

(Un)Lawful Access, Its Potentials, and Its Lack of Necessity

by Christopher Parsons¹

The Canadian government has publicly stated its intention to introduce lawful access legislation despite concerns raised by the public, members of the advocacy and academic community, and the information and privacy commissioners of Canada. Such legislation is meant to extend policing powers by making mobile and Internet subscriber data more accessible and placing data preservation and production requirements on telecommunications service providers. Over the past months, I've been working with and talking to concerned parties who would be affected by lawful access legislation. This article makes public many of the topics of these discussions. I begin by summarizing key elements of the lawful access legislation. Next, I note some of the ways that lawful access powers could be used. None of the potential issues that I identify depend on 'next generation' technologies or data management/mining procedures: only existing technologies that are operating today are used as mini-cases.² I conclude by questioning the actual need for the expanded powers.

What is Lawful Access?

Lawful access legislation enhances policing and intelligence powers. As recognized by Ontario's Information and Privacy Commissioner, "it is highly misleading to call it "lawful." Let's call it what it is – a system of expanded surveillance."³ In general, three classes of access powers are associated with such legislation: search and seizure provisions, interception of private communications powers, and production of subscriber data.⁴ On the basis of past lawful access legislation that has been tabled, but has not been passed, we can expect forthcoming legislation to 'modernize' the existing criminal code to accommodate several of these powers.

The expected legislation will likely require telecommunications service providers (such as Internet service providers, web forums, bloggers, anonymous remailers, etc.) to be able

¹ Christopher Parsons is a PhD Candidate in the University of Victoria's political science department. His research draws together Internet governance, traditional social sciences literatures, and security research to provide holistic accountings of novel legal and technological powers concerning the Internet. He thanks Joyce Parsons for her assistance in editing this document for publication.

² None of the cases that I outline offer significant insight into the operational working of stakeholders I've spoken with that can't be reproduced from public research and records.

³ A. Cavoukian. (2011). "Privacy invasion shouldn't be 'lawful'" *National Post*. Published October 31, 2011. Available at:

<http://www.nationalpost.com/news/Privacy+invasion+shouldn+lawful/5631287/story.html>

⁴ CIPPIC. (2007). "Lawful Access: Police Surveillance," CIPPIC website. Published June 2, 2007. Available at: <http://www.cippic.ca/en/lawful-access-faq>

to decrypt communications that they are responsible for encrypting. While communications might be encrypted to limit loss of private information if hackers breach network security, it must be made available on request from the government. In effect, communications will be pseudoencrypted: protected against adversaries with the same level of power as the services' users, but unprotected against the more powerful agents of the state.

In addition, telecommunications service providers (TSPs) must be capable of retaining subscriber data for up to 90 days. TSPs may be served with preservation orders, which would require them to retain data on specific individuals. Preserved data would be transferred to authorities after they have secured a production order from a judge and issued the order to the TSP. The TSP could then delete/destroy the preserved data from their servers and/or databases.

While preservation orders are used to require storage of the communication content, police can access subscriber information without first receiving a court order. TSPs might be required to disclose a wide variety of information about subscribers:

- Name
- Address
- Telephone number
- Electronic mail address
- Internet protocol address
- Mobile identification number
- Electronic serial number
- Local service provider identifier
- International mobile equipment identity number
- International mobile subscriber identity number
- Subscriber identity module card number associated with the subscribers' service and equipment⁵

This information lets authorities definitively identify individuals and the records of their communications processes that TSPs hold. Accompanying the no-warrant-required elements of the legislation is a capacity for authorities to install 'number recorders' in TSPs' communications hubs in exigent circumstances. As noted by the National Post's Kathryn Blaze Carlson:

A number recorder, which records the telephone numbers associated with outgoing and incoming calls, would be installed remotely by a telecommunications provider at their call centre hub. The installation can last up to 60 days, but it could be

⁵ For a discussion of the information contained in these fields, see C. Parsons. (2011). "The Anatomy of Lawful Access Records," *Technology, Thoughts, and Trinkets*. Published November 21, 2011. Available at: <http://www.christopher-parsons.com/blog/technology/the-anatomy-of-lawful-access-phone-records/>

extended to one year if a warrant is obtained and if the investigation involves organized crime or terrorism.⁶

The legislation introduces the ability to activate and/or monitor the signals emitted from location-enabled devices, such as smartphones, that Canadians carry with them or contact regularly. Police can do this today, but lawful access legislation would permit them to activate disabled locational systems (e.g. your phone's GPS) in overt and covert manners. Such actions could be undertaken with court supervision or, potentially, in instances of emergency or exigent circumstances. It should be noted that access to geo-locational information is more expansive than just your physical location at a particular time: the legislation would also let authorities discover the location of "transactions such as geo-tagged comments or photos from private sector service providers."⁷

