

Everything You Always Wanted to Know About Lawful Access, But Were (Understandably) Afraid To Ask

Monday February 13, 2012

Public Safety Minister Vic Toews is expected to introduce lawful access legislation tomorrow in the House of Commons. An

Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and others Acts, likely to be Bill C-30, will mark the return of lawful access in a single legislative package. While it is certainly possible for a surprise, the bill is expected to largely mirror the last lawful access bills (C-50, 51, and 52) that died on the order paper with the election last spring.

This long post tries to address many of the most common questions and misconceptions about lawful access in Canada. The questions and answers are:

- What is lawful access?
- What is Bill C-30 likely to contain?
- Isn't ISP customer name and address information similar to phone book data that is readily available to the public without privacy concerns? (first prong)
- Isn't the mandatory disclosure of ISP customer information necessary for police investigations? (first prong)
- Didn't former Public Safety Minister Stockwell Day pledge not to introduce mandatory disclosure of ISP customer information without court oversight? (first prong)
- Who pays for the surveillance infrastructure required by lawful access? (second prong)
- Does lawful access create a new regulatory framework for the Internet? (second prong)
- Does lawful access create new police powers? (third prong)
- Does opposing lawful access mean questioning the integrity of law enforcement?
- Don't other countries have the same lawful access rules as those found in Canada?
- What do Canada's privacy commissioners think about lawful access?
- Are these lawful access proposal constitutional?
- Does the government seem somewhat inconsistent on its crime and privacy policies?
- Where can I learn more about lawful access and what can I do?

Update: Bill C-30 was introduced on February 14, 2012. One important change from the last bill to the current bill is that the list of data points subject to mandatory disclosure without court oversight has shrunk from 11 to six. The IMEI numbers, discussed further below, are no longer on the list.

What is
lawful access?

The push for new Internet surveillance capabilities goes back to 1999, when government officials began crafting proposals to institute new surveillance technologies within Canadian networks along with additional legal powers to access surveillance and subscriber information. There have been several attempts at passing lawful access legislation, but each has died on the order paper without progressing through the legislative process. In fact, no lawful access bill has even made it to the committee stage for hearings and detailed examination.

What is
Bill C-30 likely to contain?

Assuming the bill mirrors the previous Conservative government approach, the bill will likely feature a three-pronged approach focused on information disclosure, mandated surveillance technologies, and new police powers.

The first prong mandates the disclosure of Internet provider customer information without court oversight. Under current privacy laws, providers may voluntarily disclose customer information but are not required to do so. The new system would require the disclosure of customer name, address, phone number, email address, Internet protocol address, and a series of device identification numbers.

While some of that information may seem relatively harmless, the ability to link it with other data will often open the door to a detailed profile about an identifiable person. Given its potential sensitivity, the decision to require disclosure without any oversight should raise concerns within the Canadian privacy community.

The second prong requires Internet providers to dramatically re-work their networks to allow for real-time surveillance. The bill sets out detailed capability requirements that will eventually apply to all Canadian Internet providers. These include the power to intercept communications, to isolate the communications to a particular individual, and to engage in multiple simultaneous interceptions.

Moreover, the bill establishes a comprehensive regulatory structure for Internet providers that would mandate their assistance with testing their surveillance capabilities and disclosing the names of all employees who may be involved in interceptions (and who may then be subject to RCMP background checks).

The bill also establishes numerous reporting requirements including mandating that all Internet providers disclose their technical surveillance capabilities within six months of the law taking effect.

Follow-up reports are also required when providers acquire new technical capabilities.

Having obtained customer information without court oversight and mandated Internet surveillance capabilities, the third prong creates a several new police powers designed to obtain access to the surveillance data. These include new transmission data warrants that would grant real-time access to all the information generated during the creation, transmission or reception of a communication including the type, direction, time, duration, origin, destination or termination of the communication.

Law enforcement could then obtain a preservation order to require providers to preserve subscriber information, including specific communication information, for 90 days. Finally, having obtained and preserved the data, production orders can be used to require the disclosure of specified communications or transmission data.

While Internet providers would actively work with law enforcement in collecting and disclosing the subscriber information, they could also be prohibited from disclosing the disclosures as court may bar them from informing subscribers that they have been subject to surveillance or information disclosures.

