which governments across Canada are monitoring Canadians' telecommunications absent new statutory government reporting requirements. Telecommunications providers are well situated to collect and disclose the aggregate number of requests they receive and respond to, the number of persons or accounts affected by government surveillance, and can legally publicize such aggregate data.[33] Moreover, only companies can report on the surveillance conducted by governments which the governments themselves refuse to publicly report about. But how effective have companies been in keeping these records? And does disclosing the number of times information was shared with government make an effective transparency report in the first place?

Consolidating Data in Corporate Reports

Internet Service Providers (ISPs) enjoy privileged roles in the daily lives of citizens. Citizens, generally, "have come to depend on them to safeguard our personal information and private communications and to prevent that information from falling into the hands of third parties. This gives ISPs power and discretion: power to control our online behaviour and discretion to alter our outcomes."[34] ISPs have historically maintained that they have narrowly exercised this discretionary power when it came to disclosing Canadians' information to state agencies. In *R. v Cuttell* a Bell Canada employee asserted that the company "will only provide subscriber information to police in child exploitation cases and will not provide it for fraud cases, copyright cases or anything else" and, similarly, a Rogers employee in *R. v. Brousseau* stated that "… save for investigation into child exploitation or in exigent circumstances, Rogers will require a warrant or a subpoena to produce information." Even as companies began issuing their transparency reports, executives maintained that warrantless disclosures had been limited; as an example the Vice-President, Regulatory, for Rogers Communications stated that he believed all the warrantless requests had pertained to child exploitation cases and that he was surprised that the warrantless requests for subscriber information pertained to unrelated kinds of cases.[35]

As of the end of 2014, two of Canada's three largest providers, Rogers and TELUS, disclosed information about the regularity at which government requested, and received, access to subscribers' data. Two other, smaller, companies, SaskTel and TekSavvy, also publicized the extent to which they received, and complied with, government requests for telecommunications data. All four companies also committed to releasing annual reports.

---

[33] Hon. James Moore. (2014). Government correspondence to Tamir Israel, July 24, 2014.
[34] Ian Kerr and Daphne Gilbert. (2004). "The Role of ISPs in the Investigation of Cybercrime," in Tom Mendina and Johannes J. Britz (Eds.). *Information Ethics in the Electronic Age: Current Issues in Africa and the World*. Jefferson, North Carolina: McFarland. Pp. 164-5.
[35] Kenneth Engelhart. (2014). Regulatory Blockbuster Panel, Canadian Telecommunications Summit. June 2, 2014.

Rogers received 87,856 requests for customer names and addresses, 74,415 requests for data under court order or warrant, 2,556 requests based on government exercising statutory powers, 9,339 requests based on exigent or emergency circumstances, 711 requests meant to respond to child exploitation emergencies, and 40 requests pursuant to Mutual Legal Assistant Treaties (MLATs). The company's responses did not record how often it pushed back against requests, the number of persons affected by requests, or the number of times that only some of the requested data was provided.[36] The company planned to track this data for future reports. TELUS, like Rogers, did not record the number of subscribers or accounts affected by requests from government agencies. The company disclosed that it responded to 3,922 court orders and 393 subpoenas, 40,900 requests for subscriber names or address information, 1,343 requests based on government exercising existing statutory powers, 56,748 emergency calls (such as when authorities request information to locate or assist persons where their life, health, or security is at risk), and 154 requests pursuant to child exploitation emergency requests, and 2 requests pursuant to MLATs.

