Transparency in Surveillance: Role of various intermediaries in facilitating state surveillance transparency[1]

By Christopher Parsons, Post-doctoral Fellow, The Citizen Lab
christopher@christopher-parsons.com

Internet access and service providers are now essential partners for private citizens' daily activities. Massive volumes of personal communications, as well as machine to machine communications, are transmitted every moment. And this data, when collected or analyzed, can be intensely revealing of what individuals or groups are doing, thinking, saying, or planning. In effect, the communicative potentials of the Internet do not just advance freedom of speech or association, but simultaneously give rise to potentially massive and untargeted surveillance that can broadly infringe on individuals' rights.

In this section we discuss how governments have expanded their surveillance capabilities in response to enhancing law enforcement, foreign intelligence, and cybersecurity powers. After outlining some of these new powers and their impact of communicating parties we proceed to discuss the impact of voluntary intermediary activities, and how they affect government surveillance capabilities. Just as private companies can facilitate government surveillance they can also facilitate transparency about surveillance by proactively working to inform their users of governments' activities. We conclude by discussing the broader implications of contemporary state surveillance practices, with a focus on the chilling effects that these practices have on social discourse writ large.

(a) Expanded State Surveillance Capabilities

Numerous OECD countries have systematically expanded the intelligence gathering and investigative techniques available to intelligence, security, and domestic agencies since 2001. In this section we concentrate on the expansion of such techniques within Canada and the United States. Many of these techniques are focused on compelling, or otherwise accessing, communications information from telecommunications intermediaries. Such intermediaries include wireless and wireline communications providers, as well as companies offering 'cloud' services such as messaging companies, social media companies, and other contemporary digital networking services.

Some of the adopted techniques include government agencies receiving legal authorization to intrude upon communications networks, by either 'disrupting' communications flows or impersonating legitimate communications equipment. Other methods empower government agencies to compel intermediaries to affect subscribers' communications on the behalf of government; sometimes this involves forcing intermediaries to preserve or produce subscribers' communications and in others even modifying systems to collect

otherwise secret information from subscribers. After outlining some of these powers we move to explain the secrecy attached to such powers and general lack of government accountability for their use.

New Powers of Investigation

The end of the 1990s saw several Western governments take computer-based criminal activities more seriously. This lead, in part, to the creation of the *Budapest Convention on Cybercrime*. The *Convention* was adopted by the Council of Europe in November 2001 and subsequently signed by countries including Canada and the United States. The convention's stated purpose included:

> (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation.[2]

Specifically, the *Convention* required national governments to "create new offences, including unlawful interception, access or interference with a computer system, computer-related forgery and fraud, and offences relating to child pornography and copyright."[3] The agreement was also used to justify new investigative powers; in Canada, this led the federal government to introduce (and, eventually, pass) lawful access legislation. Bill C-13, *Protecting Canadians from Online Crime Act*, established an offence of non-consensual distribution of intimate images, preservation of digital data and corresponding production powers, production orders for metadata or transmission data collected or generated by telecommunications companies, tracking data production orders that could be used to collect location information linked with a device, as well as indemnifying the sharing of information between companies and government while also establishing fines for organizations or persons that refuse to comply with a production order.[4] These powers, along with other legislation addressing copyright, fulfilled Canada's obligations under the *Convention*. Other nations used the convention to justify similar, or even more expansive powers, such as requiring telecommunications providers to be able to intercept subscribers' communications, enable authorities to access subscriber data without judicial order, and mandating data retention terms on intermediaries. The United States Senate

---

[2] Council of Europe. (2001). "Convention on Cybercrime," Council of Europe, November 23, 2001, retrieved November 14, 2015, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[3] Daphne Gilbert, Ian Kerr, and Jena McGill. (2006). "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers," *Criminal Law Quarterly* 51(4), p. 480.

[4] Sean Griffin, Anne-Elisabeth Simard, and Marianne Bellefleur. (2015). "Bill C-13: Lawful Access and the Relationship Between Organizations, Cyber-bullying and the Protection of Privacy Rights," *snIP/ITs: Insights On Canadian Technology and Intellectual Property Law*, February 25, 2015, retrieved March 13, 2015, http://www.canadiantechlawblog.com/2015/02/25/bill-c-13-lawful-access-and-the- relationship-between-organizations/.

ratified the *Convention* in August 2006; the Senate "took the view that prior U.S. legislation provided for all that the convention required of the United States."[5]

Beyond the powers noted in the *Convention*, and subsequently ratified by signatory nations, successive pieces of security legislation in Canada and the US have formalized and expanded the activities that state agencies can undertake following the attacks of September 11, 2001. In Canada, Bill C-36, *the Anti-Terrorism Act*, was passed in December 2001 and granted "expanded wiretap powers" along with additional security powers to government authorities.[6] The Anti-Terrorism Act also provided Canada's foreign signals intelligence agency, the Communications Security Establishment (CSE), a legislative mandate to collect foreign signals, protect government systems, and provide assistance to federal domestic authorities (i.e. 'Mandate C').[7] After acrimonious public and legislative debates the Government of Canada passed Bills C-44, the Protection of Canada from Terrorists Act, and C-51, Anti-Terrorism Act 2015, in 2015.

Bill C-44 authorised the Canadian Security Intelligence Service (CSIS) to conduct investigations inside and outside of Canada and to seek warrants to authorize foreign investigations. Moreover, the bill lets CSIS apply for domestic warrants that can be used to subsequently 'task' Canada's signals intelligence agency, the Communications Security Establishment (CSE), under Mandate C. CSE can then target communications signals which are transmitted or stored or processed by intermediaries outside of Canada. CSE may also ask for the assistance of non-Canadian intelligence partners to fulfil CSIS' requests.[8]

Bill C-51 modified the powers available to security organizations and, perhaps most significantly for this chapter, authorized CSIS to 'disrupt' threats.[9] Combined, the ability to work with signals intelligence agencies, under Bill C-44, and the potential to disrupt associations by potentially targeting telecommunications services and infrastructures, under Bill C-51, raise the prospect of Canadian security and intelligence agencies receiving court-approved warrants to interfere with communications transmitted or published using Internet intermediaries. Such interferences may, or may not, occur with the assistance of the intermediaries themselves.[10]

---

[5] William A. Owens, Kenneth W. Dam, and Herbert S. Lin (Eds). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: The National Academies Press. Pp. 280.

[6] Elinor Sloan. (2012). "Homeland Security and Defense in the Post-9/11 Era." David S. McDonough (Ed.). *Canada's National Security in the Post-9/11 World: Strategy, Interests, and Threats*. Toronto: Toronto University Press. Pp. 99.

[7] *National Defence Act*, §273.64(1)

[8] Bill C-44 also provides privilege to CSIS' human sources, meaning that they are less likely to be directly challenged in courts.

[9] Bill C-51, TITLE, §42; See also: Craig Forcese and Kent Roach. (2015). "Interrupt: Disruption When All Else Fails," in *False Security: The Radicalization of Canadian Anti-Terrorism*. Irwin Law Inc.

[10] As part of C-51, officials could apply to a court for permission to seize or to force a telecommunications provider to remove "any materials that promote or encourage acts of terrorism against Canadians in general, or the commission of a specific attack against Canadians." See: Laura Payton. (2015). "Anti-terrorism powers: What's in the legislation?" *CBC News*, January 30, 2015, retrieved February 15, 2015, http://www.cbc.ca/news/politics/anti-terrorism-powers-what-s-in- the-legislation-1.2937964.

