


McINNES COOPER

McINNES COOPER

**Privacy and
Insurance Claims:
CBANS Insurance
Law Subsection**


David T.S. Fraser
david.fraser@mcinnescooper.com
(902 424-1347)



McINNES COOPER

Outline

- Legal background
 - PIPEDA
 - Consent
 - Consent exceptions
- Video surveillance
 - PIPEDA
 - Caselaw – PIPEDA and admissibility
 - Caselaw – Privacy Commissioner’s findings
- Access to information
 - PIPEDA
 - Caselaw – Privacy Commissioner’s findings



PIPEDA

- *Personal Information Protection and Electronic Documents Act*
- Passed in 1999
- Began to apply to provincially regulated private sector on January 1, 2004
- Incorporates the Canadian Standards Association Model Code for the Protection of Personal Information



PIPEDA - Application

- Applies to the “collection, use and disclosure of personal information in the course of commercial activities”.
- “Commercial activities” means
 - “any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.”



PIPEDA – “Personal Information”

- “**personal information**” – information about an identifiable individual:
 - BUT NOT name, title, business address or telephone number of an employee of an organization
- Would include
 - name, address, income, health information, diagnosis, health number, demographics, preferences, birth date, SIN, tissue samples, statements
- Also includes
 - analysis or opinions about an individual
 - information that may be traced back to an individual
 - video images or observations



PIPEDA - Consent

- Key concept in the law
- Principle 3 from the CSA Model Code:

3. **Consent** - the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, *except where inappropriate*. Form of consent is dependent upon the sensitivity of the information.

(Ignore the “except where inappropriate”. FCT says it must be read out of the statute.)



Consent Exceptions

- Section 7 of PIPEDA sets out the allowed exceptions to the general consent rule
- These are the only exceptions.
- **Warning:**
 - Not very easy to follow.
 - May not allow you to do what you want.
 - Adult supervision required!



Consent Exceptions – s. 7

- S. 7(1) – Allows *some* collection
- S. 7(2) – Allows *some* use
- S. 7(3) – Allows *some* disclosure
- Be careful that allowed collection may not lead to allowed use → at least not according to the statute.



Consent Exceptions

- S. 7(1)(a) & 7(2)(b) – “If clearly in the interests of the individual and consent cannot be obtained in a timely way.”
 - Can be collected and used
 - No decisions yet.



Consent Exceptions

- 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



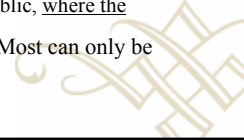
Consent Exceptions

- S. 7(1)(c) – “the collection is solely for journalistic, artistic or literary purposes; ...”
 - Allows collection
 - No decisions



Consent Exceptions

- S. 7(1)(d) – “the information is publicly available and is specified by the regulations”
- Regulations specify:
 - (a) personal information consisting of the name, address and telephone number of a subscriber that appears in a **telephone directory that is available to the public**, where the subscriber can refuse to have the personal information appear in the directory;
 - (b) personal information including the name, title, address and telephone number of an individual that appears in a **professional or business directory**, listing or notice, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the directory, listing or notice;
 - (c) personal information that appears in a **registry collected under a statutory authority** and to which a right of public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry;
 - (d) personal information that appears in a **record or document of a judicial or quasi-judicial body**, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document; and
 - (e) personal information that appears in a **publication**, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information.
- Just because it is publicly available doesn't mean it is “fair game”. Most can only be used for consistent purposes.



Consent Exceptions

- 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




Consent exceptions


- 7(3) “may disclose personal information without the knowledge or consent of the individual only if the disclosure is ... (a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;
- Allows disclosure.



Consent Exceptions

- Miscellaneous **disclosure** exceptions
 - 7(3)(g) – archival institution for the purposes of conservation
 - 7(3)(h) – after the earlier of (a) 100 years after the creation of the record or (b) 20 years after the death of the data subject.
 - 7(3)(h.2) – made by an investigative body for reasonable purposes related to investigation of breach of an agreement or the laws of Canada or a province
 - 7(3)(i) – required by law
- 

PIPEDA and Video Surveillance

- Video-taping a person is a collection of his/her personal information for the purposes of PIPEDA
 - Usual rule requires consent for all collections of personal information, unless an exception in s. 7 applies.
- 

PIPEDA and Video Surveillance

- Commissioner is on the record saying that video, even if not recorded, is personal information.
- **Decision 1** – Video surveillance of activities in public place
 - Surveillance cameras placed on rooftop by a private security company in Yellowknife. Staff monitoring the cameras, noting incidents and calling the police.
 - Were trying to market this service to the police, so this was concluded to be “commercial activity”.
 - Commissioner: "There may be instances where it is appropriate for public places to be monitored for public safety reasons. But this must be limited to instances where there is a demonstrable need. It must be done only by lawful public authorities and it must be done only in ways that incorporate all privacy safeguards set out by law. There is no place in our society for unauthorized surveillance of public places by private sector organizations for commercial reasons."