It is unlikely that a targeted Canadian will be made aware of lawful access-enabled surveillance unless charges are brought to bear. As noted in the letter sent to the Prime Minister's Office on August 2011, and reconfirmed in Blaze's piece, there are elements of the legislation that impose 'gag' orders on anyone ordered to comply with lawful access powers. Specifically,

Clause 6(2) permits the government to impose, in regulations, sweeping and categorical confidentiality obligations on service providers that will apply across all interception warrants. Second, under Clause 71, any telecommunications service provider obligated to comply with a warrantless seizure request will be subject to the secrecy provisions in proposed section 7.4 of PIPEDA. Proposed section 7.4 of PIPEDA prevents organizations from disclosing the fact of their cooperation with state efforts to spy on their customers. The sweeping nature of the secrecy measures envisioned by these provisions is in stark contrast to existing practice, where gag orders must be requested from a judge and justified on a case by case basis. The problem with such measures is that they will prevent individuals from challenging abuses of the powers granted in this Bill.⁸

Lawful Access, In Summary

This legislation can be summarized as requiring:

⁶ K. Blaze Carlson. (2011). "Laws for 21st century: A guide to Canada's proposed cyber investigation bills," *National Post*. Published October 23, 2011. Available at:

<http://news.nationalpost.com/2011/10/22/laws-for-21st-century-a-guide-to-canadas-proposed-lawful-access-laws/>

⁷ A. Slane, A. Clement, et al. (2011). "Statement re: Omnibus Crime bill." Published August 9, 2011. Available at: http://www.christopher-parsons.com/blog/wp-content/uploads/2011/08/20110809-LT_Harper-Re_LawfulAccess-FINAL.pdf

⁸ A. Slane, A. Clement, et al. (2011). "Statement re: Omnibus Crime bill." Published August 9, 2011. Available at: http://www.christopher-parsons.com/blog/wp-content/uploads/2011/08/20110809-LT_Harper-Re_LawfulAccess-FINAL.pdf

- Corporate surveillance: Internet service providers, mobile phone providers, and even the websites that Canadians visit could become agents of the state, forced to preserve records of Canadians' actions at the request of authorities.⁹
- Minimal oversight: Audit powers will be offloaded to privacy commissioners without corresponding material or legislative resources to effectively conduct audits and limit abuse.¹⁰
- Warrantless disclosures: Internet users' subscriber information will be disclosed to authorities, regardless of the information's usefulness or uselessness to an investigation.¹¹
- Secrecy orders: Authorities might collect Canadians' private information without those Canadians ever knowing about the collection or the reasons for collecting it.¹²

Lawful Access in Practice

A large number of Canadians who look at these proposals may feel some unease but then quickly assert that the legislation is ultimately innocuous. The standard rhetoric is that "if you have nothing to hide, you shouldn't fear this legislation." Such a statement obfuscates the realities of contemporary policing and what studies demonstrate about how people actually understand privacy rhetorically. Contemporary policing is deeply invested in identifying deviant behaviour and acting upon such behaviour in 'actuarial' manners. David Lyon, a world-leading surveillance studies scholar, presciently wrote the following back in 2003:

As with database marketing, the policing systems are symptomatic of broader trends. In this case the trend is towards attempted prediction and pre-emption of behaviours, and of a shift to what is called "actuarial justice" in which communications of knowledge about probabilities plays a greatly increased role in assessments of risk.¹³

Thus, being mistakenly situated in a wrong category can have significant implications on one's life regardless of whether a person has 'something to hide' or not. The degree to which one is public is (arguably) secondary to the 'types' of people one knowingly and

⁹ L. Payton. (2011). "Internet privacy experts raise concerns over crime bill," *CBC News*. Published August 9, 2011. Available at: <http://www.cbc.ca/news/canada/story/2011/08/09/pol-internet-privacy.html>

¹⁰ Privacy Commissioners of Canada. (2011). "Letter to Publish Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the current 'Lawful Access' proposals," Office of the Privacy Commissioner of Canada. Published March 9, 2011. Available at: http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm

¹¹ N. Anderson. (2011). "Need a warrant to unmask Internet users? Not if Canada gets its way," *Ars Technica*. Published August 17, 2011. Available at: <http://arstechnica.com/tech-policy/news/2011/08/need-a-warrant-to-unmask-internet-users-not-if-canada-gets-its-way.ars>

