

Privacy, personal information, law enforcement and “lawful access”

David T.S. Fraser

david.fraser@mcinnescooper.com

Canadian Bar Association – New Brunswick



What is Privacy?

- Has been characterised as the right to be left alone, to be secure in one's home and free from unwanted interference
- In the context of more modern privacy laws, privacy means having control over one's personal information
- Choice of whether to disclose information at all
 - Control over with whom it is shared
 - Control over how it is used
 - Don't lose control once you've released your information "into the wild"

Personal Information Protection and Electronic Documents Act

Purpose

3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to ***govern the collection, use and disclosure of personal information*** in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

PIPEDA – Personal Information

- Addresses “personal information” – information about an identifiable individual:
 - **NOT** name, title, business address or telephone number of an employee of an organization
 - Would include name, address, income, health information, demographics, preferences, birth date, SIN, customer numbers, unique identifiers
- Also includes information that may be traced back to an individual

Privacy Principles

- Based on the principles of the Canadian Standards Association Model Code for the Protection of Personal Information:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

The General Rule is Consent

4.3 Principle 3 -- Consent

“The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, *except where inappropriate.*”

Consent Exceptions

- Section 7 of PIPEDA sets out the only allowed exceptions to the general consent rule
 - S. 7(1) – Allows some collection**
 - S. 7(2) – Allows some use**
 - S. 7(3) – Allows some disclosure**
- **Warning:** Not very easy to follow. At all.

Consent Exceptions

- Consent exceptions are very dangerous
- Virtually all circumstances are fraught with risk:
- Permissive exceptions, not mandatory
 - S. 7 allows you to do things that would otherwise be unlawful under PIPEDA ... does not force you to do so.

Investigations by the organization

- **S. 7(1)(b) – “it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.”**
 - Can be collected and used
 - Has been used and upheld, for example by bank in the course of fraud investigation

Compelled production

- **S. 7(3)(c) – “may disclose information ... if required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records”**
 - Allows disclosure to a body that can compel the documents.

Disclosure to law enforcement

- **S. 7(3)(d) – “made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization**
 - (i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
 - (ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;”
- Allows disclosure to police, investigative bodies
- Made on the initiative of the organization
- “Investigative body” is defined in the regulations.

Disclosure to law enforcement

(c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

- (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
- (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or
- (iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

- Permits disclosure to law enforcement, at their request, if these requirements are satisfied.

What is “lawful authority”?

- Recently considered in *Re S.C.*, 2006 ONCJ 343 (CanLII) by an Ontario JP.
- Police suspected criminal activity by Bell internet user.
- Police sent a notice “pursuant to PIPEDA” (“*Letter of Request for Account Information Pursuant to a Child Sexual Exploitation Investigation*”) asking for the person’s identifying information.
- Bell complied and handed over information about the customer. Police sought to use the information to obtain a warrant.
- JP found that there was no “lawful authority” for the disclosure under PIPEDA and the information was therefore illegally obtained.

Re S.C.

- [9] However, s. 7(3) stipulates that the information can be provided without consent only if the body seeking the information has "identified its lawful authority to obtain the information" ***and*** has indicated that the disclosure is requested (in this case) for law enforcement purposes. **The Act does not set out that the existence of a criminal investigation is, in and of itself, "lawful authority" within the meaning of the Act nor, therefore, does a "Letter of Request for Account Information Pursuant to a Child Sexual Exploitation Investigation" establish such authority. Accordingly, there must still be some "legal authority" to obtain the information; in the view of this Court s. 7(3)(c.1)(ii) by itself does not establish what that "lawful authority" is.** The section provides authority for disclosing information. It does not establish the authority for obtaining and possessing the information. ...
- [11] **In the absence of express authority within the legislation, the Charter right not to have one's reasonable expectation of privacy interfered with, except through prior judicial authorization with all the protections that affords, must govern.** Accordingly, it is the view of this Court that the Informant is not lawfully in possession of the information that was provided by Bell Canada.

What should businesses do?

- Any disclosure of personal information without consent is risky.
- The consent exceptions are difficult to interpret.
- PIPEDA doesn't create any requirement to disclose information without consent.
- The most risk adverse approach would be to only disclose information where you are lawfully required to do so.

What should businesses do?

- Don't collect personal information that you don't need just because it could be useful, particularly if it could be useful to law enforcement or to private litigants.
- Even if you think you may be required to collect it later, that's no justification to collect it now.

- See principle 4 of PIPEDA.

What should businesses do?

- Don't keep personal information around any longer than you actually need it.
- If you are asked for personal information by law enforcement or private litigants, it is much easier to say you don't have it than to go to court to resist providing it.
 - See principle 5 of PIPEDA.

What should businesses do?

- It is not your job to police your customers. Mere suspicion on the organization's part is not enough of a basis to voluntarily hand over customer information without consent.
- Need to have “reasonable grounds to believe” ...

- See principle 3 and s. 7(3)(d) of PIPEDA .

What should businesses do?

- Do not provide customer information unless compelled to do so. PIPEDA does not create any compulsion.
 - See principle 3 of PIPEDA and s. 7(3)(c.1)

Lawful access

- “Modernization of Investigative Techniques Act” – Bill C-74.
- Introduced by the Liberal Government
 - To require TSPs to build-in wiretapping capability
 - To require TSPs to provide subscriber information without a warrant
- Fell off the order paper with election

Lawful access

- Apparently not a high-priority for the Harper gov't.
- “Secret” consultation launched this fall
- Lawful access *lite*
 - Only relates to Customer Information on request
 - name;
 - address(es);
 - ten-digit telephone numbers (wireline and wireless);
 - Cell phone identifiers, e.g., one or more of several unique identifiers associated with a subscriber to a particular telecommunications service (mobile identification number or MIN; electronic serial number or ESN; international mobile equipment or IMEI number; international mobile subscriber identity or IMSI number; subscriber identity module card number of SIM Card Number);
 - e-mail address(es);
 - IP address; and/or,
 - Local Service Provider Identifier, i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

Lawful access flip flop



Warrant needed to pull data on Internet users: Day

Safety minister opens closed consultations

Carly Weeks

The Ottawa Citizen

Friday, September 14, 2007

Public Safety Minister Stockwell Day announced late yesterday that the federal government will not force Internet service providers to hand over customers' personal information to police without a warrant -- a move that will surprise critics who have been expressing alarm this week that the Harper government appeared poised to intrude on the civil liberties of Canadians.

"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," Mr. Day said. "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."



NATIONAL POST

Inside the National Post

- Columnists
- News
- Canada
- Toronto
- World
- Editorials
- Letters
- Issues & Ideas
- Arts & Life
- Sports
- Legal Post
- Diversions
- 30 days Archive

Words get in way of saving children

Adrian Humphreys, National Post, with files from Allison Hanes, National Post

Published: Wednesday, October 24, 2007

With a proliferation of horrific allegations in the headlines, Canadians can be forgiven for thinking that child molesters are everywhere. But what is the actual prevalence of the problem, and how should we be dealing with it? In this, the final instalment of a four-part series, the National Post looks at what the law-and-order approach prescribes and how the current system could be fixed.

Changing a single word in a seven year-old piece of legislation -- that was designed to support and promote electronic commerce in Canada -- could help save children from horrific sexual abuse, police officers and child protection advocates say.



Technology for better business outcomes.

» Learn more about HP Software

Today's Post

'Crimes against humanity' in Iran

Lawful access

- Consultation ongoing

**COME BACK
WITH A
WARRANT.**

© 1999 HUGO BOSS AG