SaskTel is a regional telecommunications provider. It received fewer requests for information by government authorities than Rogers or TELUS. Most of the requests it received were to "confirm a customer's current name and address." SaskTel's transparency report showed there were 1,582 requests for "General" requests which "Listed Customer Name and Address." There were presumably more requests for this kind of information since the company's 'emergency requests' category is broad enough to include "[h]elping locate someone with a cellular phone and provide contact details for someone who has contacted emergency services and may be unable to communicate." There were 718 such requests during regular working hours and 3,993 that took place after-hours. The company also received 4,139 requests based on court orders, 896 requests for based on freedom of information and protection of privacy grounds, 223 on federal/provincial formal demands, and 49 in response to child sexual exploitation. The company denied 247 requests, though it did not explain what categories those denials were made under.[37]

TekSavvy, differing from the other carriers, provided comprehensive responses to the public letter issued to it by academics and civil liberties organizations; that response has become its first transparency report. In 2012 and 2013, combined, it received 52 requests from law enforcement agencies trying to correlate IP addresses with subscriber names and related subscriber information. The company listed the data fields that were returned to requesting agencies, that the information was requested retroactively, and that only one of the 52 requests was made subject to a court order. Moreover, the company provided information in 17 cases and denied the remaining 35. And unlike any other company, TekSavvy differentiated between how many requests were made by federal (37%), provincial (10%) and municipal (54%) agencies. TekSavvy also outlined the kinds of data it retains in the course of providing telecommunications services to its subscribers, the retention periods for data that is collected, and that the company's "general legal standard is to require that government agencies provide a

---

[36] Rogers Communications. (2014). "Rogers Communications 2013 Transparency Report," http://www.rogers.com/cms/images/en/S35635%20Rogers-2013-Transparency-Report-EN.pdf.
[37] SaskTel. (2014). "SaskTel 2013 Transparency Report," *SaskTel*, http://www.sasktel.com/wps/wcm/connect/019634af-8378-432a-b6bf-3c47fe2e8d55/Transparency+Report_NR_Sep14.pdf?MOD=AJPERES.

warrant, provide a production order, or demonstrate that obtaining one is justified but unfeasible die to exigent circumstances".[38]

These companies' first transparency reports have shed some light on some extent of the surveillance conducted by government agencies, insofar as the number of requests received for different kinds of request categories has been made public. And releasing the reports may deflect or respond to telecommunications providers' subscribers' concerns about how their data is disclosed to government agencies. However, as will be clear in the following discussions of data retention periods and the publicity of lawful access handbooks, the initial reports only a hint at the full extent of surveillance (how many records are accessed, on average, per request?) or contextualize the process (how, exactly, does a company deal with requests? What does 'pushing back' really mean?)? Consequently, while the reports that were released in 2014 partially improved the public's understanding of the extent of state surveillance they did not clearly explain how many records were disclosed to government agencies on an annual basis. Moreover, even with more comprehensive reports from these companies Canadians will only have a partial image of government surveillance: all telecommunications providers in Canada, such as Bell Canada (and its sister companies and flanker brands), as well as other companies across Canada such as Videotron, Shaw, Eastlink, and MTS Allstream must release reports for the public to have a clear picture of the extend of government surveillance.

Setting aside the problem of not all companies releasing transparency reports, how might existing reports be improved to make them effective in achieving all three of the policy goals associated with these reports? And, why does it matter if companies do not add data retention schedules and lawful access processes to their transparency reports?

Data Retention Transparency

The number of times that government agencies have requested telecommunications information does not reveal the extent to which data has been accessed. To put it another way, while a single request could be for one record of data that was generated yesterday, it could equally be for all of the thousands of records that have been generated, and stored, over the past ten years and associated with an individual or account. Merely disclosing the number of requests, and the number of times records were then disclosed, does not capture the extent to which government agencies can, or could, request information. Without knowing how long a company retains data it is impossible to understand the actual or potential invasiveness a data request.

Canadian ISPs, when responding to public letters issues to them in January 2014, asserted their support for Canada's privacy laws. Bell Canada stated that its commitment to privacy is reflected in its privacy policy and that it and that its management of personal information is regulated by the Canadian Radio-television and Telecommunications Commissioner (CRTC) as well as Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA).[39] TekSavvy wrote that the company works "to ensure that all of [their] practices comply with [their] PIPEDA and CRTC obligations. However, we have come to believe that it is also TekSavvy's

---

[38] TekSavvy. (2014). "Re: January 20 Data Request (items 1-10); May 1 Personal Information Template," *TekSavvy*, June 4, 2014, https://citizenlab.org/wp-content/uploads/2014/06/TekSavvy-to-Citizenlab-2014-06-04.pdf.