¹² A. Slane, A. Clement, et al. (2011). "Statement re: Omnibus Crime bill." Published August 9, 2011. Available at: http://www.christopher-parsons.com/blog/wp-content/uploads/2011/08/20110809-LT_Harper-Re_LawfulAccess-FINAL.pdf

¹³ D. Lyon. (2003). "Surveillance as Social Sorting: Computer codes and mobile bodies," in D. Lyon (ed.). *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. New York: Routledge. Pp. 15-16.

unknowingly associates with, whom their associates are connected to, and the risk profiles that are assigned to those communicative partners and their colleagues. To make this somewhat clearer, consider the following scenario: In college/university/your private life, you communicate with individuals who once did, or presently do, agitate peacefully against certain state behaviour. You might be aware of those individuals' behavior or perhaps you know nothing about it. In any case, you engage in discussions with those people online, perhaps on a website where topics include opposition to certain state behavior, or maybe in the comments section of a newspaper article, or perhaps in some other format. If the police are interested in tracking those individuals who are invested in an issue, for instance, legalization of marijuana, legal issues surrounding sex work in Canada, or protest against federal decisions concerning Sri Lankan immigrants, and with whom you've been talking, your subscriber records could be requested along with those of all the other individuals who participated in the online discussion.

Let's assume that you do not support opposing an official government position and aren't necessarily of real interest to authorities. Regardless, the police might request your subscriber data and that of everyone else engaged in these discussions. No warrant is required for authorities to request and receive this information. Now, let's further assume that you used a unique pseudonym and throwaway email address in your communication with these individuals. The authorities would gain access to your IP address and email address. They would get the same information for every participant of the discussion. With this information, they can turn to the company that provided the email account, as well as contact the ISP who provisioned the IP address at the specific time that you posted your message. With information from the email provider, they might be able to definitely identify the ISP that you use and, from that, your name, address, and so forth. Thus, your unique pseudonym, 'hungrybunny19', is identified as 'John Smith'(you), who was involved in discussion with individuals the authorities are interested in monitoring. Your real name, John Smith, is subsequently added into a database as someone who associates with persons the authorities find questionable. Mr. Smith will never know that he was added to such a database because the service provider could not legally disclose that the information had been released and, as a result, Mr. Smith's life prospects may change for legally associating and speaking with those who were similarly engaged in legal speech and association.

Perhaps you insist that this scenario doesn't describe you: you would never communicate about anything in any electronic environment with any person who would ever be of interest to authorities (and, if you can make and stand by these claims, you're vetting the people that you speak with using intelligence-service-level thoroughness!). But maybe you have a cellular phone, and you have passed near a major event that police are interested in monitoring. For example: you may have been involved in peaceful assembling during the G20 in Toronto, been a passive spectator at the 2011 Vancouver riots, visited an Occupy camp, or simply have passed union members who were protesting working conditions as you walked around your city conducting your personal business. In all cases, authorities may have an interest in monitoring individuals associated with such groups. Using a technology known in the United States as 'Stingray' or, more precisely, IMSI catcher surveillance equipment, police can impersonate a

cellular tower and capture all the IMSI numbers within several kilometers of the catcher.¹⁴ The IMSIs, or International Mobile Subscriber Identity numbers, can be taken to a mobile phone provider and used to compel the subscriber data associated with the caught IMSI numbers. Thus, should authorities deploy one of these catchers ‘just in case,’ an individual may find their personal information sent to police on the basis of their physical presence during a legal public event. The capacity to acquire IMSI numbers en masse, combined with legal powers to compel subscriber information, creates the perfect framework for mass fishing expeditions based on where citizens are physically present.

Canadians may be uncomfortable with the proposition that these fishing expeditions are possible, but quickly move to insist that such concerns are hyperbolic. In turning to a brief reflection on the history of surveillance in Canada, however, we can see that these concerns are practically banal. During the Vancouver Olympics, authorities spent incredible amounts of money on security, an element of which was allocated towards monitoring legal associations of citizens. As disclosed in memos that were accessed in the lead up to the Olympics, no specific, credible, terror threats existed against the Vancouver Olympics.¹⁵ Despite the lack of threat assessments, citizens who had specific political and economic concerns were routinely placed under surveillance.¹⁶ In effect, citizens who were conducting legal actions that might lead to disruptions of the games became targets of a surveillance apparatus designed to prevent the next Munich massacre. Surveillance and intelligence gathering did not focus solely on citizens involved in protesting government actions or others associated with the Olympics¹⁷ but also on their contacts, friends, students, former partners, and academic and professional acquaintances.¹⁸ Efforts were made to recruit neighbours, friends, and acquaintances to spy on suspected activists,¹⁹ and the RCMP tried to legally shield itself from fulfilling FOI requests under the guise of operational security.²⁰ Under lawful access legislation, the lines of inquiry could expand beyond police associating people online – the aforementioned people communicating in Web forums – to using technologies like IMSI catchers to identify who is often near citizens-under-suspicion. Having coffee with a

¹⁴ D. Strobel. (2007). “IMSI Catcher.” Published July 13, 2007. Available at:

http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf

¹⁵ B. Mackin. (2011). “BC’s \$1 Billion False Alarm: Wikileaks,” *The Tyee*. Published May 4, 2011.

