Office of the
Privacy Commissioner
of Canada

PIPEDA

Leading by Example

Key Developments in the First Seven Years of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)

2008

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP54-6/2008
ISBN 978-0-662-05731-4

This publication is also available on our website at www.privcom.gc.ca.

MESSAGE

When the *Personal Information Protection and Electronic Documents Act*, or PIPEDA, received Royal Assent in 2000, the need for private sector privacy legislation at that time was clear – Canadians were demanding adequate privacy protection in a new digital economy. In debates leading up to the adoption of the law, then-Industry Minister John Manley told the House of Commons, "All of us, consumer, business and government alike, need to feel confident about how our personal information is gathered, stored and used. The protection of our personal privacy is a basic right which Canadians cherish."

Since its inception, organizations have been adapting their business practices to comply with PIPEDA and similar new provincial standards as their customers grow increasingly concerned over the protection of their personal information. Meanwhile, the privacy landscape continues to evolve. Advances in information technology and the desire among business to compete globally have meant that the privacy challenges we face today are more complex than ever before.

Our Office's understanding of the interpretation and application of the Act continues to evolve as well. In the last seven years, we have investigated over 2600 individual complaints and have issued findings on many precedent-setting issues arising from the Act. The complaint mechanism has provided us with a window into how PIPEDA works in practice.

Leading by Example is meant to share the insights we have gained since the Act's inception by highlighting some of the leading case findings we've released on a number of important issues. The issues profiled in this report reflect current and growing concerns for businesses and their customers alike, such as the increasing surveillance phenomenon, trans-border data flows, the prevalence of data breaches, and the proliferation of using information collected for secondary marketing purposes. We hope this document will help guide businesses in the development and application of their own privacy practices through the experience of others.

Many of the case findings highlighted here were issued by former Assistant Commissioner Heather Black, who retired last year. We owe her an enormous debt of gratitude for the pioneering contribution she has made to the adoption, implementation and evolution of PIPEDA in its initial critical years, first as General Counsel, then as Assistant Commissioner responsible for PIPEDA. We wish to express our sincere thanks

to Heather and recognize her important contributions in advancing privacy rights in Canada.

We also wish to thank Alex Cameron of Fasken Martineau, who we commissioned to author earlier drafts of *Leading by Example*, as well as Patricia Kosseim, our Office's General Counsel, Ann Goldsmith, Policy Team Leader, and our Communications staff who saw this project through from conception to completion.

Jennifer Stoddart
Privacy Commissioner of Canada

Elizabeth Denham
Assistant Privacy Commissioner of Canada

TABLE OF CONTENTS

INTRODUCTION 1
1. SCOPE OF APPLICATION OF THE ACT 5
   1.1 Personal information 5
   1.2 Commercial activity 7
2. PIPEDA BEYOND CANADA 11
   2.1 Outsourcing 11
   2.2 PIPEDA's application to foreign entities 13
3. SURVEILLANCE PHENOMENA 17
   3.1 Security surveillance 17
   3.2 Employee surveillance 20
4. EMERGING TECHNOLOGIES 23
   4.1 Biometrics 23
   4.2 GPS 25
5. DATA BREACHES AND SECURITY MEASURES 27
   5.1 Data security breaches 27
   5.2 Other cases on security measures 29
6. CARELESS DISCLOSURES AND NEED FOR ONGOING EMPLOYEE TRAINING 35
   6.1 Social engineering and pretexting 35
   6.2 Careless errors 37
7. COLLECTING TOO MUCH INFORMATION 41
   7.1 Product returns and credit card usage 41
   7.2 Opening accounts and related activities 43
   7.3 Collection of health information 43
8. MEANINGFUL ACCESS TO PERSONAL INFORMATION 45
   8.1 General principles of access 45
   8.2 The impact of parallel litigation proceedings 46
   8.3 Fees for access 47
9. SECONDARY MARKETING PURPOSES 51
   9.1 Telecommunications 51
   9.2 Banking 53
   9.3 Retail 55
   9.4 Airlines 56
Conclusion 57
Table of leading cases 59

INTRODUCTION

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) was implemented in phases over a three-year period that began on January 1, 2001.

PIPEDA applies to every organization in respect of personal information that the organization collects, uses or discloses in the course of its commercial activities.[1] PIPEDA also applies to federal works, undertakings and businesses in respect of employee personal information that they collect, use or disclose in connection with their operations, whether or not these involve commercial activity *per se*.[2]

PIPEDA does not apply to an organization in respect of personal information that the organization collects, uses or discloses within Alberta, British Columbia or Quebec, (or within Ontario, in respect of personal health information collected, used or disclosed by health information custodians governed by Ontario's *Personal Health Information Protection Act*[3]) *unless*:

> (1) the organization is a federal work, undertaking or business; or
>
> (2) the personal information is disclosed outside of a province in the course of a commercial activity.

These provinces have enacted privacy laws that have been declared substantially similar to PIPEDA.[4] As a result, the collection, use or disclosure of personal information by organizations in the course of commercial activities in these provinces will be subject to the applicable provincial laws, and *not PIPEDA*, except as provided above. PIPEDA applies to organizations' commercial activities in all other provinces.[5]

---

1 The concept of "commercial activity" is discussed in section 1 of this document.

2 See PIPEDA, s. 4(1)(b).

3 *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Schedule A [*PHIPA*].

4 *Personal Information Protection Act*, S.A. 2003, c. P-6.5; *Personal Information Protection Act*, S.B.C. 2003, c. 63; *An Act Respecting the Protection of Personal Information in the Private Sector* R.S.Q., chapter P-39.1. Ontario's *PHIPA* has also been deemed substantially similar to PIPEDA.

5 Organizations in the Northwest Territories, Yukon and Nunavut are considered federal works, undertakings or businesses and therefore are covered by PIPEDA in respect of their collection, use and disclosure of personal information in the course of commercial activities, and in respect of employee personal information.

PIPEDA requires organizations to comply with a set of legal obligations that are based on the following ten principles: (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, and (10) Challenging compliance. Subsection 5(3) of PIPEDA contains the over-arching rule that organizations may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Under PIPEDA, individuals may file with the Commissioner a written complaint against an organization for contravening specified provisions of the Act.[6] As well, the Commissioner may initiate a complaint where the Commissioner is satisfied that there are reasonable grounds to investigate a matter.

The role of the Office of the Privacy Commissioner of Canada (the "Commissioner") under PIPEDA is to investigate complaints, make findings and issue non-binding recommendations where appropriate. The individual or the Commissioner may then proceed to Federal Court to seek legal enforcement.

The Commissioner has issued hundreds of findings under the Act.[7] Canadian courts have also issued numerous decisions. Seven years into the operation of PIPEDA, this growing body of case findings and court decisions provides practical insight into how some of the provisions of PIPEDA should be interpreted.

This document provides businesses and individuals with an overview of leading findings and court decisions under PIPEDA to date. Reflecting the organic manner in which the cases have evolved through the complaint mechanism in PIPEDA, this document organizes leading cases around several emerging themes:

1. **Scope of Application of the Act**
   Leading cases under PIPEDA have helped define "personal information", "commercial activity" and other essential concepts to help organizations determine whether or not PIPEDA applies in a given situation.

2. **PIPEDA Beyond Canada**
   Landmark cases on outsourcing and other cross-border activities have interpreted the boundaries of PIPEDA.

3. **Surveillance Phenomena**
   Surveillance cases are among the most contentious cases arising under the Act. Key cases have established important guidance in this area to help organizations distinguish between appropriate and inappropriate surveillance.

6 See PIPEDA, s. 11(1). An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation set out in Schedule 1.

7 The Commissioner's findings and related documents are available at http://www.privcom.gc.ca.

4. **Emerging Technologies**
   At the frontiers of PIPEDA, several cases have addressed complex privacy issues arising from the adoption and application of new technologies, including biometrics and global positioning systems.

5. **Data Breaches and Security Measures**
   High-profile data breach cases have helped define the security safeguards and procedures that organizations must put in place to protect personal information.

6. **Careless Disclosures and Need for Ongoing Employee Training**
   A number of cases have addressed situations involving careless or inadvertent disclosures of personal information. These cases often emphasize the critical importance of implementing employee training as an ongoing process, rather than a simple one-time endeavour.

7. **Collecting Too Much Information**
   Leading cases in the retail and employment sectors have helped define how organizations should limit the quantity and nature of personal information collected for different purposes, thereby reducing the risk of inappropriate use and disclosure down the line.

8. **Meaningful Access to Personal Information**
   Several cases have resolved important concerns about individuals' right to access their personal information, including cases involving parallel litigation proceedings and those relating to fees for access.

9. **Secondary Marketing Purposes**
   Key cases have established a framework for determining when opt-in versus opt-out consent is appropriate, as well as consent issues generally in the context of improper uses and disclosures of information for secondary marketing purposes.

The Commissioner and the courts have together developed an essential body of recommendations and case law over the first seven years of PIPEDA that can now better assist organizations and individuals to understand their privacy rights and obligations in Canada. Leading cases stand as powerful examples of PIPEDA in concrete action, and help chart the course for the future, particularly as organizations deploy new technologies to remain competitive in a global economy and struggle to establish responsible personal information practices that balance individual privacy rights with legitimate business needs. The key cases referred to in this document have been categorized in a table which is annexed as Appendix 1 to this document for ease of reference.

1. SCOPE OF APPLICATION OF THE ACT

PIPEDA applies to the collection, use, and disclosure of "personal information" by an organization in the course of a "commercial activity"[8].

1.1 Personal information

PIPEDA only applies to the collection, use and disclosure of "personal information." This term is broadly defined in subsection 2(1) as "information about an identifiable individual", excluding "the name, title or business address or telephone number of an employee of an organization." Although it is not always straightforward to decide whether information is "personal information," a number of key cases under PIPEDA have begun grounding the broad definition of "personal information". For example, cases have held that the following types of information meet the definition:

- Photographs;[9]
- Business e-mail addresses;[10]
- An identification number used to refer to an employee;[11] and
- Computer Internet protocol (IP) addresses.[12]

8 Both "personal information" and "commercial activity" are defined in section 2(1) of PIPEDA.

9 PIPEDA Case Summary #349- Photographing of tenants' apartments without consent for insurance purposes - http://www.privcom.gc.ca/cf-dc/2006/349_20060824_e.asp

10 PIPEDA Case Summary #297 - Unsolicited e-mail for marketing purposes - http://www.privcom.gc.ca/cf-dc/2005/297_050331_01_e.asp

11 PIPEDA Case Summary #149 - Individual denied access to personal information - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030409_2_e.asp

12 PIPEDA Case Summary #25 - A broadcaster accused of collecting personal information via Web site - http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011120_e.asp; PIPEDA Case Summary #315 - Web-centered company's safeguards and handling of access request and privacy complaint questioned - http://www.privcom.gc.ca/cf-dc/2005/315_20050809_03_e.asp; PIPEDA Case Summary #319 - ISP's anti-spam measures questioned - http://www.privcom.gc.ca/cf-dc/2005/319_20051103_e.asp. Computers utilize IP addresses when they communicate with one another on the Internet or other networks. Each computer is assigned a unique IP address while it is connected to the Internet. Knowing the IP address of a computer at a given time will, with the aid of the individual's internet service provider (ISP), usually permit an organization to identify the subscriber who was online at the time.

In a case where a property manager took photographs to show the condition of tenants' apartments for insurance purposes, the Assistant Commissioner made clear that the photographs, to the extent they are capable of identifying an individual, will meet the definition of personal information – in other words, the individual must be "identifiable" or "capable of being identified", and not necessarily identified.[13] In this case, the Assistant Commissioner concluded that the photographs might reveal information about the unit dweller and his or her standard of living, including whether they love music, art or cooking. Each photograph could be traced to an individual because the unit number and building address were listed under the photographs. This information was therefore capable of identifying the individuals.

IP addresses can be personal information since the numbers are about an identifiable individual, namely the ISP subscriber.[14] In *BMG Canada Inc. v. Doe*,[15] the Federal Court of Appeal held that ISPs cannot voluntarily disclose the identity of subscribers who were assigned particular IP addresses at given times unless consent is obtained or a lawful exception applies.

The Federal Court also discussed the concept of identifiability in *Gordon and Minister of Health and Privacy Commissioner of Canada*.[16] In analysing what constitutes identifiable information, the Court adopted the following test urged by the Privacy Commissioner:

> Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.[17]

On the facts of this case, the Court agreed with a refusal by Health Canada to disclose the 'province' field of the Canadian Adverse Drug Reaction Information System (CADRIS) database. The Court held that disclosure of the province field, when combined with other data-fields already released as well as other publicly available information (such as obituaries, for example), would "substantially increase the possibility" that particular individuals could be identified..[18] This was especially the case for unique or quasi-unique individual reports in smaller provinces or territories.