39 Bell Canada. (2014). "Inquiry concerning lawful access and other disclosures to government," issued March 3, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Bell-Canada-Lawful-Access-Request-Letter.pdf.

responsibility … to lead with respect to going beyond those obligations."[40] Responses from Bell Aliant,[41] Eastlink,[42] and Shaw Communications,[43] all, similarly, assert that the companies comply with their obligations under PIPEDA.

These company are legally obligated to comply with privacy laws. Under PIPEDA, corporations must limit use, disclosure, and retention of personal information (Principle 5) and be open about their practices and policies "relating to the management of personal information" (Principle 8). Combined, these principles mean companies should be forthright about the data they collect as well as their practices associated with handling the information. Data retention periods are inclusive of data handling practices because without knowledge of when data is disposed an individual cannot understand a company's management of their personal information. In sum then, companies are expected to be clear in their retention and disclosure of information, and of their the policies surrounding data retention and data disclosure practices.

Disclosing data retention periods must be explained consistently and clearly across the industry or else individuals may not understand differences in companies' practices. Standardized retention information in transparency reports would ideally include examples of the information contained in a given record, such as a subscriber record or SMS message or IP log, alongside the period of time the records are retained. To further contextualize this information companies could include the approximate number of records subscribers will generate of a given type, each month or year, with the understanding that some individuals will generate more or fewer records. In addition, companies could include the average number of records that are disclosed of each type when responding to a government order; is it the case that government agencies are requesting one out of a million records when they compel companies to provide data about a subscriber, or ten thousand of the million, or all one million of them?

Publicly Releasing Lawful Access Handbooks

Even disclosing the number of government requests for data along with the periods of time for which government agencies could potentially access records, cannot explain the *processes* these agencies must undertake to access corporate-handled data. When asked about the processes that have been established for receiving, and responding to, government requests for data Bell Canada responded by stating that, "all such requests are vetted by Bell Canada's lawful access group and, where there is any doubt by [the privacy officer's] office. Where necessary, the lawful access group has required government agencies to withdraw their disclosure requests where the request appears unreasonable in its scope or lacks the

---

[40] TekSavvy. (2014). "Re: January 20 Data Request (items 1-10); May 1 Personal Information Template," published June 4, 2014, available at: teksavvy.com/Media/Default/Citizen Lab/TekSavvy to Citizenlab - 2014-06-04.pdf.

[41] Bell Aliant Privacy Office. (2014). "RE: Questions Concerning Disclosure of Telecommunications Information to Government Authorities," personal email, March 3, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Response-from-Bell-Alliant.pdf.

[42] Eastlink. (2014). "RE: Questions Concerning Disclosure of Telecommunications Information to Government Authorities," personal email, March 3, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Response-from-Eastlink.pdf.

[43] Shaw Communications Inc. (2014). "Re: Request for Information," March 4, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Response-from-Shaw.pdf.

reasonable grounds required by law."[44] Another company, Eastlink, said that it "does not disclose any information except pursuant to a warrant or other order that legally compels us to disclose the information, or in very exceptional emergency circumstances as also permitted under PIPEDA."[45] In their transparency report, TELUS states that it challenged court orders "on the ground that it was either defective or overreaching", that they "don't respond to requests that come directly from foreign agencies", that they changed subscriber data disclosure practices post-*Spencer*, as well as explaining how it processes emergency calls, internet exploitation cases, and 'legislative demands.' TELUS also provided an outline of the process it uses to respond to information requests.[46] SaskTel reported that it has a dedicated group for handling data requests from government agencies but did not precisely explain the process by which it received and subsequently evaluated requests from government.[47] The company did, however, disclose the fee schedule associated with intercepting communications for government agencies.[48] While Rogers Communications stated it sometimes will "push back and, if necessary, go to court of oppose the request" if a given request is over broad, the company did not explain exactly how government requests are processed.