PIPEDA and Video Surveillance

- **Finding 114** – Employee objects to company’s use of digital video surveillance cameras
 - Railroad company placed cameras on its premises to counter theft and vandalism. (This was in addition to cameras in place for operational purposes.)
 - Informed employees of the cameras and their locations. Told employees they were not to be used for tracking employees or their productivity.
 - To ensure compliance with the intent of section 5(3) (limited to reasonable collection), the Commissioner stressed that the circumstances must also be considered. In determining whether the company’s use of the digital video cameras was reasonable in this case, he asked the following questions:
 - Is the measure demonstrably necessary to meet a specific need?
 - Is it likely to be effective in meeting that need?
 - Is the loss of privacy proportional to the benefit gained?
 - Is there a less privacy-invasive way of achieving the same end?
 - Concluded that the use of the cameras was not reasonable in the circumstances. He concluded there were more effective measures and even though the cameras were only on “public places”, the cameras would have a psychological effect on employees.
- **Federal Court of Canada reversed:** *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 (CanLII), 33 C.P.R. (4th) 1; [2004] 254 F.T.R. 169
 - Privacy Commissioner has no jurisdiction where the issue is arbitrable under collective agreement
 - In obiter: s. 7(1)(b) allows this collection without consent.

The Courts

- *Ferenczy v. MCI Medical Clinics*, 2004 CanLII 12555, 70 O.R. (3d) 277 (ON S.C.)
 - Action against physician related to treatment of wrist
 - Insurer hired PI for video surveillance
 - Plaintiff objected to introduction of video at trial. Collection by PI and disclosure to counsel was contrary to PIPEDA.



Ferenczy v. MCI Medical Clinics

- The Court:
 - PIPEDA does not apply
 - The insurer is the agent for the defendant.
 - Relationship between plaintiff and defendant is not commercial
 - PIPEDA does not apply to “personal purposes” (s. 4(2)(b))
 - Plaintiff impliedly consented by initiating lawsuit
 - Consent is not required as s. 7(1)(b), 7(2)(d) and 7(3)(c) apply.
 - Civil lawsuit is related to a “contravention of the laws of Canada or a province”
 - In any event, the evidence is probative and not prejudicial. **Admissible.**



The Courts

- Schmidt v. Daigle (NBQB unreported F/C/629/00 – May 4, 2004)
- McInnes Cooper acted for the defendant
- Plaintiff objected to use of video surveillance at trial.
- Plaintiff argued Commissioner's finding #114. – Four factors not met.
- Judge concluded that four factors **were** met.
- Video was admissible



The Commissioner

- Complaint brought against insurer and private investigator related to video surveillance (same parties as last case)
- PIPEDA Case Summary #311 - A woman's activities recorded and videotaped by a private investigator hired by an insurance company
- We argued:
 - PIPEDA does not apply (agency)
 - Implied consent
 - No consent required



The Commissioner

- Finding #311:
 - The Assistant Privacy Commissioner reviewed the circumstances surrounding the insurance company's decision to conduct surveillance, including video surveillance on the woman. **She agreed that when an individual initiates a lawsuit there is an implied consent that the other party to the suit may collect information required to defend itself against the damages** being sought by the individual who filed the suit. When the woman initiated her lawsuit against the insurance company's client and when her testimony and medical reports revealed discrepancies and were inconsistent with the injuries claimed, the Assistant Privacy Commissioner concluded that she gave her implied consent to the collection of her personal information.
 - That being said, the Assistant Privacy Commissioner emphasized that **implied consent is not without limitations**. Implied consent does not authorize unlimited or uncontrolled access to an individual's personal information, but only to the extent it is relevant to the merits of the case and the conduct of the defense.



The Commissioner

- Unsatisfying decision:
 - Assistant Commissioner assumed she had jurisdiction even though it was argued she did not. Did not address this issue.
 - Insurer decided not to seek judicial review.