Another key issue that has arisen in interpreting whether information is "personal information" is how to distinguish information 'about' an individual from information

13 PIPEDA Case Summary #349, *supra* note 9.

14 See the cases an accompanying text, *supra* note 12.

15 *BMG Canada Inc. v. Doe*, 2005 FCA 193 (CanLII) at para. 37 - http://www.canlii.org/en/ca/fca/doc/2005/2005fca193/2005fca193.html

16 *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII) - http://www.canlii.org/en/ca/fct/doc/2008/2008fc258/2008fc258.html. This case arose under the *Privacy Act*, R.S.C. 1985, c. P-21 and the *Access to Information Act*, R.S., 1985, c. A-1.

17 *Ibid*., at para. 34.

18 *Ibid*., at para. 43.

that merely represents their 'work product'. In an early finding, the former Privacy Commissioner found that physicians' prescriptions constitute their work product information and not their personal information.[19] Since this finding, however, the Commissioner's approach has evolved to a broader, contextual one. For example, in other contexts, the sales statistics of individual telemarketers[20] and the number of houses sold in a year by named real estate brokers[21] were found to constitute their personal information, subject to reasonable protection under PIPEDA. Just because information is produced in the workplace does not mean it is not personal information deserving of protection. Other contextual factors, such as, how it was produced, for what purposes, how it will be used, industry practices, etc. must also inform the analysis.

In *Wyndowe and Rousseau and Privacy Commissioner of Canada,*[22] the Federal Court of Appeal refused to read in an implicit work product exception from the current definition of "personal information" in PIPEDA. The Court of Appeal held that the handwritten notes of a doctor performing an independent medical examination ("IME") of an insured person on behalf of, and paid by, an insurance company, are not purely work product information of the physician, but rather, could constitute both the personal information of the individual examined as well as the personal information of the doctor performing the IME. Accordingly, a balancing exercise – taking into consideration the private interests of the individual and the doctor, as well as the broader public interest for and against disclosure – must be applied in determining which portions of the notes should be disclosed to the individual.[23]

1.2 Commercial activity

Subsection 2(1) of PIPEDA defines "commercial activity" as any "transaction, act or conduct or any regular course of conduct that is of a commercial character". The definition expressly includes "selling, bartering or leasing of donor, membership or other fundraising lists".

Several leading cases address the meaning of "commercial activity", including, for example:

- The Assistant Commissioner held that a daycare organization was engaged in commercial activities because

19 PIPEDA Case Summary #14 - Selling of information on physicians' prescribing patterns - http://www.privcom.gc.ca/cf-dc/2001/cf-dc_010921_e.asp; PIPEDA Case Summary #15 - Privacy Commissioner releases his finding on the prescribing patterns of doctors - http://www.privcom.gc.ca/media/an/wn_011002_e.asp

20 PIPEDA Case Summary #220 - Telemarketer objects to employer sharing her sales results with other employees - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030915_e.asp

21 PIPEDA Case Summary #303- Real estate broker publishes names of top five sales representatives in a city - http://www.privcom.gc.ca/cf-dc/2005/303_20050531_e.asp

22 *Wyndowe v. Rousseau*, 2008 FCA 39 (CanLII) - http://www.canlii.org/en/ca/fca/doc/2008/2008fca39/2008fca39.html

23 The Federal Court of Appeal adopted a balancing test similar to the one it had previously adopted in the context of a complaint arising under the Access to Information Act in *Canada (Information Commissioner)* v. *Canada (Minister of Citizenship and Immigration)*, [2002] F.C.J. No. 950, 2002 FCA 270.

it received payment for child care services, despite the fact that it was a non-profit organization;[24]

- The Assistant Commissioner held that law firms were engaged in a commercial activity where they sought credit reports on potential adverse litigants in the course of representing their clients – a professional service for which they were clearly compensated;[25]

- The Ontario Superior Court of Justice held that an organization's not-for-profit status is not determinative of whether its collection, use or disclosure of personal information is carried out in the course of a commercial activity in given situation;[26] and

- The Federal Court of Appeal held that when a doctor conducts an independent medical examination of an insured person on behalf of, and paid by, an insurance company, for the purpose of processing a claim for insurance benefits, he does so "in the course of a commercial activity".[27]

In a case involving allegations that the scholarship committee of a private school inappropriately disclosed an applicant's financial information to third parties, the Assistant Commissioner developed a two-part test for determining whether a charitable activity (in this case, education) meets the definition of "commercial activity":

1. What is the institution's core activity? Is the institution providing educational services as its core activity? If so, the activities should presumptively be considered not to have a "commercial character."

2. The presumption that the activities of an educational institution do not have a commercial character will be rebutted if the

24 PIPEDA Case Summary #309 - Daycare denied parent access to his personal information - http://www.privcom.gc.ca/cf-dc/2005/309_20050418_e.asp

25 PIPEDA Case Summary #340 - Law firms collected credit reports without consent - http://www.privcom.gc.ca/cf-dc/2006/340_20060502_e.asp

26 *Rodgers v. Calvert*, 2004 CanLII 22082 (ON S.C.) at paragraph 51. Although the court held that not-for-profit status was not determinative of the issue of whether the organization was engaged in a commercial activity, the court ultimately found that the organization in this case was not engaged in a commercial activity when it collected membership fees because "there must be something more than a mere 'exchange of consideration' to characterize a transaction as commercial".

27 *Wyndowe v. Rousseau*, *supra* note 22.

> institution has, as one of its objectives, the goal of earning a profit for the owners of the institution.[28]

Applying this test, the Assistant Commissioner concluded that the organization in question was a private school, with education as its main activity. On the second branch of the test, the Assistant Commissioner found no indication that the school's goal was to earn a profit for its owners and the evidence supported the institution's claim to be a charitable, not-for-profit organization. Therefore, the school was able to uphold the presumption that its core educational activities were of a non-commercial character.

28 PIPEDA Case Summary #345 - Private school not covered by PIPEDA - http://www.privcom.gc.ca/cf-dc/2006/345_20060705_e.asp. The Commissioner has published a Fact Sheet describing the application of PIPEDA to the "MUSH" sector – municipalities, universities, schools and hospitals. See http://www.privcom.gc.ca/fs-fi/02_05_d_25_e.asp

2. PIPEDA BEYOND CANADA

Cross-border activities have raised high-profile privacy concerns in Canada. Particular concerns have been raised about outsourcing arrangements that involve the transfer of Canadians' personal information to service providers located in or linked to the United States. Service providers located in the United States may be compelled to disclose Canadians' personal information to American authorities under the *USA PATRIOT Act*, or other lawful authority, without notice to the affected individuals.

Similar concerns have arisen in respect of the disclosure of Canadians' banking information to U.S. authorities. In these and other 'hot-button' areas, cross border activities have been the subject of landmark cases that have pushed the boundaries of PIPEDA beyond Canada's physical borders.

2.1 Outsourcing

Principle 4.1.3 of PIPEDA imposes the following obligation on organizations that outsource business functions that involve the transfer of personal information to a third party service provider:

> An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Under a separate provision, Principle 4.8, PIPEDA requires organizations to be open about their policies and practices relating to the management of personal information.

In 2005, both Principles 4.1.3 and 4.8 were at issue in a ground-breaking case before the Assistant Privacy Commissioner.[29] In this case, CIBC sent a notice to its VISA customers to inform them that it used a service provider located in the United States to process and store payment transactions and that customers' personal information may be accessible to

29 PIPEDA Case Summary #313 – Bank's notification to customers triggers PATRIOT Act concerns - http://www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp

U.S. authorities. CIBC's outsourcing arrangement had been approved by the Office of the Superintendent of Financial Institutions. CIBC had in place a contract with its service provider that included, among other things, terms regarding confidentiality, security, monitoring, oversight, audit, custody and control.

This case serves as a good reminder that, in situations where an organization outsources personal information for processing by a third-party service provider located in a foreign country, the organization remains accountable for the personal information under Principle 4.1.3. The Assistant Commissioner concluded here that CIBC had met its obligation to provide a comparable level of protection under Principle 4.1.3. through appropriate contractual means. Although there was a risk that personal information could be disclosed to U.S. authorities, the Assistant Commissioner concluded that the risk was comparable to the risk of mandatory disclosure to Canadian authorities under lawful authority here, had the service provider been located in Canada.

The Assistant Commissioner noted that PIPEDA cannot prevent covered organizations from outsourcing to foreign-based service providers. Nor can PIPEDA prevent foreign governments from compelling production of personal information controlled by organizations within their own jurisdiction and under their lawful authority. However, what the Act does demand is that the covered organization be transparent about their personal information handling practices and protect customer personal information in the hands of foreign-based third-party service providers to the extent possible by contractual means.

The CIBC case demonstrates that, taken together, Principle 4.1.3 and Principle 4.8 require that the covered organization at a minimum (1) have in place contractual or other means to provide a comparable level of protection, (2) inform its customers about its policies and practices related to the management of personal information, and 3) notify customers that their personal information may be available to a foreign government or its agencies under a lawful order made in that country.

Not long after the CIBC case, the Assistant Commissioner issued a finding regarding the cross-border sharing of personal information between a subsidiary and a parent company.[30] In this case, the Canadian division of a security company gave notice to its customers that in certain circumstances it might share information with its American parent company. The notification stated that if a catastrophic event overwhelmed a Canadian-based customer monitoring centre, then the incoming alarm signals might be routed to another monitoring centre, including one located in the United States. Customers were given the option of opting out of this sharing but were advised that they might receive a reduced level of security service if they did so.

In outsourcing situations where the organizations are related, such as a parent and a subsidiary, the Assistant Commissioner held that, although a contract is not needed

30 PIPEDA Case Summary #333 - Canadian-based company shares customer personal information with U.S. parent - http://www.privcom.gc.ca/cf-dc/2006/333_20060511_e.asp

between the related organizations, both organizations must nonetheless adhere to the same levels of data protection. In this case, the organizations had in place a closed private network and comprehensive measures to safeguard information. The Assistant Commissioner found that the organizations had provided a comparable level of protection and that customers had been given adequate notice of the risk of mandatory disclosure to lawful authorities in the United States.

In 2007, the Assistant Commissioner was faced with a third major cross-border outsourcing case – the SWIFT case.[31] The SWIFT case involved a mass disclosure of personal banking information to U.S. authorities by a service provider, SWIFT, located in Belgium. SWIFT is the Society for Worldwide Interbank Financial Telecommunication.

Canadian banks have agreements in place with SWIFT under which the banks transfer customers' personal financial information to SWIFT for the processing of foreign-bound financial messages, including money orders.

In investigating the complaint against the Canadian banks, the Assistant Commissioner carefully reviewed the contracts between the banks and SWIFT. Following the reasoning in the CIBC case, the Assistant Commissioner was satisfied that the contracts and other measures in place between the banks and SWIFT ensured a comparable level of protection. She was also satisfied that the banks had provided their customers with adequate notice of the risk of possible mandatory disclosure to foreign authorities by way of clear statements in the banks' privacy policies. Accordingly, the Assistant Commissioner found that the complaint against the Canadian banks was not well-founded.

In the context of a separate Commissioner-initiated complaint, the Commissioner considered the application of PIPEDA to SWIFT.[32] This important analysis is discussed in the next section on PIPEDA's application to foreign entities.

2.2 PIPEDA's application to foreign entities

In two landmark cases in 2007, the application of PIPEDA extended well beyond Canadian borders.

In *Lawson v. Accusearch*,[33] the Federal Court set aside a decision by the Assistant Commissioner that she lacked the jurisdiction to investigate a complaint made against an entity located outside of Canada in the particular circumstances of that case. The case involved a U.S. corporation that allegedly collected, used and disclosed personal information about individuals to paying customers. This included individuals and

31 PIPEDA Case Summary #365 - Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered - http://www.privcom.gc.ca/cf-dc/2007/365_20070402_e.asp

32 Report of Findings (April 2, 2007) - http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_e.asp

33 *Lawson v. Accusearch Inc.*, 2007 FC 125 (CanLII) - http://www.canlii.org/en/ca/fct/doc/2007/2007fc125/2007fc125.html; reversing "The Privacy Commissioner of Canada today released a letter about Abika.com, an on-line data broker in the U.S. that collects, uses and discloses the personal information of Canadians." (November 18, 2005) - http://www.privcom.gc.ca/legislation/let/let_051118_e.asp

customers in Canada, as well as many other countries. The complainant, resident in Canada, ordered, paid for and obtained from the company a background check on herself in order to demonstrate the company's personal information practices and support her contention that these were inappropriate and contrary to PIPEDA.