Non-Canadian companies' 'law enforcement handbooks' are sometimes available either voluntarily or because they have been leaked to the public. Such handbooks include the detailed procedures government agencies must follow to request corporate-held data, the kinds of identification government agents must present before information will be disclosed, the time it takes for corporations to process requests, and the costs agencies must pay for the requests to be processed. Some handbooks also identify the data fields included in each 'category' of a request, such as the fields linked with subscriber data requests and how released fields vary depending on the court orders used.[49] Publishing law enforcement handbooks reduces the confusion that government agencies may have concerning what data is stored, for how long, and the terms under which it is released[50] while revealing to the public how their personal information is handled when a state agency requests it.

---

[44] Bell Canada. (2014). "Inquiry concerning lawful access and other disclosures to government," issued March 3, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Bell-Canada-Lawful-Access-Request-Letter.pdf.

[45] Eastlink. (2014). "RE: Questions Concerning Disclosure of Telecommunications Information to Government Authorities," personal email, March 3, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Response-from-Eastlink.pdf.

[46] TELUS. (2014). "TELUS Transparency Report 2013," *TELUS*, http://about.telus.com/servlet/JiveServlet/previewBody/5544-102-1-6081/TELUS%20Transparency%20Report%202013%20-English.pdf.

[47] SaskTel. (2014). "SaskTel 2013 Transparency Report," *SaskTel*, http://www.sasktel.com/wps/wcm/connect/019634af-8378-432a-b6bf-3c47fe2e8d55/Transparency+Report_NR_Sep14.pdf?MOD=AJPERES.

[48] SaskTel. (2010). "Customer Information Requests and Wiretap Services," *SaskTel*, Effective as of March 19, 2010, accessed December 2, 2014, http://www.sasktel.com/wps/wcm/connect/afd85294-2b3c-476c-a9fd-75869c23537a/110-16.pdf?MOD=AJPERES.

[49] Colin J. Bennett, Christopher Parsons and Adam Molnar. (2014). "Forgetting, Non-Forgetting and Quasi-Forgetting in Social Networking: Canadian Policy and Corporate Practice," in Serge Gutwirth, Ronald Leenes, and Paul De Hart (Eds.) *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*. New York: Springer. Pp. 52-53.

[50] Based on interviews conducted with Canadian law enforcement officers for the Canadian Access to Social Media (CATSMI) project, 2011-12.

Larger Canadian telecommunications companies that regularly receive requests from government agencies for data have policies for how to respond to state agencies' requests. Several note either in their public statements or transparency reports that they will sometimes evaluate requests and push back against over broad requests. No Canadian company has released the processes or policies it uses to evaluate requests, however, or specifically what information authorities can obtain using the legal instruments noted in many of the 2014 transparency reports. Without such information it is unclear what information companies may, or do, disclose upon receiving a warrant or statutory demand.

A fulsome transparency transparency report would, either as an adjoining document or as part of the report itself, explain how data requests must be served on the company by government agencies and the kinds of requests that can be made (e.g. voluntary, formal requests, emergency requests, court orders). Such an explanation would also include the requirements that must be met before any given request is processed. Is specific information requested of government agencies before the company can process voluntary, versus formal legal or court ordered, versus emergency requests? And when a request is made, what kinds of data must government agencies provide for companies to identify relevant accounts or subscribers — do identifiers vary per the kind of request, or are there higher standards for guaranteeing the government agent's identity depending on the sensitivity of the data requested?

As noted, previously, it is important for subscribers to know what kinds, and amounts, of data that different requests may release to government authorities. A company should include this information to explain to government agencies what they can access while also revealing the relative potency of government's legal instruments to telecommunications subscribers. There may be cases where requests for subscriber data are accompanied by a gag orders preventing the company from notifying the subscribers of the requests; it would be useful for subscribers to know whether their telecommunications provider will reveal that their personal information had been requested by a government agency absent such a gag. Companies have noted in their transparency reports and public disclosures that they sometimes disclose information to government agencies on the basis of exigent circumstances but few explain the processes that are in place to differentiate between exigent and non-exigent requests, nor whether there are different kinds of data that can be released under such circumstances. Companies could also disclose the length of time it takes to process requests and the costs of fulfilling the requests.

