Bill C-30 "Protecting Children from Internet Predators Act" Summary

March 22, 2013 :: Version 1.0

Contents

About the CATSMI Project

The Canadian Access to Social Media Information (CATSMI) Project operates out of the University of Victoria. It is a distinctly Canadian research project, but we believe that our findings have a very wide relevance. The central hypothesis of this project is that the evolution of a more "social web" poses significant challenges to theories of informational privacy as well as to the national legal systems and regulatory policies that have been based on these theories.

The main objective of the Project is to determine how the expectations of social networking websites and environments, whose raison d'etre is the facilitation of the sharing of personal information about and by users, can be reconciled with prevailing understandings about "reasonable expectations of privacy" and the existing regimes that are designed to protect personal data. Organizations have to make decisions about the granularity and range of privacy choices to offer users. Are there significant variances between organizations' perspectives and policies on access to personal information by data subjects on the one hand, and those of government authorities on the other? Are data subjects meaningfully made aware of their own rights to access data, and the capabilities of authorities to access the same subjects' data?

The Project has adopted a three-track process to understand the relationship between social networking services and government intelligence and policing services. **First**, we have analyzed the stated policies and publicly available lawful access documents that social networking services have prepared. These documents were accessed via public Internet repositories or, in one case, through private sources. This has revealed how personal information is made available by social networking services, and the conditions for providing it to government agencies.

Second, researchers investigated whether members of social networking services could access their own records and correct misleading or incorrect fields, and thus enforce their privacy rights under the Personal Information Protection and Electronic Documents Act (PIPEDA), and substantially similar provincial legislation. This approach allows us to ascertain the actual access that Canadians might have to the profiles that they, and networking services they are associated with, are developing. It also let us ascertain whether records provided to service members contain similar, more, or less information than the data fields that may be made available to law enforcement.

Third, Project members have evaluated how existing disclosure policies are, or would be, affected by forthcoming Canadian lawful access legislation. This final level of analysis will clarify whether Canadian authorities will have new powers in excess of social networking companies' existing disclosure conditions.

The outcome of our analysis is a better understanding of how Canadians' information is collected and made available to social network members and third-parties. By analyzing the practices of major social networking sites we have sought to make it clear to Canadians how their personal information might be accessed by authorities.

CATSMI's research is funded through the Office of the Privacy Commissioner of Canada's Contributions program. The use of these funds is independent of the Commissioner; as such, information in this document reflects work that emerges from independent academic research and does not necessarily reflect the Privacy Commissioner's own position(s). Funding has also come from a Social Sciences and Human Research Council (SSHRC) grant: "Social Networking and Privacy Protection: The Conflicts, the Politics, the Technologies (2010-13).

Overview of Bill C-30 "Protecting Children from Internet Predators Act" Summary

Social networking companies such as Facebook, Twitter, Meetup, and Club Penguin could be classified as Telecommunications Service Providers under recently proposed Canadian lawful access legislation.

'Lawful Access' refers to legislation or government policies that extend authorities' powers to access communication data. Authorities can include a range of state actors, including security and intelligence services, policing bodies, 'peace officers' (e.g. sheriff, warden), or designated government regulatory organizations. In Canada, recent legislative efforts would have expanded the powers held by peace officers, policing groups, Canadian Security and Intelligence Services (CSIS), and the Competition Bureau.

These changes to law and policy are traditionally associated with three kinds of access powers: search and seizure provisions, interception of private communications, and the mandatory production of subscriber data. Search and seizure provisions govern the warrant requirements for searching individuals or property or to lawfully seize evidence. Interception provisions govern the live capture of communications, which can include audio-, video-, and text-based communications formats. Modifying production order powers can affect the ease by which authorities can collect billing information about individuals from service providers, as well as information that can subsequently be used to 'stitch together' disparate online communications. In an Internet context, this information might include IP addresses, unique mobile device identifiers, email addresses, or pseudonyms that a subscriber might have registered with the service provider.

Lawful access powers were comprehensively tabled by the federal government in February 2012 as Bill C-30 "Protecting Children from Internet Predators Act." The legislation was subsequently killed in February 2013 prior to advancing to Committee hearings. The following summarizes some of the ways that surveillance capacities could have, specifically, been expanded under this lawful access legislation.

Cite As

Christopher Parsons. (2013). "Bill C-30 "Protecting Children from Internet Predators Act" Summary," *The CATSMI Project*. Published March 22, 2013. Available at: http://catsmi.ca/resources/public-resources.

Types of Lawful Requests

The following identifies the kinds of lawful requests that a telecommunications service provider (TSP) might have received if Bill C-30 had received royal assent without any modifications to the 1st reading of the legislation.