The Federal Court agreed with the Assistant Commissioner that PIPEDA was not intended to apply extra-territorially – "Parliament cannot have intended that PIPEDA govern the collection and use of personal information worldwide". Nevertheless, the Court held that PIPEDA could still cover foreign entities that either receive or transmit communications to and from Canada, and that collect and disclose personal information *about individuals in Canada*. In the particular circumstances of this case, the Court concluded that the complainant's personal information had to have come from Canadian-based sources, even though those sources could not be identified.[34] However, the Court did not specifically address which real and substantial connecting factors to Canada must be present in future cases for the Commissioner to have jurisdiction to investigate. The fact that the investigation might be frustrated and ineffective in practice, because of the lack of collaboration by the organization and the difficulty of the Commissioner to exercise her subpoena powers over non-residents, does not preclude the Commissioner from asserting jurisdiction over the matter in the first place. The Court returned the matter to the Commissioner and directed that the Commissioner investigate the complaint against the U.S. based company in question, despite the practical difficulty that might entail.

The second case to address PIPEDA's application to foreign entities is the Commissioner-initiated complaint against SWIFT in the matter discussed above.[35] In parallel with the complaint against the Canadian banks involved, the Commissioner had to consider whether PIPEDA also covers the activities of SWIFT, the Belgium-based outsourcer that collected client financial data from Canadian banks for the purpose of processing and disclosed it to U.S. authorities. In assessing whether SWIFT was subject to PIPEDA, the Commissioner considered the following real and substantial links between SWIFT and Canada:

- SWIFT collected personal information from and disclosed it to Canadian banks;
- SWIFT charged the Canadian banks a fee for its services;
- 14 of SWIFT's shareholders were Canadian;
- one of SWIFT's directors was from a Canadian bank;

34 *Ibid.* (At paragraph 41, the Court stated: "Although the Commissioner faintly argued that there was no evidence of a connection with Canada that was not the basis of her decision. Even if the "psychological profile" on Ms. Lawson was pure fiction and written in the United States, much of the data had to have come from Canada. The Commissioner acknowledged this in her decision when she wrote: 'Abika.com has not responded to our request for the names of its Canadian-based sources.").

35 Report of Findings, *supra* note 31.

- the vast majority of the cross-border transfers of personal information to and from Canadian banks were transmitted by SWIFT; and
- SWIFT was an integral part of the Canadian financial system.

On the basis of these real and substantial connecting factors, the Commissioner concluded that SWIFT was engaged in a commercial activity within Canada, and therefore, was subject to the organizational responsibilities under PIPEDA.

On the substantive question of whether SWIFT violated PIPEDA, the Commissioner concluded that paragraph 7(3)(c) permitted SWIFT to disclose the information, as it did, in response to a valid subpoena issued in the United States. In the Commissioner's view, paragraph 7(3)(c) of PIPEDA permits organizations to respond to subpoenas, warrants and orders of not only Canadian authorities and courts, but foreign ones also. The Commissioner noted that it would be "unrealistic and unworkable" to ask multi-national companies to ignore the legitimate laws of other foreign jurisdictions where they operate in addition to Canada. To do so might be tantamount to infringing the sovereignty of another nation.[36] Organizations that legitimately move personal information outside of Canada[37] should therefore be permitted, in accordance with paragraph 7(3)(c), to disclose information to foreign authorities under lawful authority of those other countries in which they operate.

36 *Ibid*. at paragraph 48.

37 See the discussion in section 2.1 of this document.

3. SURVEILLANCE PHENOMENA

Surveillance is one of the most contentious issues under PIPEDA. Surveillance cases are an important focal point for the definition of appropriate purposes in subsection 5(3) of PIPEDA.

Subsection 5(3) of PIPEDA permits organizations to collect, use or disclose personal information "only for purposes that a reasonable person would consider are appropriate in the circumstances." This is an over-arching requirement of the Act. It cannot be waived by consent and it applies notwithstanding any consent exceptions which may also find application.

For example, paragraph 7(1)(b) of PIPEDA permits the collection of information without consent if:

> 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.

Organizations often rely on this exception when using surveillance to deter crime or to investigate employee misconduct. However, even if organizations could demonstrate that their use of video-surveillance falls within this consent exception, they must still be able to demonstrate that their purpose in resorting to video-surveillance without consent is one that a reasonable person would consider to be appropriate in the circumstances within the meaning of subsection 5(3).

3.1 Security surveillance

The seminal surveillance case under PIPEDA is *Eastmond v. Canadian Pacific Railway*.[38] This case has been cited with approval in many subsequent cases.

38 PIPEDA Case Summary #114 - Employee objects to company's use of digital video surveillance cameras - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp; *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 (CanLII), (2004), 16 Admin. L.R. (4th) 275 - http://www.canlii.org/en/ca/fct/doc/2004/2004fc852/2004fc852.html

In the *Eastmond* case, employees filed a complaint under PIPEDA after their employer, Canadian Pacific Railway (CPR), installed six fixed video cameras in a rail yard. The cameras could not pan or zoom. CPR retained the recordings from the cameras for a limited period of time in a locked cabinet. The tapes were overwritten if no incidents were reported that might have been caught on camera. The recordings were otherwise not monitored or reviewed by CPR.

CPR's stated purposes for installing the six cameras were (1) to deter incidents of theft, vandalism and trespassing, (2) to improve employee security, and (3) to aid in the investigation of any reported incidents occurring within the facility.

In assessing whether a reasonable person would find CPR's purposes to be appropriate in the circumstances, the Commissioner developed and applied a four part test under subsection 5(3) of PIPEDA:

(i) **Is camera surveillance and recording demonstrably necessary to meet a specific need?**

(ii) **Is camera surveillance and recording likely to be effective in meeting that need?**

(iii) **Is the loss of privacy proportional to the benefit gained?**

(iv) **Is there a less privacy-invasive way of achieving the same end?**

In applying the test in *Eastmond*, the Commissioner concluded that CPR's purposes were not appropriate because it had failed to demonstrate that there was a real, specific problem in need of attention. The Commissioner added that even if CPR had shown evidence of a problem, the Commissioner was not convinced that the cameras would have been effective in addressing it. The complainant applied to the Federal Court under section 14 of PIPEDA.

Although the Federal Court noted that the four-part test developed by the Commissioner might not be applicable in all other contexts, the Court proceeded to apply the four-part test based on fresh evidence adduced at the *de novo* hearing and came to a different result. This analysis is critical for any organization considering adopting a surveillance measure.

Under the first element of the test, the Court held that CPR had established a legitimate need to install the cameras based on the history of incidents at the yard and at other yards. This history, along with the possible deterrent effect of the cameras against future incidents, was sufficient to show a real problem in need of a solution.

Second, relying on evidence that no incidents had been reported at the yard since the cameras had been installed, the Court held that the cameras were likely effective in meeting CPR's need. The Court also relied on evidence of effectiveness of similar surveillance measures at CPR's other yards.

Third, the Court held that the loss of privacy was proportional to the benefit gained. In this case, the security benefits of the cameras had been made out. The loss of privacy was minimal because (1) the recording took place where individuals had a reduced expectation of privacy and (2) CPR had taken a number of steps to ensure that the invasion of privacy was kept to the minimum necessary to meet its purposes, including:

- CPR posted signs warning that cameras were present;
- The cameras did not track employees because the cameras could not move;
- The cameras were not targeted specifically at employees – contractors, visitors, suppliers and trespassers would all be captured by the cameras;
- The cameras were not intended to aid in evaluating worker performance; and
- The recordings were kept secure and the only time they were ever accessed was by CPR managers or police if an incident was reported.

Finally, in assessing whether there was a less privacy-invasive way for CPR to meet its goal in a cost-effective manner, the Court accepted CPR's evidence that it had considered and rejected other alternatives, including fences and security guards.

In the result, the Court concluded that a reasonable person would find CPR's purposes to be appropriate in the circumstances of this case.

Since *Eastmond*, and a number of other relevant cases involving use of video surveillance, the Commissioner has developed guidelines for organizations to consider when contemplating introducing video surveillance on their premises.

OPC Guidelines for Overt Video Surveillance in the Private Sector (March 2008) http://www.privcom.gc.ca/information/guide/2008/gl_vs_080306_e.asp

1. Determine whether a less privacy-invasive alternative to video surveillance would meet your needs.
2. Establish the business reason for conducting video surveillance and use video surveillance only for that reason.
3. Develop a policy on the use of video surveillance.
4. Limit the use and viewing range of cameras as much as possible.
5. Inform the public that video surveillance is taking place.
6. Store any recorded images in a secure location, with limited access, and destroy them when they are no longer required for business purposes.
7. Be ready to answer questions from the public. Individuals have the right to know who is watching them and why, what information is being captured, and what is being done with recorded images.
8. Give individuals access to information about themselves. This includes video images.
9. Educate camera operators on the obligation to protect the privacy of individuals.
10. Periodically evaluate the need for video surveillance.

Note: *These Guidelines apply to overt video surveillance of the public by private sector organizations in publicly accessible areas. They do not apply to covert video surveillance, such as that conducted by private investigators on behalf of insurance companies, or to employee surveillance.*

3.2 Employee surveillance

In another precedent-setting case, an organization used cameras – cameras that were normally used to monitor train movements and to inform crew members of train locations – to determine that employees left company property during regular working hours.[39] The employees were disciplined. Other than this incident, however, the organization did not demonstrate that there was a persistent problem with unauthorized absences by the complainants or any other employees. Nor did the organization demonstrate that it had considered other means to address unauthorized absences.

The Assistant Commissioner found that the use of the cameras for disciplinary purposes in this case would not be considered by a reasonable person to be appropriate in the circumstances, and therefore, was contrary to subsection 5(3) of PIPEDA. The Commissioner emphasized that the first avenue of recourse should always be the least privacy-invasive way of achieving the result, even in cases where an organization is relying on the exception under paragraph 7(1)(b) to collect the information without consent.

Other leading surveillance cases that have arisen in the employment context have established the following principles:

39 PIPEDA Case Summary #265 - Video cameras in the workplace - http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_02_e.asp

- Continuous, indiscriminate camera surveillance is not appropriate if it is trained on employee work areas with the express purpose of, among other things, managing employee productivity, especially when that purpose could be achieved by less invasive means – the Assistant Commissioner held that the "cost to human dignity [must] form part of the equation" in balancing surveillance;[40]

- Cameras are appropriate if the clearly demonstrated purpose for their use is for legitimate security reasons, if they are trained on areas of access to the facility and not on work areas, if the recordings are stored for a limited time then overwritten and if employees are advised of the rationale for their use and of the purposes for which their personal information is being collected;[41]

- Cameras are not appropriate in the workplace if they are not demonstrably necessary to meet an operational need or if they are not likely to be effective in meeting such need; for example, where the images captured by the cameras are not clear enough to ensure product safety -- which the company claims as its purpose -- and where there are other more effective, and less privacy-invasive means, of accomplishing that objective;[42] and

- Retaining an investigator to conduct surveillance is appropriate under paragraph 7(1)(b) if an organization has reasonable and probable cause to suspect that an employee is violating his employment contract by misrepresenting the state of his health, and less privacy–invasive means were attempted without success.[43]

An additional leading case involving surveillance by a global positioning system (GPS) is discussed in the next section of this document on Emerging Technologies.

40 PIPEDA Case Summary #279 - Surveillance of employees at work - http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040726_e.asp

41 PIPEDA Case Summary #264 - Video cameras and swipe cards in the workplace - http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_01_e.asp

42 PIPEDA Case Summary #290 - Video surveillance cameras at food processing plant questioned - http://www.privcom.gc.ca/cf-dc/2005/290_050127_e.asp. It was also relevant that the cameras did not provide a clear image of the food products being processed.

43 PIPEDA Case Summary #269 - Employer hires private investigator to conduct video surveillance on employee - http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040423_e.asp

4. EMERGING TECHNOLOGIES

PIPEDA was enacted in part as a response to technological threats to privacy. Section 3 makes this purpose clear: "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…"

PIPEDA does not contain provisions that address particular types of technologies. The statute is a general regulatory instrument that applies across all sectors and activities; it is technology-neutral. Yet, it is not surprising that privacy threats have regularly arisen in connection with the use of emerging technology.