The concerns raised by C-44 and C-51 are compounded by the pre-existing, friendly, relationship between the agencies. Journalists have found that federal agencies have availed themselves to CSE's assistance prior to the passage of Bills C-44 and -51.[11] Moreover, there are problems regarding security and intelligence agencies candor when appearing to the courts and requesting warrants. Specifically, prior to C-44, judges were deliberately misled by CSIS such that CSE's assistance was authorized, if not legal.[12] This led to Justice Mosley accusing Department of Justice lawyers of misleading the court and was the impetus for the government to introduce (and pass) bill C-44.

Like Canada, the American government has passed numerous bills that expand authorities' access to intermediary data. Under section 505 of the USA PATRIOT Act the FBI gained new conditions under which it could obtain information using National Security Letters (NSLs), such as from intermediaries.[13] Specifically, NSLs could be used so long as information requested was relevant to an investigation meant to prevent acts of terrorism or espionage. The FBI was found to be systematically abusing these powers,[14] with ongoing legal conflict over the ongoing use of the legal instrument.[15] Moreover, CALEA, the legislation which requires telecommunications carriers to provide interception capabilities to government authorities, was expanded in 2005 such that Voice over Internet Protocol (VoIP) communications had to be interceptable as well.[16] The US government has also indemnified companies that warrantlessly shared telecommunications data with the National Security Agency, while simultaneously permitting the surveillance to continue;[17] in recent years,

---

[11] Colin Freeze. (2014). "Spy agency's work with CSIS, RCMP fuels fears of privacy breaches," *The Globe and Mail*, January 31, 2014, retrieved February 3, 2015, http://www.theglobeandmail.com/news/politics/spy-agencys-work-with-csis-rcmp-fuels-fears-of-privacy-breaches/article16623147/.

[12] X (Re), 2013 FC 1275 (CanLII), retrieved November 17, 2015, http://canlii.ca/t/g2rl7; see also: Colin Freeze. (2013). "CSIS not being forthcoming with court, federal judge says," *The Globe and Mail*, November 25, 2013, retrieved November 17, 2015, http://www.theglobeandmail.com/news/national/csis-not-being-forthcoming-with-court-federal-judge-says/article15599674/; see also: Craig Forcese. (2013). "Triple Vision Accountability And The Outsourcing of CSIS Intercepts," *National Security Law: Canadian Practice in International Perspective*, December 6, 2013, retrieved November 17, 2015, http://craigforcese.squarespace.com/national-security-law-blog/2013/12/6/triple-vision-accountability-and-the-outsourcing-of-csis-int.html.

[13] Electronic Frontier Foundation. (2015). "National Security Letters," *Electronic Frontier Foundation*, retrieved November 17, 2015, https://www.eff.org/issues/national-security-letters.

[14] U.S. Department of Justice, Office of the Inspector General. (2010). "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," United States Government, January 2010, retrieved November 17, 2015, http://www.justice.gov/oig/special/s1001r.pdf.

[15] See: Electronic Frontier Foundation. (2015). "National Security Letters," *Electronic Frontier Foundation*, retrieved November 17, 2015, https://www.eff.org/issues/national-security-letters.

[16] Electronic Frontier Foundation. (2015). "CALEA," *Electronic Frontier Foundation*, retrieved November 17, 2015, https://www.eff.org/issues/calea.

[17] Electronic Frontier Foundation. (2015). "Timeline of NSA Domestic Spying," *Electronic Frontier Foundation*, retrieved November 17, 2015, https://www.eff.org/nsa-spying/timeline.

however, the federal legislative branches has modified some of the conditions under which such surveillance takes place on domestic persons.[18]

American agencies have also adopted tactics to assist one another beyond judicial scrutiny, though their methods differ from those adopted by Canadian agencies. As an example, the secretive Special Operations Division (SOD) of the Drug Enforcement Agency, and which includes the FBI, NSA, CIA, IRS, and DHS, would determine that a person was strongly suspected of violating, or known to have already broken, American law. The information would be shared as a tip to domestic agencies who, following the arrest, "pretended that their investigation began with the traffic stop, not with the SOD tip." A former DEA agent described this practice as "just like laundering money - you work backwards to make it clean."[19] The publicity of the parallel construction process is has led some persons to apply for re-trials based on potentially tainted investigations.[20] There is no evidence of equivalent practices occurring in Canada.

Combined, Western nations have empowered domestic authorities to access data transited, processed, or collected by intermediaries. These nations have also codified legal authorities that have expanded (or legalized existing) signals intelligence operations. In all cases, however, domestic- and foreign-focused departments have routinely targeted their efforts at intermediaries and the devices or software that intermediaries provide to their customers. The result is that the parties and devices responsible for transiting communications are intentionally targeted 'cyber' legislation that has passed into law following the attacks of September 11, 2001.

Expansion and Secrecy of Surveillance Techniques

A range of new intelligence and investigation methods have been adopted by domestic intelligence and security services after receiving the powers discussed above; such methods revolve around intercepting otherwise accessing transactional data as well as content from telecommunications companies.[21] Since the 1990s, and updated in the 2000s, wireline and wireless telecommunications companies in the United States have had to make voice communications accessible to government agencies under CALEA; such rules apply only to "common carriers" and "telecommunications carriers".[22] A parallel, though

---

[18] Lisa Mascaro. (2015). "Congress' passage of NSA bill will rein in surveillance, a first since Sept. 11," *Los Angeles Times*, June 2, 2015, retrieved November 17, 2015, http://www.latimes.com/nation/la-na-senate-advances-nsa-20150602-story.html.

[19] John Shiffman and Kristina Cooke. (2013). "Exclusive: U.S. directs agents to cover up program used to investigate Americans," *Reuters*, August 5, 2013, retrieved November 17, 2015, http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805; see also: "Parallel Contruction" FOI document, https://assets.documentcloud.org/documents/1011382/responsive-documents.pdf.

[20] David Ingram and John Shiffman. (2013). "U.S. defense lawyers to seek access to DEA hidden intelligence evidence," *Reuters*, August 8, 2013, retrieved November 17, 2015, http://www.reuters.com/article/2013/08/08/us-dea-irs-idUSBRE9761AZ20130808.

[21] Whitfield Diffie and Susan Landau. (2007). *Privacy on the Line: The Politics of Wiretapping and Encryption (Second Edition)*. Cambridge, Mass.: The MIT Press. Pp. 220-221.

[22] For the purposes of the law, this captures Voice Over Internet Protocol (VoIP) providers that offer managed services, but do not include non-managed VoIP services offering using peer to peer protocols or over instant

more extensive, series of requirements exist in Canada under the *Solicitor General's Enforcement Standards* (SGES). The SGES impose impose geolocation, interception, and decryption requirements on mobile telecommunications providers.[23] All providers in Canada may, however, receive warrants that compel them to either preserve or immediately disclose voice communications information to government authorities.[24] Authorities have also used production powers to compel intermediaries to compile, and subsequently disclose, information pertaining to their subscribers and their subscribers' communications. In both countries requests or demands for data controlled by intermediaries can be accompanied by gags, thus preventing the companies from alerting affected subscribers.[25]

In the United States and Canada alike, domestic authorities can request court authorization to deploy malware on target devices.[26] In addition to directly targeting persons with malware, American authorities have engaged in so-called 'watering hole' attacks. Such attacks involve infecting websites with malware that is automatically installed on the website's visitors' computers or otherwise compromising Internet infrastructures to deliver malware. These activities transform intermediaries into unknowing vectors of state surveillance.[27] Canadian legislation passed in 2015 also authorizes the use of malware to trace device locations,[28] though it remains unclear whether the CSE's malware

---

messengers. See: Jonathan E. Nuechterlein and Philip J. Weiser. (2005). *Digital Crossroads: American Telecommunications Policy in the Internet Age*. The MIT Press: Cambridge, Mass. Pp. 222-223.

