Canada's National Security Consultation I: Digital Anonymity & Subscriber Identification Revisited… Yet Again

October 6, 2016

Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), Centre for Law, Technology & Society (CLTS), University of Ottawa, Faculty of Law

Christopher Parsons, Research Associate & Managing Director, Telecom Transparency Project, Citizen Lab, Munk School of Global Affairs, University of Toronto

Last month, Public Safety Canada followed through on commitments to review and consult on Canada's national security framework. The process reviews powers that were passed into law following the passage of Bill C-51, Canada's recent controversial anti-terrorism overhaul, as well as invite a broader debate about Canada's security apparatus. While many consultation processes have explored expansions of Canada's national security framework, the current consultation constitutes the first modern day attempt to explore Canada's national security excesses and deficiencies. Unfortunately, the framing of the consultation demonstrates minimal direct regard for privacy and civil liberties because it is primarily preoccupied with defending the existing security framework while introducing a range of additional intrusive powers. Such powers include some that have been soundly rejected[1] by the Canadian public[2] as drawing the wrong balance between digital privacy and law enforcement objectives, and heavily criticized by legal experts[3] as well as by all of Canada's federal and provincial privacy commissioners.[4]

The government has framed the discussion in two constituent documents, a National Security Green Paper[5] and an accompanying Background Document.[6] The government's framings of the issues are highly deficient. Specifically, the consultation documents make little attempt to explain the privacy[7] and civil liberties implications that can result from the contemplated powers. And while the government is open to suggestions on privacy and civil liberties-enhancing measures, few such proposals are explored in the document itself. Moreover, key commitments, such as the need to impose judicial control[8] over Canada's foreign intelligence agency (CSE) and regulate the agency's expansive metadata surveillance activities, are neither presented nor discussed (although the government has mentioned independently that it still hopes to introduce such reforms).[9] The consultation documents also fail to provide detailed suggestions for improving government accountability and transparency surrounding state agencies' use of already-existent surveillance and investigative tools.

In light of these deficiencies, we will be discussing a number of the consultation document's problematic elements in a series of posts, beginning with the government's reincarnation of a highly controversial telecommunication subscriber identification power.

Access to Basic Subscriber Identifiers: Past Attempts to Legislate

Successive federal governments have sought to legislatively enshrine a state power to access subscriber identification data from telecommunications companies. Such legislative initiatives would have facilitated access to such data on an indiscriminate basis and without any judicial

authorization or control. All of these attempts have proven controversial and each has fallen in the face of public resistance. At the same time, government agencies, such as the Royal Canadian Mounted Police (RCMP) and provincial and municipal policing bodies, have routinely asserted that they need rapid access to such information, and that judicial authorization will impede their ability to develop investigations.

State agencies first raised the prospect of warrantless access to subscriber identifiers in a consultation document[10] issued by the Department of Justice in 2002. That document presented the warrantless access power as one of several ways to obtain subscriber identification information. Since that time, a number of legislative initiatives have sought to introduce administrative powers that would let state agencies compel the disclosure of various digital identifiers without any judicial control. Such powers were always introduced as part of a broader legislative package referred to as 'lawful access'.

Underpinning these various lawful access initiatives has been the claim that digital identifiers should be generally accessible to law enforcement without a warrant and indiscriminately (that is, without the need to first obtain grounds for suspicion that the identifier sought would assist in solving a crime). The rationale advanced for this warrantless regime has been that subscriber identification is simply not that private, as well as an ever-shifting list of pressing needs invoked in justification of the initiative (including, at various times, electronic crimes,[11] child pornography[12] and now national security). These efforts culminated in Bill C-30, which met with strong public opposition and, ultimately, legislative defeat. Lawful access legislation was later re-introduced and passed, but the warrantless subscriber identification regime (which was the object of heavy criticism) was explicitly omitted.

