FIPA
BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

SPIN AND COUNTER-SPIN ON THE ONLINE SPYING BILL

Stop Online Spying's petition against the Conservatives' spying bill has been signed by over 115,000 Canadians. In response, Public Safety Minister Vic Toews' office has been emailing petition signers with the government's spin on the bill. The response is full of falsehoods and deserves a thorough de-bunking, so FIPA's Vincent Gogolek and Open Media's Lindsey Pinto have prepared a point-by point refutation.

Vic Toew's "myths and facts" message is highlighted in yellow; our response is clear.

Toews' message (formatting not preserved):

Thank you for contacting my office regarding Bill C-30, the Protecting Children from Internet Predators Act.

Canada's laws currently do not adequately protect Canadians from online exploitation and we think there is widespread agreement that this is a problem.

We want to update our laws while striking the right balance between combating crime and protecting privacy.

Let me be very clear: the police will not be able to read emails or view web activity unless they obtain a warrant issued by a judge and we have constructed safeguards to protect the privacy of Canadians, including audits by privacy commissioners.

What's needed most is an open discussion about how to better protect Canadians from online crime. We will therefore send this legislation directly to Parliamentary Committee for a full examination of the best ways to protect Canadians while respecting their privacy.

For your information, I have included some myths and facts below regarding Bill C-30 in its current state.

Sincerely,
Vic Toews
Member of Parliament for Provencher

Myth: Lawful Access legislation infringes on the privacy of Canadians.

Fact: Our Government puts a high priority on protecting the privacy of law-abiding Canadians. Current practices of accessing the actual content of communications with a legal authorization will not change.

TRUTH: This bill WILL infringe on our privacy rights, and is a huge and unprecedented expansion of permanent surveillance powers. Every single provincial/territorial privacy commissioner and ombudsperson in Canada, the government's own federal privacy commissioner, and Canada's leading legal and privacy experts have spoken out against the bill and made a case for its invasive nature.

The government's online spying bill (C-30) provides a range of authorities with access to the private information of any Canadians, at anytime, without a warrant. Clearly there is a problem, and **Toews is simply refusing to listen to the people who are the acknowledged experts in this field.**

Myth: Having access to basic subscriber information means that authorities can monitor personal communications and activities.

Fact: This has nothing to do with monitoring emails or web browsing. Basic subscriber information would be limited to a customer's name, address, telephone number, email address, Internet Protocol (IP) address, and the name of the telecommunications service provider. It absolutely does not include the content of emails, phones calls or online activities.

TRUTH: This is what's known as the "Straw Man" fallacy, which is committed when a person "simply ignores a person's actual position and substitutes a distorted, exaggerated or misrepresented version."

IP addresses, combined with the other data Toews so generously listed, is what we take issue with the most. As cited on ITbusiness.ca, Ontario Information and Privacy Commissioner Ann Cavoukian describes the problem well:

"Your IP address is not just a number," Cavoukian said. The information can be linked to other personal data which will create a digital trail that reveals where you have been and when, who you see or collaborate with, what are your likes, beliefs or political affiliations. "Right now there is no assurance that once in their hands, authorities can protect that data or prevent its misuse," she added.

This on its own is bad enough. It means that the personal information of any Canadian can be accessed without a warrant. But since you brought it up, Vic, we should mention that **there are other provisions in the bill that would allow the *direct* monitoring of emails and web browsing.**

Let's see what Law Professor Michael Geist had to say about that in his blog:

> ...yet Toews has not talked about a provision in Bill C-30 that creates a voluntary warrantless system that would allow police to ask for the content of emails or web surfing habits and allow ISPs to comply with the request without fear of liability. Section 487.0195 states the following:
>
> > (1) For greater certainty, no preservation demand, preservation order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing.
> >
> > (2) A person who preserves data or provides a document in those circumstances does not incur any criminal or civil liability for doing so.

> This provision opens the door to police approaching ISPs and asking them to retain data on specified subscribers or to turn over any subscriber information - including emails or web surfing activities - without a warrant. ISPs can refuse, but this provision is designed to remove any legal concerns the ISP might have in doing so, since it grants full criminal and civil immunity for the disclosures.
>
> While many would hope that ISPs would not hand over personal information without a warrant, revelations that they already provide customer name and address information about 95 percent of the time suggests that police have little to lose in asking for more detailed data preservation and disclosure. Bill C-30 increases the likelihood of "voluntary" warrantless disclosures, creating a legal framework that makes it easy and risk-free from a provider perspective.

Myth: This legislation does not benefit average Canadians and only gives authorities more power.

Fact: As a result of technological innovations, criminals and terrorists have found ways to hide their illegal activities. This legislation will keep Canadians safer by putting police on the same footing as those who seek to harm us.

TRUTH: This bill goes far beyond just keeping up with the bad guys. As Privacy Commissioner Jennifer Stoddart wrote last year, “In brief, these bills went far beyond simply maintaining investigative capacity or modernizing search powers. Rather, they added significant new capabilities for investigators to track, and search and seize digital information about individuals.”

There also has been no evidence to support the notion that we need to “update” our framework for defending against online crime. Although the push for this expansion of electronic surveillance powers began nearly 13 years ago, no examples of its need have been presented publicly so far—and trust us, the police have tried to find them.