[23] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf; see also: Christopher Parsons and Tamir Israel. (2015). "Canada's Quiet History of Weakening Communications Encryption," *Telecom Transparency Project*, retrieved February 29, 2016, https://www.telecomtransparency.org/canadas-quiet-history-of-weakening-communications-encryption/.

[24] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 7-23, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[25] No Canadian telecommunication company, based on their responses to public letters or their own published transparency reports, have ever notified a subscriber that the government has sought (or received) access to subscriber telecommunications data.

[26] Craig Timberg and Ellen Nakashima. (2013). "FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance," *Washington Post*, published December 6, 2013, http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html; Justin Ling. (2014). "Cyberbullying law would let police 'remotely hack into computers, mobile devices, or cars'," *National Post*, last updated January 24, 2015, retrieved November 17, 2015, http://news.nationalpost.com/news/canada/proposed-cyberbullying-law-would-let-police-remotely-hack-into-computers-mobile-devices-or-cars.

[27] Kevin Poulsen. (2013). "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired*, published September 13, 2013, http://www.wired.com/2013/09/freedom-hosting-fbi/.

[28] Christopher Parsons. (2014). "Canadian Cyberbullying Legislation Threatens to Further Legitimize Malware Sales," *Technology, Thoughts, and Trinkets*, June 4, 2014, retrieved November 17, 2015, https://www.christopher-parsons.com/canadian-cyberbullying-legislation-threatens-to-further-legitimize-malware-sales/.

capabilities[29] have been, or could be, utilized to assist domestic authorities under CSE's Mandate C. Furthermore, Canadian law has been used to compel intermediaries to modify their service offerings in order to collect information from their subscribers that would otherwise remain a secret known only to their clients. This was best demonstrated in 2007 when a Canadian-based company, Hushmail, received an order from the Supreme Court of British Columbia.[30] The order required Hushmail to provide the plaintext of three individuals' inbox accounts. Hushmail "modified their product to capture the passwords of the three suspects, which it then used to decrypt the encrypted emails of the three surveillance targets."[31]

Domestic authorities in Canada and the United States also compel mobile telecommunications carriers to provide 'tower dumps'. Tower dumps involve telecommunications providers sharing records of all of the mobile devices that were in proximity to a given cellular tower, and over a particular period of time, as noted in the court order. These, or subsequent, orders can also compel telecommunications providers to identify the persons to whom the devices are registered. A congressional inquiry found that American authorities had made over 9,000 requests for records collected by cellular towers in 2012; with each request affecting between a few hundred or many thousands of persons. In one case the FBI requested cellular tower records to try and identify bank robbers; this caused telecommunications providers to share over 150,000 persons' records in an effort by the FBI to identify just two suspects.[32] In the United States, requests have also forced telecommunications providers to disclose other records such as "GPS location data, Web site addresses and, in some cases, the search terms Americans have entered into their cellphones."[33]

Canadian authorities are no more targeted when requesting cellular tower logs. A case before the Canadian courts, *R. v. Rogers Communications Partnership*,[34] saw Ontario police

---

[29] Communications Security Establishment. (2010). "CSE SIGINT Cyber Discovery: Summary of the current effort," Government of Canada, November 2010, retrieved November 17, 2015, https://www.christopher-parsons.com/writings/cse-summaries/#cse-sigint-cyber-discovery; see also: Christopher Parsons. (2015). "Canadian SIGINT Summaries," last updated June 2, 2015, retrieved November 17, 2015, https://www.christopher-parsons.com/writings/cse-summaries/#cse-sigint-cyber-discovery.

[30] Michael Geist. (2007). ""Private Email Not Always Hush Hush," *Michael Geist*. Published November 26, 2007. http://www.michaelgeist.ca/2007/11/hush-privacy-column/.

[31] Christopher Soghoian. (2012). "The Spies We Trust: Third Party Service Providers And Law Enforcement Surveillance," *Doctoral Dissertation*, July 2012, Pp. 28.

[32] Ellen Nakashima. (2013). "Agencies collected data on Americans' cellphones in thousands of 'tower dumps'," *The Washington Post*, published December 9, 2013, https://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html.

[33] Ellen Nakashima. (2013). "Agencies collected data on Americans' cellphones in thousands of 'tower dumps'," *The Washington Post*, published December 9, 2013, https://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html.

[34] *R. v. Rogers Communications Partnership, 2014 ONSC 3853*.

request log data associated with 40,000-50,000 individuals on the "reasonable grounds to believe that the information sought in the production will afford evidence of the commission of the specific offence being investigated." As a result of these challenges, Canadian authorities are recommended (though not required) to follow non-precedent-setting judicial guidance that would minimize the amount of data that is disclosed to authorities. However, despite this victory, it is unclear just how meaningful the victory was. Specifically, the aforementioned case requested the records on reasonable belief grounds; recent changes to the *Criminal Code* may let authorities request tower dump information on grounds to suspect and, as such, new legal appeals may be needed to test whether tower dumps will be a legally sanctioned way of compelling information from telecommunications carriers.[35]

Authorities also transform *themselves* into intermediaries by exploiting the technical functioning of mobile communications devices. In the United States, government agencies use cell site simulators, often referred to as 'IMSI Catchers', to impersonate cellular towers to either collect mobile devices' unique identifiers;[36] they might also use the devices to intercept data and voice transmissions between mobile devices and other communicants.[37] Attempts in the United States to determine how these devices are used have been routinely stymied by deliberate obfuscations on the parts of authorities using the devices, by freedom of information coordinators responsible to responding to requests about their use under formal freedom of information requests, and by government prosecutors who have misled courts and dropped cases when the use of IMSI catchers might be revealed in open courts.[38] Some of this has begun to change, however, as public pressures and advocacy

---

[35] Christopher Parsons and Tamir Israel. (2016). "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," *Telecom Transparency Project/CIPPIC*, March 2016, URL: Forthcoming.

[36] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, retrieved November 16 2015, pp. 2, http://www.justice.gov/opa/file/767321/download; Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved November 16, 2015, pp. 2, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/11/DHS-department-policy-regarding-the-use-of-cell-site-simulator-2015.pdf; see also: Stephanie K. Pell and Christopher Soghoian. (2014). "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy," *Harvard Journal of Law & Technology* 28(1), http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf.

[37] For a discussion of how IMSI Catchers can operate, see Christopher Parsons and Tamir Israel. (2016). "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," *Telecom Transparency Project/CIPPIC*, March 2016, URL: Forthcoming; Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. (2014). "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," Conference Proceedings of the Annual Computer Security Applications Conference (ACSAC 2014), retrieved Novermber 16, 2015, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf.

[38] See Stephanie K. Pell and Christopher Soghoian. (2014). "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy," *Harvard Journal of Law & Technology* 28(1), http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf.

efforts are not forcing government agencies to publicize their IMSI Catcher usage policies.[39] There is comparably less information about these devices' use in Canada, save that authorities similarly are resistant to disclosing whether the devices are even used or not.[40] No Canadian agency has published a policy document explaining how IMSI Catchers are, or could be, used in the course of either intelligence gathering or an investigation.