Technology is at the root of many activities that are potentially privacy-invasive. At the frontiers of PIPEDA, several important cases have addressed privacy issues arising from new technologies, including biometrics and GPS.[44]

4.1 Biometrics

In one key technology case, the Assistant Commissioner was faced with a complaint made by employees that their employer was requiring them to provide "voice print" biometric information for the purpose of authenticating users and securing remote access to the internal network. Employee access to this network was necessary for logging work-related information and absence reporting.[45] The principal issue in the case was whether the use of voice-recognition technology – called e.Speak -- was "for purposes that a reasonable person would consider are appropriate in the circumstances" within the meaning of subsection 5(3) of PIPEDA.

The voice-recognition system was chosen by the organization because its field employees carried phones on job sites and the system would provide an efficient means of permitting them to log into the organization's internal network from the field. The organization determined that the voice-recognition system was preferable to a traditional password-based system and offered the highest and most cost-effective level of security for customer

44 Technology is also implicated in the definition of "personal information". See the discussion of IP addresses and online activities in section 1.1 of this document.

45 PIPEDA Case Summary #281 - Organization uses biometrics for authentication purposes - http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040903_e.asp

data logged by employees. The organization implemented a number of tight security controls over the voice-print database and permitted a limited number of employees to access the database for limited purposes. Voice-prints were deleted within one month of an employee being no longer eligible to use the system.

Considering these factors, together with the fact that a voice-print is relatively non-sensitive personal information and that the e-speak system in this case actually enhanced the security of customers' personal information, the Assistant Commissioner found the organization's purposes to be appropriate according to the reasonable person standard of subsection 5(3). Because employees had to actively provide a sample of their voice to be included in the system, the Assistant Commissioner found that the organization had obtained implied consent of individuals whose voice-prints were collected. This finding of implied consent was not without difficulty, however, particularly given the reality of an employment context and the unequal bargaining power between employer and employee.

Pursuant to section 14 of PIPEDA, the employees applied for a hearing of their complaint in Federal Court[46] and subsequently appealed to the Federal Court of Appeal.[47] Both Courts agreed that the company's purpose for adopting the e-speak system was one which a reasonable person would consider in the circumstances, based on the following analysis:

- The degree of sensitivity associate with voice prints as personal information;
- The security measures implemented by Telus;
- The *bona fide* business objectives of Telus to which the voiceprints were directed;
- The effectiveness of voice prints in meeting those objectives;
- The reasonableness of the collection of voice prints against alternative methods of achieving the same levels of security at comparable cost and with comparable operational benefits; and,
- The proportionality of the loss of privacy of employees as against the employer's costs and operational benefits in the level of security it provides.

On the issue of consent, the Federal Court of Appeal confirmed that all of the exceptions to collection, use and disclosure of personal information without consent are set out exhaustively in section 7 of PIPEDA and that none of them applied in these circumstances. However, the Court noted that, by its very design, the e-Speak system ensures that individual consent must be provided prior to collecting their voiceprints, for without employees' active participation, the company could not create their voiceprint

46 *Turner v. TELUS Communications Inc.*, 2005 FC 1601 (CanLII)

47 *Wansink v. TELUS Communications Inc.* (F.C.A.) 2007 FCA 21 (CanLII)

and forcibly enrol them into the system. Interestingly, the Court of Appeal left open the question of whether alleged threats of disciplinary measures against non-consenting employees might vitiate meaningful consent under the Act.[48]

4.2 GPS

In a later key case involving technology, the Assistant Commissioner investigated a complaint made by employees that their employer was installing GPS units on work vehicles in order to track their daily movements while on the job including start and stop times, speed, location, mileage, and off-shift parking location.[49] It could not be turned off by the driver. The Assistant Commissioner found that the GPS data associated with an individual driver was "personal information", even though individual drivers of the vehicles were not always directly identified to all employees with access to the GPS data. Similar to the biometric case above, and other cases discussed in the Surveillance section of this document, the primary issue was whether the use of the GPS system for the organization's claimed purposes was something that a reasonable person would consider appropriate in the circumstances.

The organization claimed the following purposes for adopting the GPS system and for using the information it collected:

- *Managing workforce productivity*: The organization claimed that the GPS would be used to locate, dispatch and route employees to job sites. Information on the start and stop times of the vehicle and its location will be used in capacity planning, productivity analysis, and performance management, as required;

- *Safety and development*: The organization claimed that GPS would be used to determine if a vehicle has remained stationary for an inordinate amount of time and could provide an indication that the employee's safety may be at risk. As well, the information gathered by GPS may identify those employees who may require defensive/ safe driver training or individual coaching based on speed statistics; and

- *Asset protection and management*: Information gathered by GPS on a vehicle's location could be used to retrieve it in the event that it is stolen, abandoned or scheduled for maintenance. The organization claimed that it had

48 *Ibid.* at paragraph 28. The court noted in obiter at paragraph 29, however, that if TELUS had made threats of disciplinary measures such as suspension or firing if employees did not participate in the voice-print system, then such threats might vitiate consent.

49 PIPEDA Case Summary #351 - Use of personal information collected by Global Positioning System considered - http://www.privcom.gc.ca/cf-dc/2006/351_20061109_e.asp

also achieved cost savings since it had installed the GPS, including reduced driving and fuel consumption.

The Assistant Commissioner conducted a detailed analysis of the organization's purposes and accepted most of them in the particular circumstances of this case.

1) The Assistant Commissioner found that, in using GPS for the purpose of improving the dispatch process, the loss of privacy was proportional to the benefit gained and there was no less privacy-invasive way of achieving the same end.

2) The Assistant Commissioner also accepted the use of GPS for safety purposes, noting that it was reasonably effective for that purpose and that the loss of privacy was proportional to the benefit gained.

3) The Assistant Commissioner was further satisfied that using GPS for the purpose of asset protection and management was likewise appropriate under subsection 5(3) and was one for which employees had given their implied consent.

4) The Assistant Commissioner was troubled, however, by the potential that the GPS system could be used to evaluate the performance of individual employees based on inferences drawn from GPS information. The Assistant Commissioner stated that, although the GPS data could be used in certain "limited, exceptional, and defined circumstances" for employee management purposes where such purposes were clearly communicated to employees beforehand and where the organization established a policy outlining an appropriate process of warnings and progressive monitoring, GPS data should not be used as a matter of course in employee management situations. The Assistant Commissioner affirmed the importance of considering employee dignity in balancing privacy rights and the needs of organizations.

   The organization responded by developing a policy on GPS data utilization for performance management setting out clear terms and conditions, and explaining the exceptional circumstances in which GPS data may provide information and assist in addressing a productivity issue. The organization also committed to train all managers to ensure that they use GPS data appropriately and not for continual monitoring of employees. The organization further committed to inform all of its employees about the system and how it would be used, which normally, should be done *prior* to the roll-out of a particular program, not afterward. Accordingly, the Assistant Commissioner was satisfied that the use of GPS for performance management was appropriate for the limited, exceptional and defined purposes set out in the company policy and was reasonable as per subsection 5(3).

5. DATA BREACHES AND SECURITY MEASURES

High-profile data breach cases are on the rise worldwide. Hardly a day passes without a news report about a lost laptop containing personal information or a security breach that exposes personal information on the Internet.

Principle 4.7 of PIPEDA requires organizations to protect personal information using security safeguards that are appropriate to the sensitivity of the information, as well as the amount, distribution and format of the information. The more sensitive the information is, the stronger the safeguards must be. Principle 4.7.1 requires that the safeguards must "protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification."

Principle 4.7.3 recommends that organizations use the following methods of protection when designing safeguards:

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

(c) technological measures, for example, the use of passwords and encryption.

In Canada, a number of cases have helped define the nature and level of security safeguards that organizations must put in place to protect personal information under PIPEDA. These are discussed in this section.

5.1 Data security breaches

Although earlier cases provided some guidance, the precedent-setting 2007 case involving TJX, operator of Winners and HomeSense stores, offers a much more detailed analysis of security requirements in the current context.[50]

50 Report of an Investigation into the Security, Collection and Retention of Personal Information - TJX Companies Inc. /Winners Merchant International L.P. - http://www.privcom.gc.ca/cf-dc/2007/tjx_rep_070925_e.asp

In late 2006, TJX discovered suspicious software on one of its computer systems and learned that customer information had been accessed by an intruder. This information included credit card numbers and expiry dates, names, addresses, telephone numbers, drivers' licence data, and provincial identification numbers.

In early 2007, TJX advised the Commissioner that its computer systems had been breached, exposing the personal information of an estimated 45 million payment cards, including Canadian cards. TJX believed that the intruder had accessed its system via a wireless connection from outside two stores in Florida.

Before turning to the issue of safeguards, the Commissioner evaluated whether TJX had a reasonable purpose for collecting the compromised information in the first place. Payment card data, including credit card numbers and expiration dates, were necessary to complete sales transactions and therefore, were reasonable to collect. However, the Commissioner was of the view that the collection of drivers' licenses and other provincial identification data for return-of-good transactions was not necessary or reasonable in the circumstances. Consistent with earlier findings (discussed in section 7.1 of this document), the Commissioner held that TJX should only have collected individuals' names and addresses during the return process, not their drivers' licence or other information. Collection of the licence information put individuals at increased risk of identity theft and was not needed for the transaction.

The next issue that the Commissioner addressed was the issue of data retention. TJX reported that it retained drivers' licence and other identification numbers indefinitely. The Commissioner found that since TJX was not entitled to collect such information in the first place, it was not entitled to retain it. The Commissioner recommended that TJX cease collecting licence and identification information for merchandise returns, purge such information from all of its databases, clearly notify individuals as to the purpose, use and potential disclosure of the limited personal information it would collect in accordance with its new returns policy, and provide the Commissioner with copies of its new retention policies.

In response to the Commissioner's recommendations on collection and retention, TJX argued that it needed to collect drivers' licences for particular purposes but that it would in future convert the licence numbers using a cryptographic hashing function. This technique would convert the licence numbers into a unique new number referred to as a "hash value", thus rendering the drivers' licence numbers unreadable to any TJX employee. The Commissioner accepted this solution with the added requirement that the drivers' licence information be retained only temporarily.

Finally, the Commissioner turned to the issue of security safeguards. In addressing this issue, the Commissioner considered "whether TJX took 'reasonable' security precautions, whether the security risk was foreseeable, the likelihood of damage occurring, the seriousness of the harm, the cost of preventative measures, and relevant standards of practice." In determining the potential seriousness of harm in a given case, the Commissioner stated that organizations must consider the nature of the personal

information, the number of individuals that could be affected and the time elapsed before the breach is detected.

The Commissioner found that TJX had implemented physical, administrative and technical protection measures at the time of the breach. Physical measures included security personnel, photo identification, swipe cards, surveillance cameras and locks. Administrative measures included "an information-security governance structure overseen by the Chief Information Officer; an employee Code of Conduct; a limited number of security clearances and background checks carried out on employees; procedures for departing employees to return ID cards, key and swipe cards; ongoing employee training; and security policies and guidelines." Finally, TJX had some technical safeguards in place, such as encryption and remote access, in order to restrict access to its computer networks.

However, the Commissioner identified certain flaws in TJX's technical measures, particularly with respect to TJX's reliance on a weak encryption protocol and its failure to convert to a stronger encryption standard within a reasonable time. At the time of the breach in late 2006, TJX was still in the process of converting its wireless network from Wired Equivalent Privacy (WEP) encryption to a higher level of encryption – Wi-Fi Protected Access (WPA). The Commissioner noted that the use of WEP as a secure protocol had been in doubt since at least 2003, and that it was since September 2006 that Version 1.1 of the Payment Card Industry Data Security Standard mandated WPA encryption technology to reflect the new industry standard practice; by late 2006, TJX should have been adhering to this higher industry standard. The Commissioner further noted that TJX had a duty to monitor its systems and that if adequate monitoring had been in place, TJX would have learned of the breach much earlier.

Taking these factors into consideration, the Commissioner concluded that the risk of breach was foreseeable and that, in the circumstances, TJX had failed to meet Principle 4.7 of PIPEDA.

5.2 Other cases on security measures

Although the TJX case provides significant guidance for organizations considering their obligation to safeguard information, there are other case findings that provide examples of the kinds of security measures that the Commissioner considers acceptable and unacceptable under PIPEDA.