In spite of a definitive rejection[13] of these measures by the Canadian public (other, less controversial parts of Bill C-30 were ultimately passed into law as Bill C-13, this time presented as a presented as a solution to cyberbullying),[14] the government has now resurrected proposals for indiscriminate access to subscriber identification data. Subscriber identification data typically refers to unique number strings assigned to individual subscribers and their networked devices as a means of identifying these subscribers in digital interactions. They can include a subscriber's name, home address, telephone number or Internet Protocol address. The consultation documents paint a familiar picture in attempting to make the case for warrantless and indiscriminate access to subscriber identification data. As in past justification attempts, "slow and inconsistent access to basic subscriber information to help identify who was using a particular communications service at a particular time" is identified as an impediment to effective law enforcement. The warrant process -- seen by many Canadians as the centrepiece of a balanced policing system -- is presented as a time-consuming inconvenience engaging "considerable work and resources." Limiting access to digital identifiers of actual suspects is presented as a disproportionate obstacle to investigations that should normally be reserved for "situations involving greater privacy intrusions." The consultation documents even rely on the same historical analogies advanced repeatedly over the years, implying that access to digital identifiers is no more private than "looking up an

address in a phone book or checking out a license-plate number." While past discussions have been framed in terms of child pornography and cyber-bullying, the consultation documents advance national security as the cause du jour. However, as in the past, the power is presented as one of general application meaning that national security scenarios will constitute a small fraction of the situations in which the power is ultimately invoked.

The government's re-ignition of this debate is surprising considering that no new arguments are advanced in the consultation documents since the warrantless indiscriminate powers it advances were last rejected. Equally surprising is the one-sided manner in which the issue is presented by the consultation documents given the rich discussion that has accompanied debate of this issue in the past. Specifically, as described below, no account is given of the privacy implications that arise when state agencies are provided the power to indiscriminately identify any online activity without prior judicial authorization.

Digital Identifiers: the Key to Detailed Profiling & Online Anonymity

The government's consultation documents present basic subscriber identification information as less private than other types of data used in state investigative contexts. Specifically, access to digital identifiers is presented by the consultation documents as equivalent to "looking up an address in a phone book or checking out a license plate number". However, in the modern age, digital identifiers are left behind like indelible footprints in all of our virtual and, increasingly, real-world interactions. The ability to connect these digital footprints with real-world identities leaves little room[15] for anonymous activity, expression or exploration of ideas, and even for anonymous movement[16] in the physical world.[17] While state agencies should have latitude to identify individuals associated with activity reasonably believed to be criminal or otherwise threatening, the consultation documents describe a much broader power that would permit indiscriminate identification of almost *any* anonymous activity.

The consultation documents define basic subscriber information as "identifying information that corresponds to a customer's telecommunications subscription." The proposal does not specify a definitive list of identifying information that will be included in the power it proposes. However, past attempts to introduce warrantless access to subscriber information adopted the following legislative definition:

> ... any information in the service provider's possession or control respecting the name, address, telephone number and electronic mail address [email address] of any subscriber to any of the service provider's telecommunications services and the Internet protocol address [IP address], mobile identification number, electronic serial number, local service provider identifier, international mobile equipment identity number [IMEI], international mobile subscriber identity number [IMSI] and subscriber identity module [SIM] card number that are associated with the subscriber's service and equipment. (Bill C-52, section 16)[18]

The consultation documents indicate that each of these identifiers could be included within the new power it contemplates, while acknowledging that indiscriminate warrantless access may

be more appropriate for some of these identifiers than it is for others. However, in reality, most of the identifiers envisioned by this new power can have serious privacy implications deserving of protection.

Telephone numbers and home addresses, for example, have historically been fairly easy to uncover, with most available in public listings such as the white pages. Today, however, many Canadians have unlisted phone numbers. This means that they have made the decision to *not* provide their address in a phone book, demonstrating an intention to keep this information private. The trend is more pronounced with regard to mobile phone numbers, which are commonly kept private as a means of avoiding telemarketers.[19] For those Canadians that do list their phone numbers and addresses, however, the phone book will only reveal the name the number is listed under (not always a full, or wholly accurate, full and last name), the address, and phone number. The government is proposing a dramatic expansion of 'phone book' information. It would go from three data points to six or more items, including Internet Protocol (IP) addresses, name, home address, phone number, email address, and mobile devices' IMSI number.