Signals intelligence agencies also target foreign and domestic intermediaries. In the United States this involves collaboration between the NSA, domestic authorities, and major American companies under the PRISM program,[41] as well as through arrangements between the NSA and domestic telecommunications companies to provide the NSA with access to domestic and foreign-routed communications.[42] Systems developed by and for the NSA's signals intelligence operations are also accessible, in some cases, to domestic authorities.[43] The Canadian equivalent of the NSA, the Communications Security Establishment (CSE), also engages in domestic telecommunications surveillance[44] which is used for its own purposes (such as developing analytic techniques[45] and monitoring for

---

[39] Department of Justice. (2015). "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Government, September 3, 2015, retrieved November 16 2015, pp. 2, http://www.justice.gov/opa/file/767321/download; Department of Homeland Security. (2015). "Policy Directive 047-01: Department Policy Regarding the Use of Cell-Site Simulator Technology," United States Government, October 19, 2015, retrieved November 16, 2015, pp. 2, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/11/DHS-department-policy-regarding-the-use-of-cell-site-simulator-2015.pdf; *In the Matter of the Application of the United States of America for an Order Relating to Telephones Used by Suppressed*, Docket No. 15 M 0021, https://www.unitedstatescourts.org/federal/ilnd/317964/.

[40] Toronto Police Services Board (Re), Order No MO-3236, [2015] OIPC No 168 (ON IPC), https://www.canlii.org/en/on/onipc/doc/2015/2015canlii54747/2015canlii54747.html; Vancovuer Police Department. (2015). "Re: Records Access Request," September 11, 2015, retrieved November 17, 2015, http://d3n8a8pro7vhmx.cloudfront.net/pivotlegal/mailings/520/attachments/original/2015_09_11_VPD_-_Response_to_FOI_on_Stingray_Device.pdf?1447214666.

[41] National Security Agency. (Unknown). "PRISM/US-984XN Overview or The SIGAD Used Most in NSA Reporting Overview," United States Government, April 2013, retrieved November 17, 2015, https://nsa.gov1.info/dni/prism.html.

[42] National Security Agency. (2014). "Special Source Operations: The Cryptologic Provider of Intelligence from Global High-Capacity Telecommunications Systems," United States Government, not dated, retrieved November 17, 2015, https://www.eff.org/files/2014/06/23/special_source_operations.pdf.

[43] Christopher Parsons. (2015). "'Defending the Code' of the Network: Canadian vs. American Approaches," *Telecom Transparency Project*, June 10, 2015, https://www.telecomtransparency.org/defending-the-core-of-the-network/; Charlie Savage, Julia Ang, Jeff Larson, and Henrik Moltke. (2015). "Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border," *The New York Times*, June 4, 2015, retrieved November 17, 2015, http://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html.

[44] Communications Security Establishment. (2012). "IP Profiling Analytics & Mission Impacts," Government of Canada, May 10, 2012, retrieved November 17, 2015, https://www.christopher-parsons.com/writings/cse-summaries/#ip-profiling.

[45] Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation," in Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press.

attacks entering the Canadian networking infrastructure[46]) and is also available to select federal authorities who receive judicially approved orders to collaborate with CSE under the Establishment's Mandate C.[47] In addition to collecting information from domestic intermediaries, the NSA, CSE, and their 'Five Eyes' allies also target intermediaries outside of their borders to conduct mass surveillance of the world's communications flows.[48]

Poor Government Accountability

Governments themselves have done poor jobs in ensuring the public is kept appraised of the regularity at which government agencies use the aforementioned techniques. They have also failed to keep the public aware of the effectiveness of these techniques. In the United States there are two main kinds of surveillance information that agencies are obligated to publicly report: the number of interceptions conducted by federal agencies as well as the use of pen register and trap and trace orders. These latter two kinds of order reveal communications records in real time, such as phone numbers dialed, the 'To' and 'From' fields associated with email messages as well as "the IP addresses of computers to which a suspect connects."[49] Though the *Pen Register Act* requires US government authorities to extensively document how often such surveillance activities are conducted[50] the federal government has often failed to produce this information; between "1999-2003, there was a single document dump that failed to detail all the information required under the Pen Register Act, and there is no evidence that reports were filed for 2004-2006. All reports include *only* Federal activities; states' actions are not accounted for."[51] In contrast, Administrative Office of the US Courts is statutorily required to produce information on wiretap usage; these reports have been tabled annually and show a significant increase in wiretaps: there were only 637 in 1987 versus 2,376 in 2009. They also provide granular information, revealing "the city or country, the kind of interception (phone, computer,

---

[46] Matt Braga. (2015). "How Canadian Spies Infiltrated the Internet's Core to Watch What You Do Online," *Vice: Motherboard*, February 11, 2015, retrieved November 17, 2015, http://motherboard.vice.com/read/how-canadian-spies-infiltrated-the-internets-core-to-watch-what-you-do-online; Amber Hildebrant, Dave Seglins, and Michael Pereira. (2015). "Communication Security Establishment's cyberwarefare toolbox revealed," *CBC News*, last updated April 2, 2015, retrieved November 17, 2015, http://www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolbox-revealed-1.3002978.

[47] *National Defence Act*, §273.64(1).

[48] As examples, see: Ryan Gallagher. (2014). "Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco," *The Intercept*, December 13, 2014, retrieved November 17, 2015, https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/; Jeremy Scahill and Josh Begley. (2015). "The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle," *The Intercept*, February 19, 2015, retrieved November 17, 2015, https://theintercept.com/2015/02/19/great-sim-heist/.

[49] Christopher Soghoian. (2011). "Law Enforcement Surveillance Reporting Gap (Draft V. 1.1)," Online: http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Soghoian-Surveillance-reporting.pdf

[50] The *Pen Register Act* requires that a list detailing the period of interceptions authorized by order and number, duration, and extension of orders, along with the specific offence(s) under which the order(s) are given be published.

[51] Christopher Parsons. (2012). "Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies," *Technology, Thoughts, and Trinkets*, February 8, 2012, retrieved November 17, 2015, https://dl.dropboxusercontent.com/u/2869620/Lawful-Access-Report-v.2.2Final.pdf.

pager, fax), the number of individuals whose communications were intercepted, the number of intercepted messages, the number of arrests and convictions that resulted from the interception, as well as the financial costs of the wiretap."[52] These reports do not capture the range of state agencies' contemporary surveillance tactics: they do not account explicitly for IMSI catchers, for malware, or for other ways of compelling intermediaries to produce information about subscribers. Nor do they capture the number of times that intermediaries volunteer information to government authorities.

Canada's reporting framework is poor, even compared to the United States'. Canadian authorities are only required to publicly disclose how often they conduct interceptions each year. In contrast to the United States, Canada's federal interception reports reveal that the number of requests made by federal authorities have decreased from almost 1,200 in 1975 to under 200 in 2010. However, there was a 50% increase in the number of persons notified; whereas in 1977 roughly 800 people were notified their communications were intercepted this number rose to approximately 1,200 in 2010. Thus, though fewer interception warrants are issued today, they encompass more people that in the past.[53] These federal reports do not encompass the interceptions conducted by provincial agencies and, based on our experiences, attempting to access provincial governments' historical and contemporary interception reports is not always possible.

There are no Canadian equivalents to pen register and trap and trace reporting requirements. And like in the United States, there are no laws requiring authorities to collect statistics about the use of malware, IMSI catchers, subscriber production requests, or any other mode of state interference or demands placed on intermediaries.[54] And attempts to even ascertain whether government agencies use particular modes of surveillance, such as malware or IMSI catchers, have been rebuffed by both the agencies which would conduct the surveillance as well as Information Commissioners asked to intervene when agencies deny access to records that could explain the policies surrounding such surveillance techniques.[55]

Ultimately, save for the statutory reporting requirements that were put in place several decades ago, authorities in Canada and the United States have not been compelled to compile public reports that summarize how often they use their contemporary surveillance powers and associated devices and techniques. This failure has meant that agencies enjoy

---

[52] Chris Soghoian. (2011). "Law Enforcement Surveillance Reporting Gap (Draft V. 1.1)," Online: http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Soghoian-Surveillance-reporting.pdf.