- An organization had properly safeguarded personal information where it immediately encrypted and limited access to drivers' licence numbers and driver registration forms;[51]

- If an organization receives sensitive information by fax – a practice that the Commissioner does not approve of

51 PIPEDA Case Summary #185 - Railway's reasons for collecting personal information deemed appropriate; safeguards, adequate - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030512_2_e.asp

generally – the organization should have strict safeguards in place, such as ensuring that the receiving fax machine is in a locked room accessible to a limited number of employees responsible for receiving such information;[52]

- In a settled case, an individual was concerned that her entire credit card number appeared on a restaurant receipt. Industry practice changed in this case to mask all credit card numbers on receipts;[53]

- An automated telephone system that permits individuals with only an account number to access the last five transactions against the account does not provide adequate security of the personal information contained in the transactions; [54] and

- Leaving a laptop unattended in a locked vehicle is not an adequate security measure, even if the personal information on the laptop is password-protected.[55]

Given the growing emergence of wireless technology, the Commissioner is now of the view that the minimum standard for protecting personal information on all mobile devices is no longer simple password protection; all personal information holdings must be encrypted according to well-recognized, effective and accepted industry standards.

It is important to note that PIPEDA does not currently contain provisions that require an organization to notify affected individuals that their personal information was exposed in a data security breach. The Commissioner has asked that PIPEDA be amended to include a mandatory requirement for breach notification and in the meantime, has developed Breach Notification Guidelines to help guide organizations in deciding when to notify, whether to notify, who should be notified, how and under what circumstances.

52 PIPEDA Case Summary #226 - Company's collection of medical information unnecessary; safeguards are inappropriate - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031031_e.asp. In this case, the Commissioner found that it was not appropriate for medically unqualified human resources personnel to "receive, note, interpret and process, for the purpose of administering the company's disability plans, highly sensitive medical diagnoses" of their fellow employees. See also the discussion of over-collection of health information in section 7.3 of this document. Here, the organization's collection of employees' sensitive medical information was not limited to information necessary for identified purposes. The organization told employees that they "must" submit the information to the organization; however, the organization did not explain to employees that the organization was not required to collect the information but was instead merely facilitating claims applications.

53 Settled case summary #25 - Personal information on credit card receipts to be masked by 2007 - http://www.privcom.gc.ca/ser/2006/s25_060127_e.asp

54 PIPEDA Case Summary #292 - Former employer changed account information of Air Canada frequent flyer member – http://www.privcom.gc.ca/cf-dc/2005/292_050406_e.asp

55 PIPEDA Case Summary #289 - Stolen laptop engages bank's responsibility - http://www.privcom.gc.ca/cf-dc/2005/289_050203_e.asp

Key Steps for Organizations in Responding to Privacy Breaches

August , 2007 - http://www.privcom.gc.ca/information/guide/2007/gl_070801_01_e.asp

The four key steps in responding to unauthorized access to or collection, use or disclosure of personal information are as follows:

Step 1: *Breach Containment and Preliminary Assessment*

This first step involves taking immediate common sense steps to limit the breach:

- Immediately contain the breach
- Designate an individual with appropriate scope within the organization to lead the initial investigation.
- Determine the need to assemble a team which could include representatives from appropriate parts of the business.
- Determine who needs to be made aware of the incident internally and externally.
- If the breach appears to involve theft or other criminal activity, notify the police.
- Do not compromise the ability to investigate the breach (i.e. take care not to destroy valuable evidence).

Step 2: *Evaluate the Risks Associated with the Breach*

The next step involves assessing the risks according to the following factors:

(i) Personal Information Involved

- What data elements have been breached?
- How sensitive is the information?
- What is the context of the personal information involved?
- Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?
- How can the personal information be used?

(ii) Cause and Extent of the Breach

- To the extent possible, determine the cause of the breach
- Is there a risk of ongoing breaches or further exposure of the information?
- What was the extent of the unauthorized access to or collection, use or disclosure of personal information?
- Was the information lost or was it stolen? Has it been recovered?
- What steps have already been taken to mitigate the harm?
- Is this a systemic problem or an isolated incident?

(iii) Individuals Affected by the Breach

- How many individuals' personal information is affected by the breach?
- Who is affected by the breach?

(iv) Foreseeable Harm from the Breach

- What were the reasonable privacy expectations of the individuals affected?
- Who is the recipient of the information? Are they known and can they be trusted to safely return the data without using or disclosing it?
- What harms could result to individuals and the organization as a result of the breach? What harm could come to the public as a result of notification?

Step 3: *Notification*

In determining whether to notify, when to notify, how to notify, who should notify, the content of the notification and any third party or oversight body that should be notified, organizations should consider the following:

(i) Notifying Affected Individuals

- What are the legal and contractual obligations?
- What is the risk of harm to the individual?
- Is there a reasonable risk of identity theft or fraud (usually because of the type of information lost, such as an individual's name and address together with government-issued identification numbers or date of birth)?
- Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?
- Is there a risk of humiliation or damage to the individual's reputation?
- What is the ability of the individual to avoid or mitigate possible harm?

(ii) When to Notify, How to Notify and Who Should Notify

- Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach.
- Check with authorities whether notification should be delayed to ensure that the investigation is not compromised.
- The preferred method of notification is direct, i.e. phone, letter, email or in person
- Indirect notification (i.e. website information, posted notices, media) should generally only occur where direct notification could cause further harm, is prohibitive in cost or the contact information for affected individuals is not known.
- The organization that has a direct relationship with the customer, client or employee should notify the affected individuals.
- There may be circumstances where notification by a third party is more appropriate (i.e. in the event of a breach by a retail merchant of credit card information, the credit card issuer may be involved in providing the notice since the merchant may not have the necessary contact information)

(iii) What should be Included in the Notification?

- Information about the incident and its timing in general terms.
- A description of the personal information involved in the breach.
- A general account of what the organization has done to control or reduce the harm.
- What the organization will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm.
- Sources of information designed to assist individuals in protecting against identity theft
- Providing contact information of a department or individual within the organization who can answer questions or provide further information;
- If applicable, indicate whether the organization has notified a privacy commissioner's office and that they are aware of the situation;
- Additional contact information for the individual to address any privacy concerns to the organization;
- The contact information for the appropriate privacy commissioner(s).

(iv) Others to Contact

- Privacy Commissioners;
- Police: if theft or other crime is suspected;
- Insurers or others: if required by contractual obligations;
- Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies;
- Credit card companies, financial institutions or credit reporting agencies: if their assistance is necessary for contacting individuals or assisting with mitigating harm;
- Other internal or external parties not already notified;
- Internal business units not previously advised of the privacy breach;
- Union or other employee bargaining units.

Step 4: *Prevention of Future Breaches*

Once the immediate steps are taken to mitigate the risks associated with the breach, organizations need to take the time to investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect the significance of the breach and whether it was systemic or isolated. This plan may include:

- A security audit of both physical and technical security,
- A review of policies and procedures and any changes to reflect lessons learned
- A review of employee training practices, and
- A review of service delivery partners.

Further information about privacy breaches can be found on the Commissioner's website, including a Privacy Breach Checklist for organizations published August, 2007

See http://www.privcom.gc.ca/information/guide/2007/gl_070801_01_e.asp

6. CARELESS DISCLOSURES AND NEED FOR ONGOING EMPLOYEE TRAINING

Although technical measures are an important component of security safeguards, administrative and organizational measures are equally important. In order to avoid careless or inadvertent disclosures of information, organizations must establish comprehensive security policies and procedures with an emphasis on ongoing employee training, particularly to ward against pretexting attempts.

6.1 Social engineering and pretexting

The leading pretexting case in Canada involved the "Telco Trio".[56] In 2005, Maclean's magazine reported that it had obtained records of telephone calls made by the Commissioner from her home telephone and her office Blackberry, along with similar records for a senior editor of the magazine. Macleans' purchased these records from a U.S. company called Locatecell.com.

In the course of the investigation, the Assistant Commissioner determined that Locatecell.com had illegitimately obtained the information from Canadian telecommunications companies – Bell, TELUS Mobility and Fido – through "social engineering," including "pretexting". In other words, Locatecell.com deceived employees of the Canadian telecommunications companies into revealing customers' personal information. This was not a case of a rogue employee or a case of hacking into computer systems such as occurred in the TJX case.

The Assistant Commissioner concluded that the employees at the Canadian telecommunications companies did not follow customer authentication procedures in place at the companies. Yet, the Assistant Commissioner also found that the authentication procedures themselves and the training of employees were inadequate and failed to sufficiently safeguard customers' personal information. The companies each agreed to follow the Assistant Commissioner's recommendations that they provide their employees with additional training (including information about social engineering tactics), that they limit the amount of personal information given out to callers over the

56 PIPEDA Case Summary #372 - Disclosures to data brokers expose weaknesses in telecoms' safeguards - http://www.privcom.gc.ca/cf-dc/2007/372_20070709_e.asp

phone, and that they improve authentication procedures consistent with the identification and authentication guidance issued by the Office of the Privacy Commissioner.

OPC Guidelines for Identification and Authentication

October 2006 - http://www.privcom.gc.ca/information/guide/auth_061013_e.asp

The OPC developed the following guidelines to help organizations develop appropriate identification and authentication processes:

- *Authenticate when Necessary*

An individual's identity should be authenticated by an organization when it is necessary given the nature of the transaction.

- *Level of Authentication Commensurate with the Risk*

The stringency of authentication processes should be commensurate with the risk to the information being protected, risk being a function of the sensitivity of the information or service in question, the vulnerability of and the perceived threat to that information or service. The level of authentication and the methods of authentication may also vary depending on the nature of the interaction with the customer.

- *Responding to Changing Threats*

Organizations should regularly reassess risks and threats for each service delivery "touch point" and deploy risk mitigation measures, including adjusting the strength of authentication processes, to address changing threats. Organizations need to further ensure that the authentication processes in place are sufficiently strong to mitigate the potential additional risk of any newly added service.

- *Regularly Monitor Threats*

Organizations should regularly measure attempted attacks, breakdowns, and losses as part of a structured threat- and risk-assessment program, and evaluate customer awareness of and confidence in the authentication processes in place.

- *Employee Training*

Organizations should ensure that employees who have access to personal information receive appropriate training on the importance of protecting customers' personal information, including the importance of protecting it from unauthorized access and disclosure.

- *The Role of Individuals*

Individuals have a role to play in the protection of their personal information by questioning and avoiding the use of weak authentication processes, choosing strong authenticators and responsibly and continuously safeguarding their identifiers and authenticators.

- *Changing Authentication Information*

Organizations should give individuals the option of periodically changing their identifiers and personally selected authenticators.

- *Individual Choice*

Individuals should be provided with choices and identification/authentication options in order to manage their personal identity and privacy risks, and organizations should provide enhanced authentication processes to individuals who request them.

- *Easy to Remember, Difficult to Guess*

Where the individual chooses an authentication factor that is based on something that the individual knows, it should be easy to remember or disguise, but difficult for someone else to guess or disclose. Individuals who feel they must keep a record of their passwords should be encouraged to store them securely, for example in an encrypted computer file.

- *Personal Identity Facts*

Ideally, authentication should not be based on personal identity facts or other information and identifiers that individuals acquire during their lifetime that are not easily or often changed.

- *Authentication "Tokens"*

"Tokens" (for example, identity cards, drivers' licences, passports, etc.) should only be used for their original intended purpose. In other situations, an organization should only rely on a token when it has some assurance of the integrity of the issuance process.

- *Integrity of Authentication Processes*

Authentication processes should include effective safeguards to ensure the confidentiality and integrity of authentication information while being validated and stored.

- *Audit Logs*

The authentication process should maintain reliable audit records of authentication transactions including the date, time and the outcome/result. The level of detail in the audit logs should reflect the risks associated with the information or service.

- *"Outsourcing"*

In a situation in which an organization outsources a customer service function to a third party, primary responsibility for ensuring the adequacy of the identification and authentication processes that are used remain with the servicing organization that the individual has chosen. Even though the actual authentication may be done by the third party outsourcer, the organization remains accountable for ensuring that the authentication processes meet its requirements and reliably protect their customers' information and assets.

6.2 Careless errors

Quite apart from deliberate attempts by sophisticated third-party fraudsters or hackers, there are unfortunately still many cases of unauthorized disclosures by company employees that happen through carelessness or as a result of lack of training.[57] Several important complaint and incident investigations provide insightful guidance on the proper use of safeguards and the need for employee training.