Request Type	Summary Description
Subscriber Data	When an authorized individual (peace officer, or designated member of CSIS or Competition bureau) presents prescribed identifying information, the TSP must disclose subscriber data plus some technical elements about the subscriber (IP Address, SPIN for mobile telephony) **No warrant required to access data**
Preservation - Domestic	If data is preserved on grounds that it may be related to a Canadian Criminal Code infraction then the TSP must retain data for 21 days; after that time data can expire, or be deleted. **To access data, authorities need to serve a TSP with a production order**.
Preservation - International	If data is preserved on grounds that it may be related to a foreign then the TSP must retain data for 90 days; after that time data can expire, or be deleted. **To access data, authorities need to serve a TSP with a production order**.
Transmission	Revisions for transmission warrants would let authorities access telephonic data (as today) as well as information concerning the origin and destination of an Internet communication. **Warrants are issued on grounds of reason to suspect**. These are issued to capture data going forward in time.
Tracking	For the disclosure of the movement of a thing of individual's

Request Type	Summary Description
	movement by means of monitoring an item or thing typically worn or carried by the individual of interest. **Warrants are issued on grounds of reason to suspect**. These are issued to capture locational information going forward in time.

Notes:

The definitional elements of 'prescribed identifying information' were not contained in the legislation; thus the elements might have been in excess of stated items TSPs would have to disclose.

What Were the Preconditions to Accessing Data?

This identifies what authorities would have had to do prior to demanding that a telecommunications service provider (TSP) could cooperate with authorities.

Request Type	Summary of Access Conditions
Subscriber Data	Warrants are not required. Officers are to typically issue written requests to TSPs. Requests must be recorded. In exigent circumstances, an officer can either verbally or in writing request access to subscriber information. Subsequently, the officer must issue a written account of the request to the TSP.
Preservation - Domestic	**Preservation demands** would be issued by officers, whereas **preservation orders** would be issued by a judge or justice, on grounds that the office has reasonable ground to suspect an offence has been, or will be, committed under the Canadian Criminal Code, and the preserved data would assist the investigation. The justice or judge must expect the officer will, or has, applied for a warrant to obtain a document containing the data in question. To **access** data a **production order** or **warrant** is required.
Preservation - International	**Preservation demands** would be issued by officers, whereas **preservation orders** would be issued by a judge or justice, on grounds that the office has reasonable ground to suspect an offence has been, or will be, committed under the law of a foreign state, and the preserved data would assist the investigation. The justice or judge must expect the officer will, or has, applied for a warrant to obtain a document containing the data in question. To **access** data a **production order** or **warrant** is required.
Transmissions	A **warrant** is required to access data, which are issued based on reasonable grounds to suspect.
Tracking	A **warrant** is required to access data, which are issued based on reasonable grounds to suspect.

What Had to be Included to Get Information?

Here, we identify what information - excluding legal documents, identified in the previous section - must be provided to TSPs in order for the TSP to disclose subscriber information and data.

Request Type	What's Required to Get Information
Subscriber Data	'Prescribed identifying information' would be required. The definition of this term was not provided in the legislation, and would be developed through regulations.
Preservation - Domestic	A **demand** or **order** would have to specify a particular telecommunication or person.
Preservation - International	A **demand** or **order** would have to specify a particular telecommunication or person.
Transmissions	The **warrant** will define, to an extent, the specificity of the transmission data or individual whose transmission data is being sought.
Tracking	The **warrant** will define, to an extent, the specificity of the tracking data or individual whose transmission data is being sought.

What Information Would Have Been Disclosed?

After issuing a demand upon a telecommunications service provider (TSP), the following outlines what data or information the provider is obligated to disclose to authorities.

Request Type	Information Disclosed
Subscriber Data	When given relevant identifying information (to be defined post-legislation) a TSP would have to disclose the following in their possession: name, address, telephone number, email address IP address(es) or SPIN (mobile telephony) associated with the subscriber's account.
Preservation - Domestic	**Preservation** orders require TSPs to preserve computer or business-related data that is in their control or possession. A **production** order that follows can force a TSP to disclose the following types of information concerning subscribers/preserved data: transmission data, tracking data, financial data, or information about the specific communications in question.
Preservation - International	**Preservation** orders require TSPs to preserve computer or business-related data that is in their control or possession. A **production** order that follows can force a TSP to disclose the following types of information concerning subscribers/preserved data: transmission data, tracking data, financial data, or information about the specific communications in question.
Transmissions	**Warrants** would apply to the the following data, so long as it was not used for tracking purposes; • data related to telecommunications functions of dialling, routing, addressing, or signaling • data that is transmitted to establish or maintain connection to a telecommunications service for the purposes of communicating • data that is generated during the creation, transmission, or reception of a communication and identifies or purports to identify the following characteristics of a communication:

Request Type	Information Disclosed
	○ type ○ direction ○ time ○ date ○ duration ○ size ○ origin ○ destination ○ termination point of communication **NOTE**: for the purposes of C-30, transmission data does not reveal the substance, meaning, or purpose of the communications.
Tracking	Tracking data, which constitutes data that relates to the location of a transaction, individual, or thing.