[53] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 63-4, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[54] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 43-77, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[55] Christopher Parsons and Tamir Israel. (2016). "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," *Telecom Transparency Project/CIPPIC*, March 2016, URL: Forthcoming.

increased surveillance powers without corresponding public accountability for their actions or the costs of those actions.

(b) Intermediaries' Facilitation of Government Surveillance

Intermediaries' business activities can facilitate or inhibit government attempts to gain access to data that the companies transit, process, or retain. In what follows we examine a few of the ways that business processes and network design, data retention, and standards promulgation intersect with government requests for telecommunications data. We also, at the conclusion of this section, discuss the importance of how such requests are governed by the corporation: do companies voluntarily comply with requests for data, apply legal scrutiny to requests, or require judicially approved orders and sometimes contest even those orders' appropriateness? The decisions made by companies with regards to these questions can significantly inhibit, or facilitate state access to intermediaries data and information pertaining to their subscribers.

Network Design and Business Activities

Telecommunications companies that offer similar services, such as broadband Internet, routinely have different networking and data analysis infrastructures.[56] As an example, companies exchange data with one another so that subscribers can send and receive information to persons using different companies' networks. In the United States telecommunications companies 'peer' with one another inside the nation's boundaries. Peering lets carriers directly transfer traffic at to one another and often reduces the costs (transit fees) associated with moving data across the Internet.[57] The locations at which companies peer are the result of technological lock in -- that is, some of these locations simply 'built off' previously existing infrastructure dating back to the telegraph[58] -- and in other cases the consequence of community efforts to exchange data[59] and, in yet other instances, deliberate efforts to improve national peering infrastructures.[60]

Because American telecommunications companies route large amounts of domestic and foreign data traffic at locations within the continental United States, the federal government has sought to monitor the communications passing through these locations. Such monitoring has been targeted at both domestic and foreign communications en

---

[56] Jonathan E. Nuechterlein and Philip J. Weisner. (2005). *Digital Crossroads: American Telecommunications Policy in the Internet Age*. Cambridge, Mass.: The MIT Press.

[57] Rudolph von der Berg. (2008). "How the 'Net works: an introduction to peering and transit," *Ars Technica*, September 2, 2008, retrieved November 17, 2015, http://arstechnica.com/features/2008/09/peering-and-transit/.

[58] Andrew Blum. (2012). *Tubes: A Journey to the Center of the Internet*. Toronto: HarperCollins Publishers Ltd.

[59] Andrew Blum. (2012). *Tubes: A Journey to the Center of the Internet*. Toronto: HarperCollins Publishers Ltd.

[60] Canadian Internet Registration Authority. (2015). "Building a stronger national Internet part 1 - Local Peering," *CIRA*, June 26, 2015, retrieved November 17, 2015, https://cira.ca/blog/building-a-stronger-national-internet-part-1-local-peering.

masse.[61] The successes of the US government to conduct mass surveillance of telecommunications traffic partially stems from these central 'hubs' existing within the United States itself.

To put the American system in contrast, major Canadian telecommunication providers tend not to directly peer with one another on the basis of competitive rationales; smaller competing ISPs experience higher costs when they cannot centrally peer with all ISPs in Canada, including the large providers.[62] As a result, attempts to target peering points for surveillance activities by Canadian authorities meet with a diminished return in comparison to their American counterparts. Business decisions in how, and why, to trade traffic with other Internet service providers can thus have significant impacts on how companies can shape state surveillance activities.

Beyond how intermediaries actually exchange data, companies can influence potential state surveillance capabilities based on how the companies collect and analyze telecommunications data traffic for their own business purposes. In the United States, AT&T researchers built a system in the late 1990s to data mine the company's telephone and Internet access records. It was "originally created to develop marketing leads and as an anti-fraud tool to target new customers who called the same numbers as previously identified fraudsters" but in 2007 "it was revealed that the FBI had been seeking "community of interest" or "calling circle" records from several telecommunications providers."[63] AT&T was able to comply with these requests because of the data mining system it had previously established for legitimate business purposes. One of its competitors, Verizon, could not perform equivalent surveillance for the FBI because it did not have an comparable data mining system.[64]

In a related vein, the period of time for which intermediaries retain data can have significant effects of the availability of information to government agents. In the Canadian context, one of the country's largest home Internet providers, Rogers, must retain records of the Uniform Resource Locators (URLs) that subscribers visit for at least 31 days; these records are needed to modify webpage content in order to notify Rogers customers when

---

[61] Andrew Clement. (2014). "NSA Surveillance: Exploring the Geographies of Internet Interception," *iConference 2014 Proceedings*, retrieved November 17, 2015, https://www.ideals.illinois.edu/bitstream/handle/2142/47305/119_ready.pdf.

[62] Andrew Clement and Jonathan A. Obar. (2015). "Canadian Internet "Boomerang" Traffic and MAss NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges," in Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press.

[63] Christopher Soghoian. (2012). "The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance," Doctoral Dissertation, July 2012, retrieved November 17, 2015, pp. 29, http://files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf.

[64] Christopher Soghoian. (2012). "The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance," Doctoral Dissertation, July 2012, retrieved November 17, 2015, pp. 29, http://files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf. It must be noted, however, that the absence of the system did not prevent the US government from accessing or analyzing communications records. Instead, Verizon and other telephone companies provided the National Security Agency (NSA) with access to call records and the NSA itself performed the community of interest analysis.

they approach their allocated monthly bandwidth capacities.[65] One of Rogers' competitors, Teksavvy, maintains a 0-day retention protocol. One consequence of these different business decisions is that government authorities could request Rogers to divulge a particular subscriber's web history and expect it to be retroactively provided. To get URL records from Teksavvy, however, the same authorities would need to compel Teksavvy to deliberately start keeping logs about a particular subscriber's communications activities, and no retroactive provision of web activity could be provided. In a reversal, Rogers can retroactively provide details of its subscribers' call records going back as far as ten years whereas TekSavvy retains similar records indefinitely.[66]

Telecommunications companies in Canada and the US alike sometimes have similar retention periods because records must be kept per government regulations; in the case of call logs, Canadian companies retain the data to comply with government regulations. However, these minimum logging periods can be, and are, exceeded. There is a relative dearth of information concerning how long such data are maintained in corporate databases, however, and most companies in Canada and the US alike have generally been loathe to divulge their retention times. The result is that individuals are challenged in understanding the potential for their data to be retroactively accessed by government authorities, whereas authorities can ascertain these periods of time by merit of filing requests on companies and then being told the respective companies' data retention periods.

Standardizing and Complying With Government Requests

Many intermediaries receive surveillance or interception requests from government agencies. The precise requests vary based on national laws but, at the most general level, can include interception requests and preservation/disclosure requests. Interception requests involve government authorities asking or compelling intermediaries to capture telecommunications information transmitted or received by a particular person or set of persons in real or near-real time. That intercepted data is either directly provided to the requesting government agency or temporarily held in a storage repository until disclosed to the requesting agency.[67] Federal laws in Canada and the United states empower authorities to make such requests, and internationally agreed upon standards ensure that

---

[65] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 51, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[66] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 50, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[67] For a diagrammatic presentation of this process, see pp. 27 of Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

telecommunications intermediaries can purchase data routing equipment capable of fulfilling such demands.