Available at: <http://thetyee.ca/News/2011/05/04/OlympicFalseAlarm/>

¹⁶ CBC News. (2009). “Anti-Olympic activists decry ‘Orwellian’ treatment,” *CBC News*. Published November 18, 2009. Available at: <http://www.cbc.ca/news/canada/nova-scotia/story/2009/11/18/ns-antigonish-olympics.html>

¹⁷ J. Ryan. (2010). “During the Olympics, The Feds Will Be Reading Your Tweets – And The Blotter,” *ABC News*. Published February 13, 2010. Available at: <http://abcnews.go.com/Blotter/olympics-feds-reading-tweets/story?id=9825070>

¹⁸ CBC News. (2009). “Olympic security follows protestor’s friend,” *CBC News*. Published October 6, 2009. Available at: <http://www.cbc.ca/news/canada/british-columbia/story/2009/10/06/bc-olympic-security-protester-surveillance.html>

¹⁹ P. Belperio. (2009). “Thought police working overtime in Whistler,” *Rabble.ca*. Published May 19, 2009. Available at: <http://rabble.ca/blogs/bloggers/word-rings/2009/05/thought-police-working-overtime-whistler>

²⁰ The Vancouver Sun. (2008). “RCMP sought ‘special exemption’ on information,” *Canada.com*.

Published October 15, 2008. Available at:

<http://www.canada.com/vancouvernews/news/westcoastnews/story.html?id=eb555565-41a6-42fc-a732-089c19d1915c>

work friend who advocates for social justice on the weekends could lead to unsuspecting, and utterly uninvolved, citizens being stuck in the same net as their law-abiding colleagues who are caught in the web of actuarial justice.

Further, Canadian authorities have a history of monitoring the least-advantaged in society. Consider that Military Intelligence places native communities under intense surveillance. As reported in the *Globe and Mail*, Canadian Military Intelligence generated eight reports in 18 months.²¹ Surveillance was conducted to record Natives' concerns surrounding new tax policies, potential to blockade Highway 401, and possible future protests, lobbying activities, and lawful associations. The group responsible for this surveillance was a counter-intelligence body charged with "identifying, investigating and countering threats to the security of the Canadian Forces and the Department of National Defence from foreign intelligence services, or from individuals/groups engaged of espionage, sabotage, subversion, terrorism, extremism or criminal activities." At no point in the reports is it evident that native groups fell under the latter set of descriptors. With the introduction of lawful access legislation, other authorities such as CSIS, RCMP, and local policing bodies could become increasingly involved in similar surveillance actions and compel telecommunications providers to disclose the contents of communications. In effect, the legislation has the capacity to massively extend the state's intelligence gathering powers, some of which will almost certainly be used to target citizens engaged in legitimate protest. Further, using previously mentioned tactics that are embedded in the legislation, subscriber information and who was communicating with who could be determined without warrant or court oversight.

In short, it is entirely plausible that lawful access could be utilized to expand existing surveillance practices conducted by Canadian authorities. There are serious oversight concerns. Specifically, the Office of the Privacy Commissioner of Canada has stated that it would be hamstrung in auditing the surveillance and its motivations, and the legislation fails to extend the powers of that Office to accommodate the expansion of police powers.²² Further, where local or provincial police conduct surveillance, audit responsibilities would fall to provincial commissioners and they similarly lack resources to mount full-scale audits of authorities' proposed expansive surveillance practices. This position is forcefully stated by the Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian:

Canadians must press the federal government to publicly commit to enacting much-needed oversight legislation in tandem with any expansive surveillance measures. Intrusive proposals require, at the very least, matching legislative safeguards. The courts, affected individuals, future Parliaments and the public must be well

²¹ S. Chase. (2011). "Military intelligence unit keeps watch on native groups," *The Globe and Mail*. Published October 14, 2009. Available at: <http://www.theglobeandmail.com/news/politics/military-intelligence-unit-spies-on-native-groups/article2199496/>