What Were the Interception Requirements?

The following identifies what telecommunications service providers (TSPs) must do to be capable of complying with authorities' requests under Bill C-30.

Request Type	Inception Compliance Requirements
Subscriber Data	TSPs must be capable of disclosing subscriber information, even as they develop and upgrade their systems and platforms. TSPs do not need to collect subscriber information beyond that demanded by their regular course of business.
Preservation - Domestic	Must be capable of retaining data for up to 21 days. Degree of specificity concerning communications preservation remains unclear (i.e. all HTTP communications, all Facebook communications, or all Facebook communications between particular parties). After the 21 days, the TSP must delete information that is not retained in the regular course of business. Interception capabilities cannot degrade over time as new equipment/services are offered, or as more subscribers join the service. New services and software deployed by the TSP must remain compliant with C-30 interception and preservation requirements. Regulations would set baseline number of prospective simultaneous interceptions; the Minister could subsequently expand that number (with government paying for extra costs).
Preservation - International	Must be capable of retaining data for up to 90 days. Degree of specificity remains unclear (i.e. all HTTP communications, all Facebook communications, or all Facebook communications between particular parties). After the 21 days, the TSP must delete information that is not retained in the regular course of business. Interception capabilities cannot degrade over time as new equipment/services are offered, or as more subscribers join the service. New services and software deployed by the TSP must remain

Request Type	Inception Compliance Requirements
	compliant with C-30 interception and preservation requirements. Regulations would set baseline number of prospective simultaneous interceptions; the Minister could subsequently expand that number (with government paying for extra costs).
Transmissions	TSPs are obligated to have a technological infrastructure to which authorities can install, activate, use, maintain, monitor or remove transmissions data recorders, including covertly. There is not an obligation for TSPs to assist in the attachment or use of a device, though assistance may be provided. Data capture and disclosure can function for 60 days or, when the investigation involves organized crime or terrorist offences, up to 365 days.
Tracking	TSPs are obligated to have a technological infrastructure to which authorities can install, activate, use, maintain, monitor or remove tracking devices, including covertly. There is not an obligation for TSPs to assist in the attachment or use of a device, though assistance may be provided. Tracking data capture and disclosure can function for 60 days or, when the investigation involves organized crime or terrorist offences, up to 365 days.

Were TSPs Prevented from Informing Users?

The following identifies whether all, or some, elements of the lawful access powers limit how telecommunications service providers (TSPs) communicate with their subscribers.

Request Type	Is Disclosure Limited?
Subscriber Data	**Yes**. Lawful access requests for subscriber data would be governed by Section 9 of PIPEDA, which includes prohibitions on informing subscribers that personally identifiable information was disclosed to authorities.
Preservation - Domestic	**Potentially**. Production orders can be accompanied by non-disclosure clauses. Also, regulation may clarify that non-disclosure is required by default.
Preservation - International	**Potentially**. Production orders can be accompanied by non-disclosure clauses. Also, regulation may clarify that non-disclosure is required by default.
Transmission	**Potentially**. Transmission warrants can be accompanied by non-disclosure clauses. Also, regulation may clarify that non-disclosure is required by default.
Tracking	**Potentially**. Tracking warrants can be accompanied by non-disclosure clauses. Also, regulation may clarify that non-disclosure is required by default.

References

C-30 "Protecting Children from Internet Predators Act" is available at http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Bill=C30.

About the Authors

This document was researched and written by Christopher Parsons.

Christopher Parsons is a privacy-by-design ambassador, a well-recognized member of the Canadian privacy community, and a Principal at BlockG Security and Privacy Consulting. He has over a decade's experience working with challenging privacy issues that are linked to digital technologies. He specializes in how Canadian privacy law intersects with digital systems, and the implications of such law on the development and deployment of novel projects and practices. Christopher is presently completing his Ph.D in the Department of Political Science at the University of Victoria, where he is a fellow at the Centre for Global Studies. He has published in the Canadian Journal of Law and Society, European Journal of Law and Technology, Canadian Privacy Law Review, CTheory, and has book chapters in a series of academic and popular books and reports.

Legal Information

Electronic version first published at www.catsmi.ca in Canada in 2013
by The Canadian Access to Social Media Information (CATSMI) Project.

Header designed by Karen Yen of Can Poeti Branding and Design.

Information presented in this document is for academic and educational purposes only. These materials do not constitute solicitation or provision of legal advice. The CATSMI Project makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. Nothing herein should be used as a substitute for the legal advice of competent counsel.