IP addresses can be extremely private insofar as they can used to expose an individual's detailed biographical profile. In most digital interactions, IP addresses are left behind as a byproduct of most digital interactions. The websites we visit, the message boards we comment on, the YouTube videos we upload or view, the files we download,[20] and the online purchases we make will often generate a record tied to us by our IP address. Given the richness of modern day online activity, it is possible to compile a detailed profile[21] by correlating different activity associated with an IP address. As online activity is often sensitive, associating an IP address with even one single anonymous interaction can be highly revealing of sensitive personal information.[22] Once an IP address is correlated with an individual, it can readily reveal future private perspectives or activities[23] as well. The ability to conduct anonymous online activity is important to the exploration of ideas and to expression of a wide range of views. Research has shown[24] that the possibility of indiscriminate surveillance can chill online activity and particularly the anonymous exploration and discussion of potentially controversial topics. The indiscriminate subscriber information power contemplated by the government's consultation document would permit state agents to compel telecommunications service providers such as YouTube, Reddit, Ashley Madison, Gmail, or others to provide IP addresses associated with online activity, and to then compel ISPs such as Teksavvy, Rogers or TELUS to disclose real-world identities associated with those IP addresses. The harms of such an indiscriminate power to identify individuals associated with anonymous online activity could be far reaching.

Online identifiers such as IP addresses and email addresses can also be used by state agencies to develop[25] a rough map of where a person has physically visited. Digital identifiers associated with mobile devices, such as the IMSI and IMEI numbers, are even more conducive to facilitating real-world tracking. Much like IP addresses, IMSI and IMEI numbers, which are uniquely associated with cellular subscribers and devices, respectively, are collected by cellular

towers as individuals move around their city.[26] The indiscriminate identification power contemplated by the consultation document could therefore operate as a real-world tracking power. It is framed in a manner that could be used to compel a mobile service provider to disclose, for example, all IMSI / IMEI numbers that were collected by a given set of cell towers at a given time. This would, by extension, identify all individuals who were at that location within the given time (for example, during a bank robbery, cultural event, or a political protest).

Anonymous activity is increasingly recognized as attracting high expectations of privacy and anonymity in particular is seen as an important constitutional value in the digital ecosystem. As our digital and physical activities increasingly generate 'some' record and occur in semi-public spaces, anonymity has become integral to maintaining any meaningful semblance of privacy. As noted by then-UN Special Rapporteur Frank La Rue, the "[a]nonymity of communications is one of the most important advances enabled by the Internet, and allows individuals to express themselves freely without fear of retribution or condemnation." The Privacy Commissioner of Canada has also acknowledged[27] the importance of protecting basic subscriber identifiers, as these are "sensitive in nature in that [they] can be used to determine a person's leanings, with whom they associate, and where they travel … each of these pieces of information can be used to uncover further information about an individual." The Supreme Court of Canada came to the same conclusion in *R v Spencer*, 2014 SCC 43:

> Anonymity permits individuals to act in public places but to preserve freedom from identification and surveillance. … [s]ubscriber information, by tending to link particular kinds of information to identifiable individuals, may implicate privacy interests relating to a person's identity as the source, possessor or user of that information … the police request to link a given IP address to subscriber information was in effect a request to link a specific person to specific online activities. This sort of request engages the anonymity aspect of the information privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized in other circumstances as engaging significant privacy interests.