²² Privacy Commissioners of Canada. (2011). "Letter to Publish Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the current 'Lawful Access' proposals," Office of the Privacy Commissioner of Canada. Published March 9, 2011. Available at: http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm

informed about the scope, effectiveness and damaging negative effects of such intrusive powers.²³

The Need for Lawful Access

Over the past months, I've had the opportunity to speak with counselors, engineers, privacy officers, and policy staff for telecommunications service providers. These discussions have ranged from with ISPs to an ex-VoIP provider employee to webmasters responsible for large online environments to policy wonks at massive Internet-based corporations. The various parties I've spoken with have held varying opinions on lawful access legislation; everything from cost issues, to rights problems, to implementation woes, to issues of being identified as a 'problem' in the policing process.

All, however, have told me that in almost every case in which data is requested on exigent circumstances grounds, it is, in fact, *disclosed*.

What, specifically, is the need driving the legislation then? Authorities have routinely insisted that lawful access powers would be used only when investigating the most serious of crimes²⁴ but in other jurisdictions we have regularly seen expanded surveillance used to investigate less serious offences. For extensive documentation of such 'expanded uses,' see Priest's and Arkin's *Top Secret America: The Rise of the New American Surveillance State*. Moreover, there have been substantiated claims that the FBI conducted dragnet surveillance to trace bank robbers,²⁵ claims that routine conversations lead individuals to be labeled as potential terrorists in American government databases,²⁶ reports on inappropriate monitoring of hundreds of UK citizens each year,²⁷ factual claims of yearly monitoring of over 500,000 UK citizens' communications records,²⁸ or the uses of terror-based surveillance provisions to ensure children are registered in correct school districts.²⁹ I cannot state emphatically enough: this is a very small sampling of how widely our closest economic, political, and military allies use lawful-access style legislation. There is no reason that Canadian authorities won't demonstrate similar types of behaviour.

²³ A. Cavoukian. (2011). "Privacy invasion shouldn't be 'lawful'" *National Post*. Published October 31, 2011. Available at:

<http://www.nationalpost.com/news/Privacy+invasion+shouldn+lawful/5631287/story.html>

²⁴ Such assurances were perhaps most prominently made in a series of interviews conducted by the CBC's *Spark*. The interviews are available at: <http://www.cbc.ca/spark/2011/09/tom-stamatakis-and-murray-stooke-on-lawful-access/>

²⁵ D. McCullagh. (2010). "ACLU: FBI used 'dragnet'-style warrantless cell tracking," *CNET News*. Published June 22, 2010. Available at: http://news.cnet.com/8301-31921_3-20008444-281.html

²⁶ J. Leopold. (2009). "Revisiting Echelon: The NSA's Clandestine Data Mining Program," *The Public Record*. Published July 15, 2009. Available at: <http://pubrecord.org/nation/2290/revisiting-echelon-nsa/>

²⁷ Out-Law.com. (2011). "MI5 admits to wrongful surveillance of innocent people, new report says," *Out-law.com*. Published July 5, 2011. Available at: <http://www.out-law.com/page-12055>

²⁸ C. Williams. (2010). "UK.gov's phone and net snooping hits record high," *The Register*. Published July 28, 2010. Available at: http://www.theregister.co.uk/2010/07/28/intercept_commissioner/

²⁹ M. Kennedy. (2009). "Officials seek access to phone and email record data, 1,381 times a day," *The Guardian*. Published August 10, 2009. Available at: <http://www.guardian.co.uk/uk/2009/aug/10/email-phone-intercept-requests-police>

British Columbia's Information and Privacy Commissioner, Elizabeth Denham, has asserted that authorities have not demonstrated evidence that investigations have been, or are being, thwarted under existing access powers.³⁰ Authorities have failed to provide empirical data that reveal a clear and present need for the enhanced powers contained in past, or forthcoming, lawful access legislation. Authorities have noted concerns with warranting processes and if these concerns are legitimate (insofar as they can be documented using empirical datasets), perhaps Parliament should consider modifying the warranting process or increase resources so that warrants can be processed more rapidly. If, however, authorities are simply looking abroad and finding their power lacking in comparison – and cannot clearly outline why they need their compatriots' powers to protect us from truly serious crimes, – they should not be granted expanded powers. Police and other authorities should not be permitted to infringe upon Canadians' rights and further erode expectations of communicative privacy, associative privacy, or basic dignities on the basis of cross-jurisdictional envy.

³⁰ C. McInnes. (2011). "Lawful access would trample rights," *The Vancouver Sun*. Published September 30, 2011. Available at: <http://www.vancouversun.com/technology/Lawful+access+would+trample+rights/5482150/story.html>