The vendors of 'lawful interception' equipment certify their compliance with standards from organizations such as the Alliance for Telecommunications Industry Solutions (ATIS) and the European Telecommunications Standards Institute (ETSI), amongst others.[68] Within ATIS, it is the Packet Technologies and Systems Committee Lawful Authorized Electronic Surveillance (PTSC LAES) subcommittee that develops standards for intercepting wireline telecommunications traffic. Specifically, this group develops standards "in response to, legal and regulatory frameworks (per USA CALEA law and related FCC regulation, and Canadian regulations)."[69] There is also a subcommittee focused on wireless technologies (Wireless Technologies and Systems Committee Lawful Intercept). Both groups coordinate with other standards bodies including the ITU so that vendors can continue to sell next-generation networking equipment while ensuring that telecommunications customers can comply with their lawful interception and access requirements.

ETSI provides parallel expertise and develops standards which are taken up by vendors selling products into Europe. ETSI's Technical Committee on Lawful Intercept "determines how to integrate the interception and retention requirements of government agencies into technical specifications" and "also develops and publishes handover interface specifications and the rules for technology-specific interceptions."[70] Core ETSI documents explain to government agencies what must be done to exchange data between telecommunications carriers and government,[71] how different network functions operate and interoperate,[72] and how ETSI-compliant telecommunications systems can interface with government agencies' own reception systems.[73] Both ATIS and ETSI are, in effect, ensuring that

---

[68] For more, see: Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 28-33, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[69] Michael Fargano. (2011). "ATIS Lawful Intercept (LI/LAES) Standards Development," Global Standards Collaboration, October 31-November 3, 2011, Canada, Halifax.

[70] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 30, , https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[71] ETSI. (2001). "ETSI TS 101 331 v.1.1.1: Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf.

[72] ETSI. (2002). "ETSI ES 201 158 v1.2.1: Telecommunications security; Lawful interception (LI); Requirements for network functions," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_es/201100_201199/201158/01.02.01_50/es_201158v010201m.pdf.

[73] ETSI. (2006). "ETSI TS 101 671 v2.15.1: Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_ts/101600_101699/101671/02.15.01_60/ts_101671v021501p.pdf; ETSI. (1999) "ETSI ES 201 671 v1.1.1: Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_es/201600_201699/201671/01.01.01_60/es_201671v010101p.pdf; ETSI.

telecommunications companies can implement new technical systems while ensuring ongoing compliance with national surveillance laws.

Telecommunications intermediaries must procure routing equipment that complies with national surveillance laws. However, these same intermediaries also work in standards bodies to discuss government access standards which exceed lawful requirements. In ETSI, as an example, Canadian telecommunications company Rogers Communications worked with Alcatel Lucent to develop lawful interception systems intended to defeat forward and backward security protections built into communications security protocols such as MIKEY-IBAKE. Specifically, they proposed using pseudo-random, as opposed to truly random, number generation systems so that all communications encrypted using MIKEY-IBAKE could be retroactively decrypted upon request from government agencies.[74] Also at ETSI, telecommunications companies that provided wireline and wireless services discussed the extent(s) to which cloud providers like Google should be required to develop and provide a lawful interception solution for that company's products.[75] In neither the MIKEY-IBAKE or Google examples were there laws proposing or requiring such decryption or data access requirements; instead, the involved parties sought to standardize providing data to government authorities in excess of the law as written.

Perhaps more seriously, companies can exercise significant levels of discretion when voluntarily complying with government requests and with court orders. In the latter case, orders are predicated on either permissive laws (which permit intermediaries to determine whether they will divulge information) or permissive policy decisions adopted by the intermediary. With regards to the former, the laws governing an intermediary may place discretion in the organization's hands. For example, companies located in the United States must comply with the Stored Communications Act (SCA). The SCA differentiates between content and non-content data, as well as between 'government entities' (i.e. U.S. government entities) and non-government entities. US companies can disclose non-content records to these foreign agencies at their discretion, whereas they cannot do the same for US agencies which must serve the company with a court order. Consequently "an internet company can choose whether or not to voluntarily disclose content to foreign law enforcement officers."[76] Other kinds of data, including content information, is primarily accessible to non-American governments through the Mutual Legal Assistance Treaty

---

(2002). "ETSI TR 102 053 v1.1.1: Telecommunications security; Lawful Interception (LI); Notes on ISDN lawful interception functionality," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_tr/102000_102099/102053/01.01.01_60/tr_102053v010101p.pdf.

[74] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 31-32, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[75] Rogers Wireless. (2014). "Web Encryption Discussion," 3GPP TSG-SA3LI, SA3LI #55, October 28-30, 2014, Portland, Or.

[76] Kate Westmoreland and Gail Kent. (2015). "Foreign Law Enforcement Access To User Data: A Survival Guide And Call For Action," SSRN, Last Reviewed January 17, 2015. Last accessed January 22, 2015. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2547289.

(MLAT) process.[77] In a related vein, until mid-2014 telecommunications companies in Canada understood that they were authorized - though not required - to disclose subscriber data to government agencies absent a court order. Such data might include a person's name, address, association with a given Internet Protocol address, and so forth.[78] Legislative efforts throughout the 2000s sought to establish such processes in law, as opposed to in interpretations of law.[79] The consequence of this understanding of the law was that government agencies requested information about hundreds of thousands of Canadians; this practice of disclosing subscriber data to Canadian authorities only (largely) stopped following a Supreme Court of Canada ruling that established the need for authorities to first receive court authorization before requesting this information from telecommunications intermediaries.[80]

Associated with weak legal safeguards for subscribers are poor scrutiny of corporate policies for dealing with requests from government agencies. In the aforementioned subscriber data disclosure scenario, companies had established a system of broadly disclosing subscriber data records upon request despite conflicting case law concerning the appropriateness of such disclosures. The result was that voluntary compliance on the part of telecommunications companies reduced the privacy associated with subscribers' personal data, and without the subscribers ever learning that they had had their information shared with a government agency. Indeed, the full magnitude of the annual disclosures -- roughout 800K subscribers affected, with over 1.1 million requests a year[81] -- followed from journalists learning about the extent of these disclosures two years after the government had tabulated these estimated numbers.[82]

(c) The Role of Intermediaries in Facilitating Transparency

Intermediaries are well positioned to explain what kinds of surveillance they conduct to accommodate government demands or requests, as well as how many requests are received, how often, and the rationales for such surveillance. It simply cannot be left to subscribers to divine such information because they generally depend on intermediaries to safeguard their "personal information and private communications and to prevent that

---

[77] Kate Westmoreland and Gail Kent. (2015). "Foreign Law Enforcement Access To User Data: A Survival Guide And Call For Action," SSRN, Last Reviewed January 17, 2015. Last accessed January 22, 2015. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2547289.

[78] Slane, A., & Austin, L. M. (2011). What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations. *Criminal Law Quarterly*.

[79] Christopher Parsons. (2015). "Stuck on the Agenda: Drawing Lessons from the Stagnation of "Lawful Access" Legislation in Canada," in Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, University of Ottawa Press.

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

[81] 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.

[82] Alex Boutillier. (2014). "Government agencies seek telecom user data at 'jaw-dropping' rates," *Toronto Star*, April 29, 2014, retrieved November 17, 2015, http://www.thestar.com/news/canada/2014/04/29/telecoms_refuse_say_how_often_they_hand_over_customers_data.html.

information from falling into the hands of third parties. This [privilege] gives ISPs power and discretion: power to control our online behaviour and discretion to alter our outcomes."[83] One of the discretions that intermediaries exercise includes notifying customers and potential customers of government surveillance requests. In this section we discuss how companies can disclose surveillance activities to individuals specifically targeted by state surveillance, to the public at large using transparency reporting, and by explaining the policies government agencies must conform to before receiving information from the intermediary in question.