OpenMedia.ca recently released the contents of a message that the CACP sent to law enforcement officials, which asks them to provide examples, even those with “confidential operational information”, of situations in which current online privacy provisions have hindered investigations. This exercise itself—not to mention its failure—makes it clear that this legislation is a solution in search of a problem. As current legislation already grants ISPs the options to disclose customer names and address information, and gives police permission to bypass warrants in emergency situations, no examples have turned up yet.

Additionally, Lindsey Pinto tackled this issue from another angle in a piece she co-wrote for the Georgia Straight:

> At this time the average Canadian, especially those in communities or generations that are recent adopters of information technology, will not know how to find or use things like anonymous remailers and overlay networks. While computer code can trump law for the more savvy and consequentially more dangerous criminals, law-abiding citizens would have to live with the government looking over their shoulder as they go about their everyday lives. **The worst offenders would get away every time, while the rest of us grow more and more paranoid about what we do online**, who we interact with, and how our interests, questions, or discourse could be interpreted by state authorities. In short, the only things these bills are likely to hinder are our fundamental freedoms of expression and association.

> Case-in-point: in October the hacker group Anonymous took down one of the largest hosts of child pornography, which was being run over a concealed “darknet”, or anonymized network. The government’s proposed “lawful access” bills would likely not have discovered this kind of online activity to begin with; under the new regime, the Anonymous brand of online vigilante justice will still be needed to combat this kind of illegal activity. One might want to ask the question then, just what exactly does the government hope to achieve with its online spying agenda, if it can’t address more sophisticated and nefarious forms of Internet crime?

It’s frankly disgusting that the government would use brutally serious crimes to defend this sloppy, invasive legislation. If the government wants to stop criminals, they should write legislation that targets those criminals. That would be far more effective. Instead, they’re targeting every Canadian, and they refuse to tell us why.

Myth: Basic subscriber information is way beyond “phone book information”.
Fact: The basic subscriber information described in the proposed legislation is the modern day equivalent of information that is in the phone book. Individuals frequently freely share this information online and in many cases it is searchable and quite public.

TRUTH: In what we found to be an amusing piece, cybersecurity expert Christopher Parsons takes aim at the phonebook fallacy. Here’s part of the introduction to his very detailed post. We hope you can later take a moment to read the whole thing:

> In response to concerns aired in public, the Public Safety Minister has insisted that the legislation would merely let police access “phone book” information from telecommunications providers. **Such assertions obfuscate the sheer amount of information contained in the records that authorities would collect.** The aim of this post is to make clear just how much information is contained in a single lawful access “phone record”, demonstrating that the government is seeking information that grossly exceeds what is contained in the white or yellow pages today. As a result, I first provide an example phone record that resembles those in every phonebook in Canada and then offer an example of a lawful access record.
>
> Remember that such requests may be filed to multiple service providers (e.g. Internet service provider, web forum hosts, blogs, mobile phone companies, etc) and thus a swathe of records can be combined to generate a comprehensive picture of any particular individual. By the conclusion of the post it should be evident that information provided under lawful access powers is more expansive than the phone records government ministers allude to and lay bare those ministers’ technical obfuscations.

If Parson’s unreserved destruction of this fallacy isn’t enough, we should add that in an extensive response to an earlier Public Safety consultation on online surveillance legislation, the Privacy Commissioner of Canada expressly contradicts what the government claims as fact.

Many, if not all, of the various types of personal information included within the ill-named category of "customer name and address" information constitute personal information to which a reasonable expectation of privacy attaches. We strongly recommend that due consideration be given to the Charter implications of any legislation that would make it

mandatory for a TSP to disclose this personal information when confronted with a warrantless request that is, in reality, a demand.

Myth: Police and telecommunications service providers will now be required to maintain databases with information collected on Canadians.

Fact: This proposed legislation will not require either police or telecommunications service providers to create databases with information collected on Canadians.

TRUTH: It may not "require" them to create these databases, but they almost certainly will do so either for administrative convenience (ISPs wanting to avoid expensive searches when the authorities come calling) or because that is why they want access to this data (police, government). These registries will have to be giant, and will in all likelihood be unsecure and expensive.

Myth: "Warrantless access" to customer information will give police and government unregulated access to our personal information.

Fact: Federal legislation already allows telecommunications service providers to voluntarily release basic subscriber information to authorities without a warrant. This Bill acts as a counterbalance by adding a number of checks and balances which do not exist today, and clearly lists which basic subscriber identifiers authorities can access.

TRUTH: So the Protecting Children from Internet Predators Act is really about protecting Canadians' privacy?

Phillippa Lawson's research paper deals with this, along with many other topics:

One might expect that the proposals to expand police powers would be accompanied by an oversight regime with strong measures to ensure public accountability, at least where the normal requirement for prior judicial authorization is absent. Yet, there is no proposal for meaningful oversight of warrantless access powers and only a few weak measures (e.g., internal reporting and internal audits) designed to allow for some accountability.

Unlike the regime governing covert interception of private communications by state authorities, there is no requirement to account publicly for the use of powers to gather data about subscribers and/or users of telecommunications services without warrant, even though data gathered in these ways can now reveal more about an individual than may be revealed by real-time interception of private communications.

Also, Vic, check in with your Privacy Commissioners one more time. They don't seem to agree with you.

*** * ***

So there you have it. **Canadians, keep spreading the word about the petition at http://StopSpying.ca**, emailing your MP, writing letters to the editor, and otherwise making noise. You're not the ones who aren't paying attention.

FIPA: fipa@vcn.bc.ca