Conclusion: PIPEDA and Video Surveillance

- Can collect personal information by video surveillance if
 - It is reasonable in the circumstances
 - There should be some reason to disbelieve the plaintiff
 - You can't get the same relevant evidence by other means
 - The information collected is limited to that which is relevant to the matters in dispute
- Insurers should document the decision made and the circumstances considered that made it necessary



Access to Information

- Principle 9 provides:
 9. **Individual Access** - Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
- Must respond within 30 days;
- Need to let the individual know to whom the information has been disclosed, so must keep a record of how your data is used.
- Should be at “minimal or no charge”;
- Must be comprehensible to the individual;



Access to Information

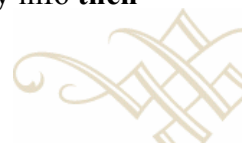
- But you cannot provide access to third-party information:

9. (1) ... an organization shall not give an individual access to personal information if doing so would likely reveal personal information about a third party. However, if the information about the third party is severable from the record containing the information about the individual, the organization shall sever the information about the third party before giving the individual access.
- (2) Subsection (1) does not apply if the third party consents to the access or the individual needs the information because an individual's life, health or security is threatened.



Access to claims materials

- *PIPEDA* Case Summary #314 - Insurance company denies access to personal information in statement of claim
 - Released last week
 - Weird ... refers to "statement of claim"
- Facts
 - Insured in car accident, insurer settled with third-party
 - Insured disputed that she was at fault and asked for claims information, including "statement of claim"
 - Claims info included personal information of the third-party
 - Insurer denied access on basis of third-party info
- **Assistant Commissioner**
 - Insurer had obligation to sever the third-party info **then** provide access.



Access to claims materials

- Again, the Commissioner did not consider any agency principles
- Arguably, the insurer collected all the claims materials on her behalf and providing copies would not be a disclosure
 - You can't disclose information to yourself and agent-principal are one in law.
- Again, not entirely satisfying.



Questions?



McINNES COOPER

David T.S. Fraser

Direct Dial 902 424 1347
Email david.fraser@mcinnescooper.com

David is the chair of McInnes Cooper's Privacy Practice Group, working with clients to implement compliance programs for the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and provincial privacy laws. He regularly provides opinions related to Canadian privacy law for Canadian and foreign organizations and is a frequently invited speaker on this topic. In addition, David is the Chair of the Privacy Law Subsection of the Canadian Bar Association – Nova Scotia and the co-chair of the IT.Can Privacy Committee.

David has advised insurers on compliance with privacy laws and with respect to complaints before the Privacy Commissioner of Canada. He is the author of the *Physician's Privacy Manual* and the *Pharmacy Privacy Manual*. He is also the author of "The Canadian Privacy Law Blog", an online privacy blog at <http://www.privacylawyer.ca/blog>.

He is a member of the faculty of Dalhousie Law School, where he teaches Internet and Media Law, Law and Technology, and Law and Policy for Electronic Commerce. David is secretary and director of advocacy for the Information Technology Industry Alliance of Nova Scotia (ITANS).

McINNES COOPER

The Canadian Privacy Law Blog

<http://www.privacylawyer.ca/blog>

[Privacy Law Blog](#) | [Privacy Resources](#) | [Privacy Articles](#) | [Contact Info/Profile](#) | [Useful Links](#) | [Travel Resources](#)

The Canadian Privacy Law Blog

The Canadian Privacy Law Blog: Developments in privacy law and writings of a Canadian privacy lawyer, containing information related to the Personal Information Protection and Electronic Documents Act (aka PIPEDA) and other Canadian and International laws.

Sunday, October 23, 2005

Search this blog

Colleges Protest Call to Upgrade Online Systems

I wrote recently about the prospect of VoIP companies having to build-in law enforcement tapping abilities into their systems ([The Canadian Privacy Law Blog: Internet bugging may dictate technologies and call-routing for VoIP services](#)). The rule change also apparently applies to Universities in the US, who are not happy about having to spend untold thousands of dollars to modify their systems: [Colleges Protest Call to Upgrade Online Systems - New York Times](#)

 [Permalink](#)/posting time: 5:02:43 PM :: [Leave/see comments \(0 comments\)](#)

W-Five feature on personal information theft and fraud

Last night (and this afternoon) was the season premiere of CTV's investigative news program, *W-Five*. The second feature on the show was about the theft of and trafficking in personal information that occurs in Canada and the United States. It chronicled a Canadian connection to the infamous Shadowcrew bust in the US and the efforts to two local police departments to deal with the Canadian angle. The RCMP refused to appear on camera but wrote to the reporters that they did not deal with it because of a lack of resources. Not a high priority, the reporter inferred.

About this page and the author

The author of this blog, David T.S. Fraser, is a Canadian privacy lawyer who practices privacy law with the Canadian firm of McInnes Cooper. He is counsel to National Privacy Services Inc. and the principal author of the Physicians' Privacy Manual. David is also a part-time member of the Faculty of Law at Dalhousie University and an associate of the Law and Technology Institute. He has a national and international practice advising corporations and individuals on matters related to Canadian privacy laws.

For full contact information and a brief bio, please see [David's profile](#).

Links

Subscribe to this Blog as a Weblog