The Ontario Superior Court of Justice has likewise recognized an enduring privacy interest[28] that is engaged where state agencies seek to obtain mobile phone information for the purpose of locating individuals, as have the Information & Privacy Commissioners of British Columbia and Ontario, in the context of cell phone tracking[29] and indiscriminate automated license plate tracking.[30]

There is no doubt that such identification capabilities can be useful to state agencies in the course of legitimate investigations. However, while it is generally open to the government to empower itself to access data on a more permissive basis where there is a lower expectation of privacy, the sensitivity of the information revealed by subscriber identification demands a higher level of protection. Moreover, as elaborated in the following section, there is no practical justification for granting state agencies indiscriminate access to such identification capabilities. Basic digital identifiers can be used to develop a detailed composite picture of an individual

based on who they associate with, where they visit or travel, and whom they communicate with. Indiscriminate access to such identifiers threatens to chill association and speech. In the next section we discuss why warrants do not pose an impediment to police investigations and how they can facilitate greater trust in government's use of investigatory powers.

Indiscriminate Access to Digital Identification: Has the Case Been Made?

In addition to implying that subscriber identification information is not very private, the consultation documents advance some pragmatic arguments to try and justify indiscriminate access to subscriber identification information. The consultation documents claim that the current general production power relied upon by state agencies is not effective at obtaining subscriber identification information in a timely manner and that the need to obtain prior judicial authorization is generally inconvenient. The documents also argue that following a recent Supreme Court of Canada decision that acknowledged a privacy interest in IP addresses, *R v Spencer*, 2014 SCC 43, obtaining subscriber identification information has become more difficult. The consultation documents advance two types of relief to address these perceived challenges, and resemble past attempts to introduce such a power:

- access to digital identifiers should be available to state agencies without the need to obtain prior authorization from a judge; and
- access to digital identifiers should be available to state agencies indiscriminately, even where these agencies have no reason to believe the subsequent identification will help prevent a crime or advance an investigation.

This section will explain that while there is a gap in Canada's current electronic surveillance framework with respect to subscriber identification information that can be filled by carefully formulated legislation, the proposals advanced in the consultation document offer no such tailored proposal. Instead, the consultation document constitutes yet another installment in the government's repeated attempts to provide state agencies with unfettered access to highly sensitive identifying information, this time putatively in the name of national security.

Currently, law enforcement agencies seeking access to subscriber information generally rely on a general production order (section 487.014 of the *Criminal Code*) to compel service providers to disclose this information. The consultation documents suggest that the *Spencer* decision, which held that digital identifiers (notably, IP addresses) are too sensitive for state agencies to obtain from service providers on an informal and voluntary basis, has imposed a new barrier for state agency investigative activities. The consultation document significantly overstates the investigative impact of *Spencer*, however. While the *Spencer* decision did, indeed, impact on some voluntary sharing of identifying information by ISPs, such voluntary sharing was only regularly available to law enforcement in the context of child pornography investigations as part of a program adopted by major Canadian ISPs for that context alone[31] (p 47). The decision would therefore impose minimal impedance in the national security context specifically, and in other law enforcement contexts generally.

The consultation document also argues that the general production power in section 487.014

of the *Criminal Code* was not introduced for accessing subscriber data. However, neither the legislative history nor historical practice of this power lend support to that proposition. Legislatively, the general production power was first introduced in 2003[32] and became law in 2004,[33] with the express purpose of facilitating access to digitized data records in a timely manner, as noted by the government upon its first introduction of the new power:

> Law enforcement agencies and crown prosecutors have been asking for a new investigative tool for some time and with the proliferation of the Internet and the widespread adoption of new communications technologies, the timing is right for this form of investigative tool. The production orders will solve a number of nagging issues for investigators including extraterritorial searches and timing issues. … [T]he new production orders will be time sensitive so that the third party served with the order will either have to produce the information within the time specified in the order or report back to the court within the specified time as to why he or she cannot comply. This solves the problem of the inherent nature of informal arrangements which is they are informal and they often lack specific mechanisms such as timing mechanisms. [at 1635][34]

This was, in fact, the legislative response to a 2002 Department of Justice consultation document[35] which explicitly outlined the need for production powers to access digitized records, including telecommunications services subscriber information. Parliament explicitly chose to introduce a general production power for all computer data records, foregoing the adoption of an additional specific production order for subscriber data.