Hacking and Lawful Requests for Data

Governments have increasingly passed legislation which authorizes state agencies to 'hack' their targets using malware, remote exploits, or other digital attacks. In addition to this 'back door' method of collecting data, government agencies can serve formal legal orders on companies. Such lawful orders, which often take the form of interception, preservation, production, or equivalent legal orders, offer a 'front door' method for state agencies to access intermediaries data. In this section we outline how intermediaries could notify specific persons affected by either kind of government data access attempt and the associated limits of current efforts.

Google began warning a subset of its users that they might be the targets of state-sponsored attacks by inserting a warning notification at the top of users' screens when they log into Google properties as of 2012.[84] Google is well situated to conduct analyses of such attacks and provide the warnings because of the company's ability analyze and investigate incoming malware and phishing attacks that are issued from a long list of threat actors and targeted towards a wide range of individuals and organizations. Similar warnings are also provided by Facebook as of October 2015.[85] The notifications from these companies are important because few individuals are positioned to understand whether a particular phishing, spearphishing, or malware attack originates from a commercial, state, or other actor. Moreover, the warnings can help individuals to correlate other abnormal activities to a similar threat actor or set of actors. In effect, these companies' investigations and warnings can help individuals realize the threats facing them and subsequently try to adjust their behaviours to reduce their risks.

However, these notifications systems highlight a correlated problem with informing users of alleged state surveillance activities: the precise methodologies that are used to

---

[83] Ian Kerr and Daphne Gilbert. (2006). "The Role of ISPs in the Investigation of Cybercrime," in T. Mendina & J. J. Britz (Eds.), *Information Ethics in the Electronic Age: Current Issues in Africa and the World*. Jefferson, North Carolina: McFarland, pp. 164-5.

[84] Eric Grosse. (2012). "Security warnings for suspected state-sponsored attacks," *Google*, June 5, 2012, retrieved November 17, 2015, https://googleonlinesecurity.blogspot.ca/2012/06/security-warnings-for-suspected-state.html.

[85] Alex Stamos. (2015). "Notifications for targeted attacks," *Facebook*, October 16, 2015, retrieved November 17, 2015, https://www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766?_rdr=p.

determine who is responsible for an attack are not well publicized.[86] The heuristics or analysis or investigatory techniques that goes into determining whether an attack is state sponsored thus cannot be directly analyzed and validated (or refuted) by the broader security community. Further, there is no indication of *which* country may be engaged in these sorts of sponsored attacks, or whether the US-based companies would notify individuals of a US government-sponsored attack or just of attacks sponsored by non-US government attackers. Notably, the attacks that Google and Facebook alike notify users about are linked to 'hacking' attempts; subscribers whose data is requested using a lawful access tool do not receive equivalent notifications. The result is that even the 'best of breed' analysis and investigation systems that inform specifically affected subscribers have significant deficits.

Beyond notifying specific individuals of having been targeted by a state actor using malware or other attack tools, companies can try and notify individuals whose data is requested by such agencies. When subscribers have their data requested by government agencies, they rarely learn of such requests unless charged with breaking a criminal code. The effect is that their personal information can be captured by government agencies, and used or disseminated amongst such agencies, entirely absent the consent or knowledge of the individual. And, where a criminal charge is not brought against the individual, they may never have an opportunity to contest the legitimacy of the government possessing -- or having requested -- that information in the first place. Only intermediaries are positioned to know whether a subscriber's information has been requested; as such a powerful way for intermediaries to facilitate transparency surrounding state-driven surveillance is to commit to information subscribers of such requests.

Transparency Reports and Policy Guidelines

Beyond notifying individuals about attempts to lawfully access their personal information, companies can issue 'transparency reports' that aggregate the number of time, types, and rationales driving governments' efforts to access subscribers' data. Such reports aggregate statistics about government requests for data, and can include information about the number of warrants or production orders received, the numbers of subscriber accounts affected, number of times that individuals are notified of the requests, and break down the requests as linked to 'normal' criminal investigations, child exploitations investigations, or national security investigations. There may also be an indication whether requests were made by domestic authorities or by foreign agencies using the MLAT process.[87]

---

[86] Facebook, as an example, states that "[t]o protect the integrity of our methods and processes, we often won't be able to explain how we attribute certain attacks to suspected attackers. That said, we plan to use this warning only in situations where the evidence strongly supports our conclusion. We hope that these warnings will assist those people in need of protection, and we will continue to improve our ability to prevent and detect attacks of all kinds against people on Facebook."

[87] For a more extensive discussion of what information transparency reports could contain, see: Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 43-61, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf; Christopher Parsons. (2015). "Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports," *Social Sciences*

To be effective transparency reports must do more than just disclose statistics: they must, ideally, be standardized across an industry so that analysts of the reports can understand the full extents of government agencies' attempts to compel or request information from intermediaries. Where companies have wildly different modes of reporting requests it can be impossible to ascertain the actual number of times requests are made, per year, to intermediaries in similar industry categories (e.g. telecommunications, social). The consequence is that subscribers and analysts alike can be left without a clear understanding of the actual regularity, scope, or common rationales for data requests.[88]

Transparency reports also need to include information concerning a given company's data retention policies; a production order for text messages served on a company that permanently retains all its subscribers' texts will likely produce significantly more data than a company that operates with a thirty-one day retention period. For subscribers to understand the full extent of government agencies' requests, then, retention periods of different types of data must also be disclosed. Failing to provide such information undermines individuals' abilities to determine the number of records which may be accessible to government authorities. Of note, it can be difficult for individuals to ascertain what these retention periods are when they request the retention periods of different data types from intermediaries.[89] Authorities, in contrast, are less likely to run into these knowledge deficits as they can determine record keeping periods by either consulting companies' (private) law enforcement authority guideline handbooks or by speaking with other security and intelligence professionals who have made requests of various intermediaries in the past.

The policies adopted by intermediaries to respond to state agencies' requests are often documented in companies' Law Enforcement Agency (LEA) Guideline handbooks. These sorts of handbooks "include the detailed procedures government agencies must follow to request corporate-held data, the kinds of identification government agencies must present before information will be disclosed, the time for corporations to process requests, and the costs agencies must pay for the requests to be processed."[90] Companies can choose to publish these handbooks and, in the process, clarify to government agencies and subscribers alike "what kinds of data the company stores, for how long, and under what terms it can be (and is) released" while also clarifying to subscribers "exactly how a TSP

Research Network, last revised January 14, 2015, retrieved November 17, 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546032.

[88] Christopher Parsons. (2015). "Restoring Accountability for Telecommunications Surveillance In Canada," *The Mackenzie Institute*, August 11, 2015, retrieved November 17, 2015, http://www.mackenzieinstitute.com/restoring-accountability-telecommunications-surveillance-canada/; Christopher Parsons. (2015). "Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports," *Social Sciences Research Network*, last revised January 14, 2015, retrieved November 17, 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546032.

[89] In Canada, efforts to learn about intermediaries data retention periods were largely fruitless despite availing themselves to a range of advocacy and legal tactics. For more, see: Andrew Hilts and Christopher Parsons. (2014). "Enabling Citizens' Rights to Information in the 21st Century," *The Winston Report*, Fall 2014.

[90] Christopher Parsons. (2015). "Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports," *Social Sciences Research Network*, last revised January 14, 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546032.

handles their personal information … when presented with different kinds of court orders."[91] Intermediaries routinely receive requests from foreign state agencies for access to corporate data and these handbooks can also clarify "how the company must process foreign authorities' requests for company-held data, identify whether customers are notified of either domestic or foreign authorities' requests, outline the period of time the company can take to respond to requests, and state whether the costs incurred in fulfilling the government request must be compensated or not."[92] Centrally, these handbooks establish what exactly a company retains, for how long, and under what conditions it may disclose particular subscribers' information to government agencies. This stands in contrast to the more common practice of companies keeping such handbooks or policies internal to a company and, thus, not opening their practices to public evaluations. In the US several companies, predominantly Internet companies such as Yahoo!, Microsoft, and Google have either published their law enforcement guideline handbooks or had them leaked to the public. No Canadian companies have published correspondingly detailed handbooks.