57 *Richard Breithaupt and Peggy Fournier v. Hali MacFarland and Calm Air International Ltd.* (Federal Court No. T-2061-04) involved an alleged disclosure of itinerary information from an airline employee to an RCMP officer. This case was settled through mediation with the Commissioner in 2005.

In the first three incident reports under PIPEDA, the Commissioner found that PIPEDA was violated after personal information was transmitted by fax to incorrect fax numbers. In one case, health information was mistakenly faxed to an apartment manager.[58] In other cases, banking information was inadvertently faxed to businesses and individuals in Montreal, Dorval and the United States over a period of years.[59] Misdirected fax cases continue to arise under PIPEDA.[60] Misdirected email cases have also arisen.[61] Such types of careless errors are a subject of significant concern.

Misappropriate disposal of personal information is likewise troublesome. The Assistant Commissioner has found that disposing of sensitive personal banking information in a recycling bin is a violation of PIPEDA.[62] In this case, the complainant learned that his personal banking information – including the complainant's and his wife's names, address, social insurance numbers, account number and transaction history – was found by a third party in an unattended recycling bin in a parking garage. The bank determined that two of its employees had inadvertently put the information in a recycling bin rather than in a shredding bin when cleaning out the desk of a former employee. In addition to finding that the organization had violated PIPEDA's safeguards provision, the Assistant Commissioner was troubled by the fact that the information had been left in the desk of the former employee for a year. The Assistant Commissioner stated that such information should be shredded as part of a systematic approach to dealing with any confidential information in the custody of a departing employee.

There are a number of additional cases that, taken together, provide useful guidance regarding the requirements of PIPEDA in connection with inadvertent disclosures and employee training. Briefly, these cases can be summarized into the following principles. Although some of these principles arise in unique circumstances, the rules developed in the cases have general application:

- It is not acceptable for staff to handle payroll information of their fellow employees when the staff have not signed a confidentiality agreement or received any training and there is no other appropriate safeguard in place;[63]

58 Incident Summary #1 - Misdirected faxes containing health information end up in apartment managers' hands - http://www.privcom.gc.ca/incidents/2004/041221_e.asp

59 Incident Summary #2 - CIBC's privacy practices failed in cases of misdirected faxes - http://www.privcom.gc.ca/incidents/2005/050418_01_e.asp; Incident Summary #3 - Misdirected faxes - http://www.privcom.gc.ca/incidents/2006/003_061204_e.asp

60 PIPEDA Case Summary #332 - Bank issues new guidelines and educates employees after customer information is faxed to the wrong individual - http://www.privcom.gc.ca/cf-dc/2006/332_20060412_e.asp

61 PIPEDA Case Summary #360 - Bank erroneously e-mails employees' personal information to client - http://www.privcom.gc.ca/cf-dc/2006/360_20061114_e.asp

62 PIPEDA Case Summary #356 - Customer's banking personal information found in a recycling bin - http://www.privcom.gc.ca/cf-dc/2006/356_20061023_e.asp

63 PIPEDA Case Summary #242 - Individual objects to temporarily assigned workers handling payroll information - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031204_06_e.asp

- Failing to educate employees about the importance of maintaining confidentiality can itself be a violation of PIPEDA;[64]

- Use of a single measure – a number recorded on a signature card – to authenticate the owner of a safety deposit box is an insufficient safeguard when it results in a customer's safety deposit box being opened by another customer in error;[65]

- Disclosing financial information to an individual's fiancé directly and by leaving a file visibly open on a desk at a bank is a violation of PIPEDA if done without ensuring that the fiancé had proper written authority to act on behalf of the individual in dealings with the bank;[66]

- Disclosing information about an individual's overdue account to the person who referred the individual to the organization, but has no authority to act on behalf of the individual, would be a violation of PIPEDA;[67]

- Using an automated system to leave a message on an answering machine for an individual about an overdue credit card payment (without their permission), though potentially useful information for the individual, is a violation of PIPEDA because the message can be heard by anyone with access to the answering machine;[68] and

- Inadvertently sending sensitive financial information in an unsealed envelope is a violation of PIPEDA's safeguards provisions.[69]

As demonstrated by the key cases discussed in this section, employees of an organization can make careless mistakes resulting in unauthorized disclosure of personal information.

64 PIPEDA Case Summary #54 - Couple alleges improper disclosure of telephone records to a third party - http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020628_2_e.asp

65 PIPEDA Case Summary #344 - Couple's safety deposit box opened in error – http://www.privcom.gc.ca/cf-dc/2006/344_20060717_e.asp

66 PIPEDA Case Summary #200 - Bank disclosure results in cancelled wedding - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030806_01_e.asp

67 Settled case summary #27 – (Dental) Clinic discloses client information when trying to collect a debt - http://www.privcom.gc.ca/ser/2006/s27_060516_e.asp

68 PIPEDA Case Summary #270 - Bank agrees to modify automated message - http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040504_e.asp

69 PIPEDA Case Summary #154 - Couple dismayed at receiving unsealed envelope from bank - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030415_1_e.asp

These mistakes can be just as harmful to an organization and the affected individuals as intentional attacks or technical data security breaches can be.

Organizations must address the human element of their operations and ensure that their employees are not the weakest link in an overall security system. Proper policies, procedures and training are key elements in a security program. Employees must be trained about the proper collection, use and disclosure of personal information not only at the time that they are hired, but also on an ongoing basis. Ongoing employee training is an essential component of ensuring that personal information is effectively safeguarded.

7. COLLECTING TOO MUCH INFORMATION

Subject to certain exceptions outlined in section 7 of PIPEDA, Principle 4.3 requires organizations to obtain consent for the collection, use and disclosure of personal information. Principle 4.4 requires organizations to limit the personal information they collect to that which is necessary for the purposes identified by the organization. Principle 4.4.1 prohibits the indiscriminate collection of personal information.

A number of leading cases have helped define the quantity and character of personal information that may be collected in different situations.

7.1 Product returns and credit card usage

In the retail sector, many organizations require customers to supply forms of identifying information if they wish to return or exchange a product. This information is generally collected for the purpose of preventing fraud and error. In a leading case addressing the collection of photo identification in the product return and exchange context, the Retail Council of Canada put forward several examples of how collecting customers' personal information helped combat theft and fraud: :

- Reduction of theft by employees. Employees can no longer claim that an item had been returned for refund by an unknown person. Information about the customer is now available so stores can verify the return.

- Identification of multiple returns made by the same person or by persons who have different names but are connected with the same address or telephone number.

- Identification of buying patterns. For example, people may buy an item and then use half of it. They then return the unused portion and claim the item is defective or was not full upon purchase.

- Reduction of "receipt theft." This is the theft of items listed on receipts that people find outside a store or in a mall.[70]

At issue in this case was whether the collection of photo identification was reasonable for the purpose of combating retail fraud and whether individuals had knowledge of, and given meaningful consent to, the collection.[71]

In addressing the issue of reasonableness, the Assistant Commissioner noted that the loss of privacy was minimal because the photo identification information, though asked for, was not actually recorded by the store. Faced with a lack of alternative means to achieve the same end of preventing fraud, the Assistant Commissioner concluded that the purpose for requesting the showing of photo identification was reasonable in the circumstances. In stores where production of photo identification is made a condition of a product return or exchange, the store must explicitly state the purpose under Principle 4.3.3.

Although the store in this case stated in a number of places that photo identification was required for refunds and exchanges, the Assistant Commissioner found that the store had not explained why the photo identification was necessary for this purpose. Accordingly, the Assistant Commissioner found that the store was not obtaining meaningful consent with the individuals' knowledge as required by PIPEDA. The Commissioner recommended that the store explain in its return policy why collection of photo identification and other personal information is required for both product returns and exchanges in order to prevent fraud.

Fact Sheet: Photo Identification Guidance

September 2007 - http://www.privcom.gc.ca/fs-fi/02_05_d_34_tips_e.asp

Together with the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner of British Columbia, the Commissioner issued a Fact Sheet in September 2007 to address the use of photo identification in connection with the use of a credit card to purchase goods.

The commissioners accept that organizations may require photo identification when customers wish to make purchases by credit card. However, the commissioners make clear that "[the] collection of personal information must be limited to examination of identification only and must not involve recording of personal information from the identification offered, including driver's licence numbers or addresses." This limitation is designed to balance privacy rights against the need of organizations to prevent credit card fraud.

70 PIPEDA Case Summary #361 - Retailer requires photo identification to exchange an item - http://www.privcom.gc.ca/cf-dc/2006/361_20061114_e.asp

71 The store also collected the complainant's name, address and phone number. Although the complainant was not concerned about this collection, the Commissioner nevertheless considered it and found that it was reasonable in the circumstances. This information involved a minimal loss of privacy.

7.2 Opening accounts and related activities

In the context of opening an account and related application-type activities, a number of cases have drawn parameters around what information is and is not necessary to be collected for different purposes. Briefly, below are the principles that have emerged from key cases:

- A Notice of Assessment is not needed for income verification purposes in connection with securing a line of credit or obtaining additional credit as it contains additional information that not required for the purpose of verifying income;[72]

- A record of a drivers' licence or other identification information should not be recorded by a DVD-rental store for the purpose of opening an account with the store;[73]

- A Social Insurance Number is not required when signing an apartment lease,[74] or when signing up for an Internet connection;[75] and,

- For the purpose of processing an insurance claim for the theft of personal property, an individual cannot be required to disclose information about his credit history, financial information, medical information, driver's record, and employment information. This information is not necessary for the purpose of processing this type of claim.[76]

7.3 Collection of health information

In a series of employment cases involving the collection of medical information, the Commissioner and the Assistant Commissioner have helped define how much personal information organizations need to collect in order to administer benefit plans, grant sick leaves, and manage other activities.

72 PIPEDA Case Summary #169 - Individual objects to bank's requirement to provide Notice of Assessment for income verification purposes - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030424_2_e.asp

73 Settled case summary #28 - DVD-rental store revises membership application process - http://www.privcom.gc.ca/ser/2006/s28_061214_e.asp

74 Settled case summary #19 - SIN not required when signing apartment lease - http://www.privcom.gc.ca/ser/2006/s19_060203_e.asp

75 PIPEDA Case Summary #22 - Company asks for customer's SIN as a matter of policy - http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011105_02_e.asp

76 PIPEDA Case Summary #368 - Insurance adjusters' consent form considered overly broad – http://www.privcom.gc.ca/cf-dc/2007/368_20070111_e.asp

In one case, the Commissioner found that organizations are permitted to require a medical certificate for an extended sick leave. However, the individual cannot be required to submit diagnostic information about their condition or illness to their employer – the note of the doctor should be considered sufficient.[77]

In a similar case, the Commissioner found that collecting details about the nature of an employee's illness was abusive inasmuch as it was not necessary – the Commissioner concluded that a statement by the employee's doctor on the medical certificate was sufficient to confirm that an absence from work was justified.[78]

However, the Commissioner has also found that organizations may request information about an employee's expected date of return to work so that the organization can plan accordingly (provided that the request is clearly worded to state that the organization is seeking a prognosis and not a diagnosis).[79]

The Assistant Commissioner has elsewhere found that, without the consent of the employee, an organization's occupational health and safety advisor is not permitted to contact a hospital where an employee had a medical exam in order to ask for information about the exam.[80]

77 PIPEDA Case Summary #257 - Employees objected to corporation's requirement for medical diagnosis on sick leave certificates - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031009_01_e.asp

78 PIPEDA Case Summary #233 - An individual challenged the requirement to provide the medical diagnosis on her doctor's certificate for sick leave - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031003_e.asp

79 PIPEDA Case Summary #135 - Individual alleged that employer asked for too much medical information - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030306_4_e.asp

80 PIPEDA Case Summary #235 - Individual challenges employer's refusal to grant sick leave - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031107_03_e.asp

8. MEANINGFUL ACCESS TO PERSONAL INFORMATION

Subject to certain exceptions identified in section 9 of PIPEDA, Principle 4.9 requires organizations to provide individuals with access to their personal information upon request. Organizations must specifically inform individuals of the "existence, use and disclosure" of their personal information.

Section 8 of the Act requires that access be granted not later than 30 days after the request is made. Section 8 permits organizations to respond to access request at a cost, provided that the individual is informed of the approximate cost and does not withdraw the request. However, Principle 4.9.4 further stipulates that access shall be provided at "minimal or no cost" to the individual. Several cases have resolved important questions regarding individuals' right to access their personal information, including those that arise in the context of parallel litigation proceedings and charging fees for access.