Perhaps more importantly, since the introduction of the general production power, law enforcement have consistently and successfully relied upon such orders to obtain subscriber identification data from telecommunications companies in large volumes. Halifax Regional Police, for example, compelled production of telecommunications subscriber identification data approximately 4,507 times while only relying on voluntary disclosure by service providers 2,354 in the largely pre-*Spencer* period spanning January 2011 - December 2014. During the same period, the Vancouver Police Department obtained 25,189 production orders for subscriber identification data while relying on voluntary disclosure only 13,407 times. The general production power therefore enjoys a long track record of success in many investigative contexts. Indeed, past iterations of this justification exercise have similarly struggled to demonstrate[36] any *actual* shortcomings in the existing framework, with internal law enforcement emails[37] demonstrating an inability to find "sufficient quantity of credible examples" in support of unfettered access to subscriber identification data. [Data obtained by Dr Christopher Parsons by means of Provincial right to information regimes and on record with the author. Halifax Regional Police Dataset.[38] Vancouver Police Department Dataset.[39]]

While the *Spencer* decision may have affected the ability of law enforcement investigations in one particular investigative context where ISPs had historically agreed to voluntarily identify Internet customers without a warrant,[40] that investigative context raises no special challenges to render general production orders ineffective. These investigative scenarios (documented in

dozens of judicial decisions where criminal charges were actually laid against the individual in question after identifying information was obtained) overwhelmingly conform to a template: anonymous online activity (namely, the anonymous downloading or uploading of demonstrably unlawful child pornography) is associated with an IP address and law enforcement seeks to connect this IP address (and the anonymous activity in question) to a real-life identity. None of these situations occurred under conditions that would present an obstacle to obtaining a general production order - all exhibit clear grounds for suspicion and no time pressures that could possibly be frustrated by seeking judicial authorization. Even arguments pointing to the inconvenience involved in documenting evidence in order to obtain a production order ring hollow, as the investigative trail must be carefully documented if law enforcement hopes to successfully present the evidence in a criminal trial or as justification for further search powers.

There is simply no demonstrable need for providing unfettered access to digital subscriber identification data. On the other hand, once relieved of the obligation to demonstrate the existence of a reasonable basis for believing that the identification data sought will provide evidence of a crime, law enforcement appears to cast a very broad net. Prior to the *Spencer* decision, for example, telecommunications service providers received immense numbers of requests for voluntary disclosure of customer data, reaching[41] over 1.1 million requests in 2011 alone. This high volume of requests (implicating close to 800,000 Canadians or about 5% of the population in a single year) suggests that the voluntary regime was being used well outside its stated parameters. While no consistent statistical reporting is available to uniformly assess the proportionality of these measures, there are relatively few judicial decisions in which convictions were ultimately obtained on the basis of these millions of non-judicial and indiscriminate requests.

To the extent there is a gap in Canada's electronic surveillance regime with respect to the ability to access subscriber identification information, it rests solely in situations where there is an imminent threat of harm to life. While police do not need a warrant to enter and search premises in such exigent contexts, and can even conduct emergency wiretaps (subject to strict conditions),[42] they do not have the power to compel a service provider to produce subscriber identification data without a court order. This gap is not well documented, and is unlikely to have impeded law enforcement in many actual situations where a threat of harm to life arose. This is because most service providers will voluntarily comply with reasonably framed requests for subscriber identification information sought under exigent conditions. Such voluntary sharing remains constitutional under the Supreme Court of Canada's *Spencer* framework [paras 71-74].[43] However, explicitly recognizing an emergency subscriber identification power could provide consistency and help ensure that access is not frustrated by fringe service providers. A properly formulated and explicit emergency subscriber identification power can also address potential *Charter* implications arising from the current voluntary regime, which lacks any accountability measures whatsoever,[44] while ensuring emergency powers are not misused. Such misuse is far from unlikely - the US Office of the Inspector General, for example, found in 2007 that the US FBI had frequently misused emergency subscriber identification

access powers[45] in order to avoid its non-emergency authorization regime. A properly formulated emergency access power would therefore include statistical reporting, individual notification and 'report back' obligations to secure some level of *ex post* accountability.