Isn't ISP

customer name and address information similar to phone book data that is readily available to the public without privacy concerns? (first prong)

No. The last bill included the following data points:

- name and address
- telephone number
- electronic mail address

- Internet protocol address
- mobile identification number
- electronic serial number (ESN)
- local service provider identifier
- international mobile equipment identity (IMEI) number
- international mobile subscriber identity (IMSI) number
- subscriber identity module (SIM) card number that are associated with the subscriber's service and equipment.

This data goes well beyond phone book data and can be used for invasive investigations without court oversight. For example, IMSI catchers

can be used to capture all IMEI numbers in a geographic location so that anyone with mobile device would have this information captured. Law enforcement could use this tool to capture information all cellphones in a given area - say at a G20 protest, visiting Parliament Hill, or at a community event - and then require Canada's telecom companies to disclose the corresponding names and addresses. All without court oversight. Christopher Parsons provides a detailed look at this issue.

Isn't the mandatory disclosure of ISP customer information necessary for police investigations? (first prong)

No. To date neither the government nor law enforcement agencies have provided evidence that the current law - which permits disclosure without a warrant but does not mandate it - has created an investigatory barrier. Indeed, earlier this month, police in Ontario arrested 60 men on child pornography charges after obtaining information

on hundreds of IP addresses using the current law. This is but one example of numerous successful child pornography investigations in Canada in recent years (here,

here,
here,
and here).

These successes have not stopped Toews from arguing opponents of lawful access will make things easier for child predators

Similarly, the successful anti-terror investigations involving the Toronto 18 involved computer and Internet-based investigations using current law.

Given the lack of evidence on the need for these changes, politicians and police have been scrambling to find justifications for the change. In 2009, then-Public Safety Minister Peter Van Loan pointed to a 2009 kidnapping case in Vancouver as evidence of the need for legislative change, describing witnessing an emergency situation in which Vancouver police waited 36 hours to get the information they needed in order to obtain a warrant for customer name and address information. That sounds like a credible case, but according to documents obtained under access to information, no Internet provider records were actually sought during the investigation. More recently,

Open Media obtained internal police documents seeking examples of why legislative change is needed. The document acknowledged that previous efforts "lacked a sufficient quantity of good examples." David Fraser has also looked at this issue [here](#).

Didn't former Public Safety Minister Stockwell Day pledge not to introduce mandatory disclosure of ISP customer information without court oversight? (first prong)

Yes. Former Conservative Public Safety Minister Stockwell Day stated in 2007:

"we have not and we will not be proposing legislation to grant police the power to get information from Internet companies without a warrant. That's never been a proposal. It may make some investigations more difficult, but our expectation is rights to our privacy are such that we do not plan, nor will we have in place, something that would allow the police to get that information."

Toews has now backed away from that pledge. According to a letter sent to NDP MP Charlie Angus in November 2011, Toews wrote:

It is correct that former Public Safety Minister Stockwell Day did, at one time, endorse a subscriber information regime that would have required a warrant in order to access the information. However, since that time, the Government has consulted further with law enforcement and justice officials and determined that a warrant requirement for basic subscriber information would negatively impact the ability to carry out investigations and would introduce an additional burden on the criminal justice system.

I have filed Access to Information requests with Public Safety, Justice, the RCMP, and CSIS on these consultations. Thus far no one has provided any documentation or evidence.

Who pays for the surveillance infrastructure required by lawful access? (second prong)

Cost is a big question mark on lawful access, though costs will ultimately be borne by the public. According to documents obtained under the Access to Information Act, many telecom and Internet providers have been primarily focused on the costs associated with installing surveillance equipment and with processing law enforcement requests. The government may provide financial assistance to smaller Internet providers to help address their costs or provide an implementation delay. Some smaller providers have indicated they may be forced to close if they bear the costs alone. Providers will likely also be able to charge fees for complying with law

enforcement requests.