Companies can also demonstrate their commitment to subscribers' privacy by contesting overbroad requests for data. Companies such as Google and Facebook, as well as telecommunications companies including TELUS and Rogers, contest overbroad requests. And transparency reports by many companies indicate the number of times that agencies' requests are refused. Such scrutiny of agencies' requests serves a double purpose. First, it indicates to subscribers that their intermediaries are careful in disclosing their personal information and thus the actions can build trust between subscribers and the company in question. Second, it can indicate to government agencies that they must carefully target their requests and that superfluous requests will be refused by the intermediary. As a result, such commitments to evaluate legal orders can promote better cultures within government agencies of ensuring that they need, and have lawful authority to access, data stored by intermediaries.

All of the aforementioned intermediary transparency information are limited insofar as they tend to either not disclose, or cannot holistically account for, intrusions into intermediaries' own infrastructures by unauthorized parties. In the wake of Edward Snowden's disclosures it has become apparent that government agencies employ both 'front door' tactics to gain information from intermediaries (through lawful access mechanisms) as well as 'back door' tactics (through hacking into intermediaries' infrastructures). The Snowden disclosures, as an example, revealed that a program codenamed PRISM was used by the NSA to access large volumes of data held by some of the largest Internet intermediaries in the United States, including Microsoft, Yahoo!, Google,

---

[91] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 54, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[92] Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, retrieved November 17, 2015, pp. 54, https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

and Apple, amongst others. The PRISM program was a 'front door' program that depended on formal legal requests. In contrast, the NSA also ran 'back door' operations to collect information from these same intermediaries. The MUSCULAR program, as an example, involved the NSA monitoring data transfers between Google's and Yahoo!'s data warehouses outside of the continental United States.[93] While technical solutions to prevent these particular backdoor tactics were deployed once Google was appraised of the activity[94] it nevertheless demonstrates a problem of transparency efforts: to date, these corporate transparency cannot effectively capture *all* the methods of state access to data carried, processed, or stored by intermediaries simply because intermediaries may not *know* how government is accessing such data.

Moreover, governments have established limits on how companies can report on national security-related requests for intermediaries' data. In the United States, intermediaries can only disclose they have received National Security Letters (NSLs) in ranges of between 249 or 999.[95] Thus, companies can state they have received between 0 and 999 of these letters, or 1,000 to 1,999, and so forth. Fundamentally this means intermediaries cannot firmly tell their subscribers or the public writ large that they have, or have not, received an NSL, nor the expansiveness of any NSLs they have received. Some companies have resorted to publishing 'warrant canaries' on their webpages, which affirm that the company has not received a national security-related request. The theory is that when and if these warrant canary statements vanish from the intermediaries' websites that the public can intuit that they have received such a request.[96] The problem, however, is that companies routinely fail to update their canary statements (thus making it seem like the canary has 'died')[97] or modify their corporate disclosure policies which leads the public to believe the company has received a request.[98] No intermediary in Canada has adopted warrant canary language, and guidelines published by Industry Canada would severely restrict the specificity of intermediaries' transparency reporting.[99]

---

[93] Barton Gellman and Ashkan Soltani. (2013). "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post*, October 20, 2013, retrieved November 17, 2015, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?hpid=z1.

[94] Sean Gallagher. (2013). "Googlers say "F*** you" to NSA, company encrypts internal network," *Ars Technica*, November 6, 2013, retrieved November 17, 2015, http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/.

[95] Electronic Privacy Information Center. (2014). "National Security Letters," *EPIC.org*, retrieved November 17, 2015, https://epic.org/privacy/nsl/.

[96] Naomi Gilens. (2015). "The NSA Has Not Been Here: Warrant Canaries As Tools For Transparency In The Wake Of The Snowden Disclosures," *Harvard Journal of Law & Technology* 28(2), http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech525.pdf.

[97] See: https://news.ycombinator.com/item?id=8796307; https://news.ycombinator.com/item?id=9162186.

[98] Jeff Roberts. (2014). "Apple's "warrant canary" disappears, suggesting new Patriot Act demands," *Gigaom*, September 18, 2014, retrieved November 17, 2015, https://gigaom.com/2014/09/18/apples-warrant-canary-disappears-suggesting-new-patriot-act-demands/.

[99] Christopher Parsons. (2015). "Industry Canada Transparency Report Guidelines Intensely Problematic," *Telecom Transparency Project*, June 30, 2015, retrieved November 17, 2015,

Intermediary transparency, then, is a complicated subject. The best of breed efforts are often confusing to readers and analysts, or not directly comparable across all members in an industry category. And the reports either gloss over or fail to account for back door attempts to access data processed, collected, or retained by given intermediaries. The result is that we cannot expect intermediary transparency to be the full solution to exposing government surveillance activities but, instead, part of a broader effort to understand the scope and implications of government activities. Governments themselves must become more transparent and accountable for their activities; failing to do means that legislators cannot hold the government to account and surveillance of communications continue without a meaningful way of understanding, let alone contesting, the ways in which the government intrudes into citizens' private lives.

(d) Implications of Non-Transparent State Surveillance

The secrecy surrounding contemporary state surveillance methodologies creates a chilling environment wherein individuals cannot know whether intermediaries may intercept or disrupt communications on the basis of either corporate practice or government demand. Such an environment establishes a chill on political speech, writ broadly, for at least three reasons.

First, the laws that states exercise to disrupt or monitor speech are often poorly understood by legislators and the electorate both. In many cases, the laws government may use to censor speech itself rest on secretive interpretations of law, with the consequence that neither citizens or legislators are genuinely 'responsible' for law. As a result, in such situations citizens cannot be understood as democratically legitimizing law, nor their representatives as acting on their constituents' behalves, to the effect of transforming citizens into serfs subject to governmental edict.

Second, secretive or opaque telecommunications surveillance has the effect of discouraging members of the population from taking part in 'risky' speech or activity online on the basis that government or agents working alongside the government might be monitoring for particular activities. The relative secrecy concerning what is 'risky' in and of itself exacerbates this problem. No state that strongly supports democratic norms such as freedom of speech, association or freedom from unwarranted searches will presumably thrive over time under such conditions.

Finally, revelations concerning corporate and government surveillance alike are significantly predicated on corporate generosity, such as transparency reports, whistleblowers, in terms of national security disclosures, or lengthy adversarial journalism pieces. While these tactics are essential to understanding how intermediaries are invested in monitoring and affecting communications flows they do not provide the equivalent degree of information that government itself might produce, nor are comprehensive accounts of corporate involvement typically included. The result is that citizens tend to

---

https://www.telecomtransparency.org/industry-canada-transparency-report-guidelines-intensely-problematic/.

only possess limited volumes of information that are significantly lacking in detail, comprehensiveness, or evidentiary accuracy.

At a high level, telecommunications surveillance establishes chilling conditions that are accentuated by poorly implemented or limited corporate transparency methods that are 'complemented' by weak government statutory accountability practices. These lacking information disclosure practices in tandem with opaque interpretations of law mean that government and intermediaries can operate outside of the public eye and without citizens' authorizations for such kinds of activity. Though the surveillance conducted by government bodies and corporations alike can serve a useful function in maintaining order and social peace the surveillance itself should be authorized by citizens/consumers. Failing to do so risks the long-term normative principles of democratic nations for the short-term gains of contemporary social stability that is predicated on secret law, secret surveillance, and secret weakening of basic democratic rights.