Finally, while there is no demonstrable need for a departure from the existing general production power regime, it is certainly open to the government to formulate a specialized production power for subscriber identification. The government has, indeed, introduced such specialized production powers for different types of data, including tracking data, communications tracing data and transmission data. Such a power, however, must be reasonably formulated and commensurate with the highly sensitive privacy interests it engages.[46] This would require at bare minimum an obligation to demonstrate grounds that the identifying information sought will help prevent an anticipated crime or investigate a historic one. It should also include *ex post* accountability measures as well as retention limitations. (The authors note that David Fraser has drafted[47] an eminently reasonable proposal for a specialized subscriber identification production power).

Conclusion

In keeping with past attempts to introduce an unfettered digital identification power, the consultation documents have failed to make the case that such indiscriminate powers are needed. The documents repeat long enduring claims that current access mechanisms are 'inconsistent and slow', but fail to acknowledge the fact that such claims have been repeatedly discredited[48] in the past. Moreover, the government has failed to explain to the public that law enforcement have long relied on existing production powers to access subscriber identification information in all but a few narrow investigative contexts.

Perhaps worse, in making its pitch to the public, the consultation document revitalizes an ill-considered and outdated characterization of digital identifiers as 'not so private'[49] - a characterization that has been flatly rejected by the general public[50] in its opposition to past iterations of the unfettered identification power it proposes, by multiple evidence-based[51] research reports[52] demonstrating its far-reaching capacity to invade and by the Supreme Court of Canada.[53] Replicating a trend that is regrettably evident throughout the consultation documents, the documents treat privacy in subscriber information as, at best, an afterthought. By ignoring the rich and detailed historical debate that has occurred in Canada on this matter the government has failed to acknowledge the privacy issues associated with indiscriminate access to digital identification.

Finally, while it is encouraging that the government is willing to engage in a public consultation prior to setting its national security agenda, it is disappointing to see yet one more cause du jour invoked in justification of what is clearly intended to be a generalized policing tool. In the context of this national security consultation, unfettered access to digital identifiers is presented as a national security measure intended to address critical counter-terrorism matters that are currently at the forefront of national attention and concern. However, as in past attempts to introduce this legislation, the power proposed is one of general application, meaning it will be used predominantly in other investigative contexts. Further, no specific explanation is provided

for why this exceptional power is necessary even in the national security context. Indeed, upon the 2013 defeat of this proposal as embodied in Bill C-30, then Director of CSIS (an agency with broad counter-terrorism responsibilities) indicated[54] that unfettered access to subscriber identification information is "not absolutely critical for us to do our work." While on the one hand these identification powers may not be 'absolutely critical' to national security, their indiscriminate availability to agencies such as CSIS and CSE can have even more serious and far-reaching privacy implications, which will be explored in a future post.

Anonymity is one of the most important bastions of privacy in the digital world. As eloquently explained[55] by UN Special Rapporteur David Kaye, along with encryption:

> … anonymity, today's leading vehicles for online security, provide[s] individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.

This does not mean that individuals can hide behind anonymity so as to commit crimes with impunity. However, de-anonymizing individuals does demand a carefully considered, narrowly tailored, and proportionate authorization mechanism that is commensurate with the important constitutional and democratic values it implicates. Yet the consultation documents wholly disregard these important values in yet another attempt to justify an unfettered and uncontrolled power to identify online activity. It is perhaps unsurprising that no reasonably tailored and proportionate proposal is evident in its resulting treatment of online identification.