Does lawful access create a new regulatory framework for the Internet? (second prong)

The lawful access proposals create what can only be described a new regulatory environment for Internet providers. Every provider must:

- submit a report within six months on their equipment and surveillance capabilities
- submit a report on new equipment if acquire another provider
- face possibilities of audits from the RCMP and others
- assist law enforcement with testing facilities for interception purposes
- provide the names of all employees involved in interceptions. The RCMP may conduct background checks with consent
- meet operational requirements to enable interception, isolate communications, provide proscribed information, and conduct multiple interceptions

Does lawful access create new police powers? (third prong)

Yes. As noted above, it envisions at least three new warrants. By definition, these involve court oversight. The warrants are:

- Transmission warrants, which cover information related to the transmission of information such as routing or addressing, along with all the additional header-type information created by messages.
- Preservation orders, which require the temporary retention of data on particular subscribers or communications
- Production orders, which can require disclosure of transmission data, tracking data, financial data or information on specified communications

Does opposing lawful access mean questioning the integrity of law enforcement?

In Toews' November 2011 letter to Angus, he states:

For you to suggest that authorities would use these identifiers to track individuals without first obtaining the necessary judicial authority is to question the integrity of those entrusted to keep our communities safe.

We can expect more of this line of argument in the months ahead. All Canadians recognize the need for security and to ensure that law enforcement has the tools they need. Yet the experience in other jurisdictions points to the dangers of blanket powers with no oversight. For example, in the United States, the National Security Administration has admitted in "over-collection" of domestic email messages and phone calls. In Greece, more than 100 cell phones owned by the Prime Minister and senior government officials were surreptitiously wiretapped. Despite the best of intentions, mistakes happen which is why oversight and reporting is crucial.

Don't other countries have the same lawful access rules as those found in Canada?

Some do, but the experience in other countries is illustrative of why the Canadian approach is so dangerous. Christopher Parsons recently released a detailed paper that examines the experiences in countries such as the UK and the U.S.

In the U.K., there are dozens of examples of errors over the last few years. Moreover, the rules have been used for things such as ascertaining "a family's eligibility to send their children to a local school." In the U.S., similar surveillance powers have been used thousands of times with ISPs and Internet companies. Targets have included journalists conducting investigations.

What do Canada's privacy commissioners think about lawful access?

Canada's privacy commissioner have been unanimous in their criticism of the government's lawful access proposals. A letter signed by all Canadian commissioners can be found [here](#). Privacy Commissioner of Canada Jennifer Stoddart posted a follow-up open letter in late October 2011 (an [As It Happens](#) interview [here](#)). Ontario Privacy Commissioner Ann Cavoukian has also been very active on the lawful access issue with a full website that includes video from a symposium, a public letter to Toews with detailed legal analysis, an op-ed, and a Search Engine podcast.

Are these lawful access proposal constitutional?

The Supreme Court of Canada may ultimately be asked to answer that question. One of the most comprehensive legal and constitutional analyses of the lawful access proposals comes from Pippa Lawson in a recent paper titled [Moving](#)

Toward a Surveillance Society: Proposals to Expand "Lawful Access" in Canada, commissioned by the BC Civil Liberties Association.

Does the government seem somewhat inconsistent on its crime and privacy policies?

If by inconsistent you mean supporting the creation of widespread surveillance capabilities, removing foundational privacy principles requiring court oversight, and claiming the need to support police investigations, while:

- killing the long gun registry over the objections of the Canadian Association of Chiefs of Police

- planning to delete the data from the long gun registry on privacy grounds (Toews: "to maintain the registry and the information is a complete violation of law and the principles of privacy that all of us in the House respect")

- scrapping the mandatory long-form census on privacy grounds

then, yes, they seem somewhat inconsistent.

Where can I learn more about lawful access and what can I do?

Given the widespread concern, there are many excellent resources on lawful access. These include:

- Unlawful Access, a 15 minute video that includes interviews with many Canadian experts including Andrew Clement, David Fewer, David Lyon, David Murakami Wood, Dwayne Winseck, Ian Kerr, Natalie Des Rosiers, and Ron Deibert (I'm in the film as well).

- CIPPIC FAQ on lawful access

- Christopher Parsons posts on lawful access

- David Fraser's posts on lawful access

If you are concerned with lawful access, speak out:

- Ontario Privacy Commissioner Ann Cavoukian has a form to send a message to your MP

- Open Media is running a

petition

font-weight: bold;/li