8.1 General principles of access

In a case involving an access request made to a lawyer at a law firm, the Assistant Commissioner held that organizations must establish practices and procedures for handling access requests as part of an overall privacy program.[81] The lawyer in this case simply refused to provide any information to the individual but did not cite any provision in PIPEDA that justified the refusal. The lawyer did not forward the access request to the firm's Chief Privacy Officer. In response to the Assistant Commissioner's intervention, the firm notified its staff that all requests for access to personal information should be forwarded to the Chief Privacy Officer for response. The Assistant Commissioner approved of this measure and reasoned that it would help ensure that, in the future, the law firm respond to personal information access requests in accordance with its obligations under Principle 4.9.

In another case, the Federal Court held that PIPEDA does not guarantee that individuals can access their personal information in a particular form.[82] If information in a document is retained in a format other than how it was initially collected, then providing access

81 PIPEDA Case Summary #367 - Need to establish procedures for handling access to personal information requests stressed - http://www.privcom.gc.ca/cf-dc/2007/367_20070119_e.asp

82 *Vanderbeke v. Royal Bank of Canada*, 2006 FC 651 (CanLII) - http://www.canlii.org/en/ca/fct/doc/2006/2006fc651/2006fc651.html.

to the alternative form of information is sufficient to meet the access obligation under PIPEDA.

8.2 The impact of parallel litigation proceedings

PIPEDA case findings clearly start from the position that an individual's right of access is a fundamental right, untempered by an individual's motive for seeking access. This is so, even in cases where the individual seeks access to documents under PIPEDA that may be relevant in parallel litigation proceedings. Some organizations have refused access on the grounds that an individual should not be permitted to obtain, through PIPEDA, documents that they should rather seek to obtain through the normal rules of discovery under civil procedure. In several cases, the Commissioner has found that the mere existence of parallel civil litigation proceedings between the parties does not displace the operation of PIPEDA. Notwithstanding ongoing litigation, organizations must continue to receive and handle access to personal information requests as per their obligations under the Act. Litigation proceedings should not automatically preclude consideration of an individual's stand alone right of access to his or her personal information under PIPEDA. Nor should traditional rules of evidence, such as the rule of relevance and the rule against fishing in the context of litigation, limit the scope of personal information to which individuals are independently entitled to access under PIPEDA. Unless the documents requested are subject to an applicable exception, organizations must provide access to these documents under PIPEDA. Such exceptions include solicitor-client privilege under paragraph 9(3)(a)[83], confidential commercial information under paragraph 9(3)(b) or information generated in the course of a formal dispute resolution process under paragraph 9(3)(d).

In a leading case involving access and litigation, an airline initially refused to provide an individual with access to his personal information pursuant to his request under PIPEDA.[84] The airline did not treat the access request as per the requirements under the Act, but handled it instead as part of the ongoing litigation proceedings between the parties. The airline took the position that, when litigation commences, there are well-defined evidentiary rules and procedures that govern the discovery of documents and that PIPEDA was not intended to have application so as to override those rules. In an important finding that resolves part of the inconsistency that can arise between litigation discovery and PIPEDA, the Assistant Commissioner found that PIPEDA continues to apply notwithstanding parallel civil litigation proceedings and that *all* access requests must be considered in their own right, subject to applicable exceptions under the Act.

83 For the purposes of interpreting and applying PIPEDA, the term "solicitor-client privilege" has been taken to include both legal advice privilege and litigation privilege: See *Blank v. Canada (Minister of Justice),* 2006 SCC 39, as applied in *Rousseau v. Wyndowe*, 2006 FC 1312 (Canlii) at para. 34, appealed on different grounds.

84 PIPEDA Case Summary #352 - Airline delays granting access to personal information, citing ongoing litigation - http://www.privcom.gc.ca/cf-dc/2006/352_20060908_e.asp See also an earlier case which stands for the same proposition in the context of litigation proceedings between a former employee and his former employer: PIPEDA Case Summary #285 - Company refuses former employee's request for access - http://www.privcom.gc.ca/cf-dc/2004/cf-dc_041221_01_e.asp

The Assistant Commissioner found the airline in violation of PIPEDA for failing to consider and manage the access request under the rules of PIPEDA and provide timely access as required by the Act, subject to any lawful exceptions that may apply in the particular circumstances.

In another case, a medical examiner was hired by an insurance company to conduct an independent medical examination of an individual.[85] The medical examiner refused to provide the individual with access to his examination notes, which included personal information about the individual which he recorded during the examination. The medical examiner claimed that his examination notes were exempt from access as information protected by solicitor-client privilege under paragraph 9(3)(a) or as information generated in the context of a formal dispute resolution process under paragraph 9(3)(d). The Assistant Commissioner rejected both of these claimed exceptions. The Assistant Commissioner noted that, in the circumstances of the complaint, the medical examiner had been retained by the insurance company as an expert simply for the purpose of assessing a claim of eligibility for benefits under a group insurance policy. As there was no contestation yet between the parties, the examination was not carried out in the context of litigation or even anticipated litigation. Similarly, an independent medical examination carried out for the routine purpose of assessing and processing claims cannot be said to have been done in the course of a formal dispute resolution process.

The Assistant Commissioner's findings were upheld by the Federal Court.[86] The Court indicated that in order for the litigation privilege exception to apply for the purpose of refusing an access to personal information request under PIPEDA, paragraph 9(3)(a)) requires that (1) there is a reasonable prospect of litigation at the time of the communication, and (2) that litigation was the dominant purpose for the creation of the communication. In this case, the Court held that the dominant purpose of the independent medical examination was not litigation, but rather to determine whether the complainant was entitled to disability benefits.

Similarly, the Court held that there was no evidence to suggest that an independent medical examination requisitioned by an insurer is an ongoing dispute resolution process. On the contrary, the Court noted that submitting to a medical examination was a standard part of the insurance contract. In the subsequent letter which the insurer sent Mr. Rousseau informing him or its decision to terminate his benefits, it indicated that the decision could be appealed. It was therefore open to Mr. Rousseau to initiate a formal dispute resolution process at that point, by choosing to appeal the decision. However, such a process could only be initiated after having received the insurer's decision, which in turn, could only be made after having received the independent medical examination.

85 PIPEDA Case Summary #306 - Physician refuses to provide access to individual's personal information - http://www.privcom.gc.ca/cf-dc/2005/306_20050317_e.asp

86 *Rousseau v. Wyndowe*, 2006 FC 1312 (CanLII) – appealed and upheld on different grounds – http://www.canlii.org/en/ca/fct/doc/2006/2006fc1312/2006fc1312.html

8.3 Fees for access

Several precedent-setting cases have provided much-needed guidance on the issue of charging fees for access to personal information. Although section 8 of PIPEDA permits an organization to provide access at a cost, Principle 4.9.4 mandates that access shall be provided at minimal or no cost. PIPEDA does not specify either what those fees should be or on what basis fees can be calculated.

In one case, an individual complaint was brought against an organization that had indicated it would cost the individual $1500 to respond to an access request under the Act since the request was sweeping, virtually requiring a "forensic audit".[87] The Assistant Commissioner rejected this fee outright, noting that PIPEDA requires access be granted at "minimal or no cost to the individual." In the Assistant Commissioner's view, the language of PIPEDA implied that the fee should be a token amount; $1500 was clearly not a token amount.

In another case, an individual brought a complaint against a bank for charging a standard $25 flat fee for any access to personal information request.[88] The Assistant Commissioner did not approve of the bank's practice and held that flat fees for access contradict the spirit of the Act. The Assistant Commissioner made clear that organizations should only consider charging fees in exceptional cases, and even then, at minimal cost. The bank's objective of deterring access requests was found to be an illegitimate objective of a fee-for-access policy.

Recognizing that providing copies of records containing personal information can involve costs for organizations, the Assistant Commissioner issued another finding which suggests ways organizations can mitigate costs while at the same time satisfying the obligation to provide access.[89] In this case, an organization wished to charge an individual a $20 fee to retrieve their file from a third-party storage company, as well as $0.20 per page for photocopying. Since there were over 1000 pages to be copied, the organization's total fee for access was $225. For starters, the Assistant Commissioner rejected the standard fee for retrieving one's file from storage. File storage is the responsibility of the organization and as a normal cost of doing business, it should not be transferred onto individuals. Although the Assistant Commissioner was prepared to find a $0.20 per page fee for copying as being reasonable in the circumstances, she urged the organization to permit less costly alternatives for providing access. Providing access to personal information under PIPEDA does not necessarily mean providing copies of documents. For example, the organization could provide individuals with an opportunity to view their file on site in order to obtain the information they seek, or in order to determine with

87 PIPEDA Case Summary #285 - Company refuses former employee's request for access - http://www.privcom.gc.ca/cf-dc/2004/cf-dc_041221_01_e.asp

88 PIPEDA Case Summary #283 - A bank charged fees to process requests for personal information - http://www.privcom.gc.ca/cf-dc/2004/cf-dc_041021_02_e.asp

89 PIPEDA Case Summary #354 - Fees for access questioned - http://www.privcom.gc.ca/cf-dc/2006/354_20061025_e.asp

greater precision which specific documents they would like to obtain a copy of. The $0.20 per page photocopying fee would then apply only for those specific copies requested and made.

Another interesting case involved a third party medical records storage company that provides secure storage for physicians who retire or move out of province, but who are required by their professional regulatory body to maintain their patient files a minimum number of years.[90] The Assistant Commissioner found that the storage company's practice of charging fees for access which correspond to the recommended fee structure set out by the Ontario Medical Association was reasonable, although, as above, the Assistant Commissioner urged the company to provide less costly alternatives for access. The medical records company agreed to modify its privacy policy to permit patients to view their files in-person on site at no cost, and to only charge for actual photocopies made or for transferring the file to a new physician. On this basis, the Assistant Commissioner found that the complaint regarding fees for access was resolved.[91]

90 PIPEDA Case Summary #328 - Medical records storage company revises its access policy - http://www.privcom.gc.ca/cf-dc/2006/328_20060609_e.asp.

91 The complaint was primarily about access, although it raised a number of other important policy issues which the Assistant Commissioner referred to in her findings.

9. SECONDARY MARKETING PURPOSES

Organizations sometimes collect individuals' personal information for the purpose of providing the primary service contracted for but wish to use or disclose the information for secondary marketing purposes. Secondary marketing can be extremely profitable from the point of view of the organization, but which may --or may not -- always be desirable from the point of view of potential customers. Some organizations engage in secondary marketing directly; others disclose information to third parties who use the information for secondary marketing purposes.

Secondary marketing can raise a number of personal information issues under PIPEDA, including consideration of opt-in vs. opt-out consent, the reasonable expectations of the individual (Principle 4.3.5), conditioning the supply of a service on overbroad consent (Principle 4.3.3), the adequacy of knowledge and consent generally (Principles 4.3 and 4.3.2), the timing of identifying purposes (Principles 4.2.3 and 4.3.1), the right to withdraw consent (Principle 4.3.8) and the appropriateness of marketing purposes (subsection 5(3)).

Since the coming into force of PIPEDA, several important cases have arisen regarding organizations' use of customers' personal information for secondary marketing purposes. The Commissioner has rendered relevant findings in a number of different industries taking into account the reality of each sector, including telecommunications, retail, banking and airlines. These findings can serve as helpful guidance for organizations as they consider further uses of the personal information they collect.

9.1 Telecommunications

The case of *Englander v. TELUS*[92] involved, among other things, the issue of consent for secondary purposes of personal listing information by first-time TELUS customers. The Federal Court of Appeal held that, in the circumstances, proper consent was not, and could not have been given, by first-time customers with respect to the variety of secondary

92 Englander v. TELUS Communications Inc., 2004 FCA 387 (CanLII), (2004), 247 D.L.R. (4th) 275 • (2004), 1 B.L.R. (4th) 119 • (2004), 36 C.P.R. (4th) 385 - http://www.canlii.org/en/ca/fca/doc/2004/2004fca387/2004fca387.html

uses[93] to which TELUS put their telephone listing information. These secondary purposes were not identified at the time of customer enrolment and there was no evidence that these secondary purposes were so connected with the primary purpose of creating public telephone directories that a new customer would reasonably consider them as being appropriate. The Court was of the view that TELUS had not made any "effort," let alone any "reasonable" effort within the meaning of Principle 4.3.2, to ensure that first-time customers were advised of any secondary purposes for the use of their personal listing information at the time of collection.