List of Referenced Hyperlinks

[1] http://www.cbc.ca/radio/day6/episode-236-transgender-parenting-trauma-and-genetics-bobby-baun-gun-lobbyists-vs-bill-c-51-more-1.3098757/why-conservatives-libertarians-and-gun-lobbyists-oppose-bill-c-51-1.3098851

[2] http://poll.forumresearch.com/post/256/most-see-bill-having-negative-effect-on-their-lives/

[3] https://bccla.org/news/2012/01/report-says-canada-moving-towards-a-surveillance-society-with-lawful-access-proposals/

[4] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2011/let_110309/

[5] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016/ntnl-scrt-grn-ppr-2016-en.pdf

[6] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf

[7] https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar_201516/

[8] http://luxexumbra.blogspot.ca/2015/10/cse-related-items-in-liberal-platform.html

[9] http://www.theglobeandmail.com/news/politics/privacy-watchdog-urges-ottawa-to-pass-metadata-legislation/article32094827/

[10] http://www.canada.justice.gc.ca/eng/cons/la-al/la-al.pdf

[11] http://www.parl.gc.ca/content/hoc/Bills/403/Government/C-52/C-52_1/C-52_1.PDF

[12] http://www.parl.gc.ca/content/hoc/Bills/411/Government/C-30/C-30_1/C-30_1.PDF

[13] http://www.michaelgeist.ca/2013/02/bill-c-30-dead/

[14] http://www.cbc.ca/news/politics/cyberbullying-bill-raises-alarm-for-privacy-commissioner-1.2842034

[15] http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

[16] http://www.pnas.org/content/113/20/5536.full

[17] https://privacyinternational.org/node/573

[18] http://www.parl.gc.ca/content/hoc/Bills/403/Government/C-52/C-52_1/C-52_1.PDF

[19] http://crtc.gc.ca/eng/info_sht/t1048.htm

[20] https://www.christopher-parsons.com/writings/cse-summaries/#levitation-and

[21] https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar_201516/

[22] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

[23] https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/

[24] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

[25] https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/

[26] https://cippic.ca/en/news/report_calls_for_proactive_transparency_and_control_of_IMSI_catchers

[27] https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/

[28] http://www.canlii.org/en/on/onsc/doc/2016/2016onsc70/2016onsc70.pdf

[29] https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-surveillance.pdf

[30] https://www.oipc.bc.ca/investigation-reports/1480

[31] http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf

[32] http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=981207

[33] http://www.parl.gc.ca/content/hoc/Bills/373/Government/C-13/c-13_4/c-13_4.pdf

[34] http://www.parl.gc.ca/content/hoc/House/372/Debates/129/HAN129-E.PDF

[35] http://www.canada.justice.gc.ca/eng/cons/la-al/la-al.pdf

[36] http://www.michaelgeist.ca/2012/02/lawful-access-faq/

[37] http://business.financialpost.com/fp-tech-desk/police-scrambling-to-justify-lawful-access-laws

[38] https://drive.google.com/open?id=0B3NEKmwodtrOUXRuRmh1TENMd1E

[39] https://drive.google.com/open?id=0B3NEKmwodtrOVjg4UGdOVWhJQms

[40] http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf

[41] https://www.priv.gc.ca/media/1103/let_gowling_e.pdf

[42] http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/8002/index.do

[43] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

[44] http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/8002/index.do

[45] https://oig.justice.gov/special/s0703b/final.pdf

[46] https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar_201516/

[47] http://blog.privacylawyer.ca/2016/09/lawful-access-2016-there-i-fixed-it-for.html

[48] http://www.michaelgeist.ca/2012/02/lawful-access-faq/

[49] https://necessaryandproportionate.org/principles

[50] http://www.michaelgeist.ca/2013/02/bill-c-30-dead/

[51] http://www.pnas.org/content/113/20/5536.full

[52] https://privacyinternational.org/node/573

[53] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

[54] http://www.michaelgeist.ca/2013/02/bill-c-30-dead/

[55] http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

***** End of Document *****