These elements are included in non-Canadian law enforcement handbooks and help government agencies to make requests for information while also demystifying the capabilities of telecommunications companies to assist governments conduct state-compelled surveillance. Combined with explicit data retention schedules and detailed information about the annual number of government requests for data, lawful access handbooks make clearer whether governments are engaged in high amounts of per-capita telecommunications surveillance.

Enhancing the Effectiveness of Transparency Reports

Transparency reporting is becoming a normal aspect of providing telecommunications services, as evidenced by the prominent companies around the world that are regularly releasing reports. As more companies produce and publish these reports subscribers, citizens, elected representatives, other companies, and government watchdogs can better act against either companies or government agencies based on inappropriate requests for, or disclosures of, information between companies and governments.

Transparency reports are not 'new' kinds of statements nor are companies likely to stop producing them in the near future. Transparency reports are, however, largely unregulated in terms of the content that they include, how content is presented, and how requests and disclosures are recorded. Some variation between industry sectors (e.g. Internet service providers, such as Rogers, versus providers such as Google) is expected. But even within the Canadian telecommunications industry there is variation amongst companies that released relatively short reports; while there were overlaps in how categories appeared to related across companies the reports were not been designed to harmonize with other companies' disclosure categories.

Standardization would enhance the effectiveness of the reports and let individuals make choices to prefer some companies over others based on their handling of law enforcement requests. To facilitate this kind of choice companies need a common standard for presenting existing data categories (e.g. court order/warrant, emergency request, child exploitation emergency, etc) and also include standardized data retention schedules and lawful access handbooks. For the reports to be useful in testing their effectiveness in deflecting or responding to subscribers' concerns associated with their provider disclosing information to authorities some kind of a feedback mechanism is needed to understand whether the company's lawful disclosure policies played a role in the customer's choice of a company's services.

Canadian transparency reports currently respond to the problem of insufficient data about government surveillance. Companies are best suited to fill this gap, especially given governments' recalcitrance to propose statutory reporting requirements alongside proposed new surveillance powers. What is missing, however, is that the data communicated by each company, barring TekSavvy, tends to be abstract because it lacks detailed information about the companies' respective data handling and disclosure policies. And there are no standards across the industry in presenting the reported data. As a result, any decisions that individuals take based on the reports released by Rogers, TELUS, Sasktel, or TekSavvy are based on incomplete or challenging-to-compare information.

Reports released in 2014 partially met the goal of expanding and contextualizing the information concerning the extent of government surveillance of telecommunications systems. They might be deflecting or responding to telecommunications subscribers' concerns about how their data is shared between telecommunications providers and government agencies. And as companies continue to release reports, as well as new Canadian companies join them in releasing reports, the very process of releasing aggregated surveillance information will be legitimized and become routine. But reports largely fail to explain the processes of disclosure, the full rationales, or the amounts of data that can be released and is released on average. The result is that reports released to date represent starting points, rather than end points, in the path towards telecommunications transparency in Canada.

In March 3, 2014 Rogers Communications stated it could not share information about the extent to which it disclosed information to government agencies "[d]ue to confidentiality, law enforcement and national securities concerns" and that there were "restrictions around the disclosure of information about access and intercept requests that Rogers receives from government agencies." TELUS stated that it could not "publicly disclose the information that has been requested" by Canadian academics and civil liberties groups. A few months later, and four companies disclosed information about the extent of government telecommunications surveillance. A culture of transparency around government surveillance is being built, piece by

piece, from scratch. Each of the pieces of information in the reports matter and, as of the end of 2014, we have more pieces to the domestic surveillance jigsaw than ever-before. But to complete it more context about the dimensions of the puzzle itself is required.