Once individuals are properly informed of potential secondary uses, the question then turns on what form of consent will be appropriate for the purposes of the Act. There are cases where opt-out consent may be appropriate for secondary marketing purposes subject to the following conditions:

> The personal information must be clearly non-sensitive in nature and context.
>
> The information-sharing situation must be limited and well-defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure.
>
> The organization's purposes must be limited and well-defined, stated in a reasonably clear and understandable manner, and brought to the individual's attention at the time the personal information is collected.
>
> The organization must establish a convenient procedure for easily, inexpensively, and immediately opting out of, or withdrawing consent to, secondary purposes and must notify the individual of this procedure at the time the personal information is collected.[94]

For example, the choice of opt-out consent was upheld in a case where a telecommunications company included an insert in customers' monthly bills that described the organization's privacy practices in respect of secondary marketing and provided customers with a variety of straightforward ways to opt out.[95] The organization permitted individuals to opt-out through a toll-free number, e-mail, or on the organization's website. The telecommunications company indicated that, in addition to the monthly insert, it would provide individuals with the ability to opt-out at the time that they activate their phone. The Commissioner considered this an exemplary use of opt-out consent.

93 *Ibid.* at paragraph 65. Namely, its Internet directory assistance service, in its directory file service and basic listing interchange file service and its CD-ROM service.

94 PIPEDA Case Summary #192 - Bank does not obtain the meaningful consent of customers for disclosure of personal information - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030723_01_e.asp

95 PIPEDA Case Summary #207 - Cell phone company meets conditions for "opt-out" consent - http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030806_02_e.asp

9.2 Banking

On the issue of opt-out consent for secondary marketing purposes, an opposite result was reached in a case where the Assistant Commissioner found that a bank provided no means of opting out of receiving marketing materials in a monthly credit card bill.[96] In this case, the bank refused to permit an individual to opt-out of receiving 'statement stuffers' – advertisements for products and services – with his credit card statements. Although the bank agreed to cease telemarketing and direct marketing to the complainant, the bank claimed that to cease the 'statement stuffers' would require it to manually intercept the complainant's bill out of a master production run. The bank argued that this was unreasonable and that it was not using the complainant's personal information in any event since the 'stuffers' were placed into every envelope.

The Assistant Commissioner disagreed with the bank, finding that the bank was using the complainant's personal information when it inserted advertising into the envelope with the complainant's credit card statement. This use was secondary to the purpose for which the complainant had initially given his consent, namely to receive a credit card. Finally, the Assistant Commissioner concluded that individuals must always have the right to opt-out of secondary marketing and that to refuse to do so was a violation of Principles 4.3.3 and 4.3.8 of PIPEDA because the bank was requiring consent to purposes beyond that to fulfill servicing the complainant's credit card account and refusing to permit a withdrawal of consent.

In a similar case, the Assistant Commissioner expressed concern regarding the common banking industry marketing practice of issuing unsolicited convenience cheques to credit cardholders that contain their personal information, including name, address and account number.[97] These convenience cheques were enclosed with customers' monthly statements and were mailed to customers as part of various promotions or at a customer's request. In this case, a customer's mail was stolen and a convenience cheque that was contained in the mail was fraudulently cashed for $900. In the wake of the finding the Assistant Commissioner issued Further Considerations, recommending that the bank cease sending unsolicited convenience cheques to its customers as enclosures to their monthly statements and instead consider informing customers about how they could order such cheques separately should they wish. Citing increased costs, the bank advised that it could not introduce a separate marketing mechanism for ordering convenience cheques; however, it did agree to implement opt-out options and to improve convenience cheque security.

96 PIPEDA Case Summary #308 - Opting-out of marketing inserts in account statement - http://www.privcom.gc.ca/cf-dc/2005/308_20050407_e.asp

97 PIPEDA Case Summary #299 - Thief cashes convenience cheque on cancelled credit card account - http://www.privcom.gc.ca/cf-dc/2005/299_050331_03_e.asp#update. See the Update statement at the conclusion of this case summary.

In another leading case, the Commissioner addressed the privacy practices of a bank that used and disclosed personal information for secondary marketing purposes in connection with information in its customers' credit card accounts.[98] The Commissioner found that:

- the credit card application form requested consent in tiny lettering on the reverse side of the form;
- the credit card agreement referred broadly to the organizations to which the bank disclosed information;
- the online credit card application contained no link to the credit card agreement and no reference to disclosure to third parties;
- credit card applications made by telephone included a request for a very broad consent;
- the bank's privacy policy is more detailed but it was not provided as a matter of course – customers had to request a copy or visit the bank's website; and
- on the credit card application and the agreement, customers were informed that they could opt out of secondary marketing by writing to the bank.

The bank argued that the foregoing efforts formed a sufficient basis for knowledge and consent under PIPEDA; the Commissioner disagreed. The Commissioner concluded that the bank had not made reasonable efforts to inform individuals of the purposes for which information would be used or disclosed. Individuals could not reasonably understand what they were being asked to consent to because, among other things, the bank did not provide sufficient information for individuals to use as a reference in deciding whether to give consent, the bank had used overly broad wording and in one case the bank used "legalistic" wording and "miniscule lettering". Nor did the bank adequately explain that some services would be provided by third parties to which it would disclose customers' personal information.

The Commissioner held that the bank was in violation of virtually every aspect of consent (Principles 4.3, 4.3.2, 4.3.3) and that its purposes were not appropriate in the circumstances.[99] On the issue of opting-out, the bank's failure to provide a "convenient, immediate, and easy means of withdrawing consent" to secondary marketing purposes

98 PIPEDA Case Summary #83 - Alleged disclosure of personal information without consent for secondary marketing purposes by a bank - http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021016_1_e.asp

99 Similar shortcomings led to a similar finding against a marketing firm in connection with its disclosure, for marketing purposes, of information it collected during consumer product surveys. PIPEDA Case Summary #91 - Marketing firm accused of improper disclosure of survey information - http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021122_e.asp

did not meet the reasonable expectations of the individual and thus contravened Principle 4.3.5.

9.3 Retail

In a case involving Ticketmaster (a US company whose main commercial activity includes selling tickets on behalf of venues, concert promoters, and sports teams and leagues for events held in Canada), an individual complained that Ticketmaster was using personal information it collected for marketing purposes by third parties and that customers were not properly informed of this practice nor provided a viable alternative if they wished not to share their information. The complainant alleged that the policies and practices of the company with regard to the collection, disclosure and use of customers' personal information did not respect the principles of openness (Principle 4.8 and 4.8.1), access (Principles 4.1.4, 4.5, 4.9 and 4.9.3), accountability (Principle 4.1.3) and consent (Principles 4.3, 4.3.2 and 4.3.3) of Schedule 1 of PIPEDA.

The Assistant Commissioner determined that, although Ticketmaster had a privacy policy in place, it was long and complex and therefore failed to meet the requirement of openness. As well, the Assistant Commissioner deemed the complaint regarding consent as well-founded and resolved. Although Ticketmaster's purposes in collecting customers' personal information to process ticket payments, to deliver tickets, to notify customers of cancellations or postponements, to verify customer identity when tickets are picked up, and to replace lost tickets were reasonable, it was not reasonable for personal information to be used for marketing purposes without customer consent. As marketing is a secondary use, fully informed customer consent or an opportunity to opt out without being penalized was required. Furthermore, TM's original policy was not specific about whether event providers used customer information for marketing purposes, and, if so, how they used it.

In another case, the Commissioner considered a complaint against an organization that was sharing individuals' personal information with its affiliates across provincial borders for consideration for secondary marketing purposes.[100] This case involved a 'frequent buyer' program under which individuals earned points when purchasing products from the sponsors of the program. The organization shared individuals' personal information with these sponsors for marketing purposes. Individuals could sign up for the 'frequent buyer' program in person by filling out a form, over the telephone, or online.

The Commissioner reviewed the organization's privacy-related documents and concluded that the organization offered a 'privacy pledge' for individuals signing up in person or online. This pledge met the requirements of PIPEDA because it clearly identified the purposes for which the organization collected, used and disclosed personal information, including secondary marketing. Individuals were offered the ability to withdraw consent to marketing purposes in writing. Individuals enrolling in the frequent buyer program

100 PIPEDA Case Summary #78 - Alleged disclosure of personal information without consent for secondary marketing by a company - http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021016_6_e.asp

over the telephone, however, were not offered the same level of information about the organization's privacy practices – specifically, they were not told that the marketing purposes were optional, nor were they given the option to withdraw consent to any of the purposes.

The Commissioner concluded that, with the exception of the telephone applications, the organization had made a reasonable effort to ensure that individuals were aware of secondary marketing purposes and disclosures. As such, their consent for such purposes was valid. However, by requiring individuals to opt-out of marketing purposes in writing, the organization had failed to provide a convenient and immediate means of opting out – the organization should provide a toll-free number for opting out.

9.4 Airlines

In an early case involving Air Canada and Aeroplan, the Commissioner laid an important foundation on the issue of opt-out consent.[101] In this case, Air Canada collected, used and disclosed the personal information of members of the Aeroplan program for certain purposes. At a later time, Air Canada began sharing the information with third parties without the consent of the affected individuals. Air Canada sent a notice to 1% of its members to offer them the ability to opt-out.

The Commissioner found Air Canada to be in violation of PIPEDA in a number of ways. First, the Commissioner held that sending the opt-out notice to only 1% of members was insufficient. The Commissioner noted that Air Canada had to take into account the sensitivity of information in determining the appropriate form of consent. In this case, information about individuals' purchasing habits and preferences was considered sensitive information and warranted opt-in consent. The Commissioner also noted individuals cannot validly consent to a purpose that is incomprehensible because it is too vague and open-ended.

101 PIPEDA Case Summary #42 (Update) - Air Canada allows 1% of Aeroplan membership to "opt out" of information sharing practices - http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020320_e.asp

CONCLUSION

In this document, we have attempted to provide organizations with some of the lessons learned through the concrete experience we have had interpreting and applying PIPEDA to date. It is a retrospective account of just some of the issues we have had to deal with at a very practical level during the first seven years of PIPEDA.

Given the new generation of challenges that lie ahead, what might a document like this look like, another seven years from now? What kinds of new privacy issues will PIPEDA have to address?

With the growing prevalence of social networking sites, behavioural marketing, wireless technology, sensor systems, surveillance systems and nanotechnology, we are just now beginning to see some of the privacy implications of these emerging technologies. Globalization and the growth in online business will only increase the flow of data across jurisdictions. The persistent push towards national security will continue to infiltrate the private sector in incremental, yet pervasive, ways, as organizations come under increasing obligations by the state to participate in anti-terrorism and law enforcement efforts. The commodification of personal information and its increasing value will only increase the appetite for more and more data by legal – and sometimes not so legal – means.

Is PIPEDA up to the task of protecting personal information in this ever-changing world? The legislative review of PIPEDA currently underway is an opportunity now to address this very question. Individuals will no doubt continue to voice complaints about how their lives are being impacted by these trends. These are the underlying stories PIPEDA was meant to address, and certainly redress. They serve as powerful examples, demonstrating how organizations may learn from the experience of others to improve their personal information management practices to better protect privacy and mitigate unnecessary risks.

We look forward to seeing PIPEDA in action as we turn the page on its next chapter.

TABLE OF LEADING CASES

The following table identifies the leading cases broken down by theme as discussed in this document, including relevant PIPEDA sections and principles and the industry sector in which the cases arose. Although in many instances the cases discussed in this document address multiple sections and principles of PIPEDA, the following table identifies only the ones most generally relevant to the discussion in this document.

1. Scope of Application of the Act			
Case	*PIPEDA*	*Industry*	*Issue*
Case Summary #349	s. 2(1)	Landlord/tenant	Photograph as personal information
Case Summary #297	s. 2(1)	Sports organization	Business e-mail as personal information
Case Summary #149	s. 2(1)	Transportation/ airport	Employee ID number as personal information
Case Summary #25	s. 2(1)	Broadcaster	IP address as personal information
Case Summary #315	s. 2(1)	E-mail provider	IP address as personal information
Case Summary #319	s. 2(1)	Internet service provider	IP address as personal information
BMG Canada Inc. v. Doe, 2005 FCA 193	s. 7(3)(c)	Internet service providers	IP address as personal information
Gordon v. Canada (Health), 2008 FC 258	Privacy Act and Access to Information Act	Health	Identifiability and personal information
Case Summary #14 & 15	s. 2(1)	Health	Work product
Case Summary #303	s. 2(1)	Real estate	Work product
Case Summary #220	s. 2(1)	Telemarketing	Work product
Wyndowe v. Rousseau, 2008 FCA 39	s. 2(1)	Health/Insurance	Work Product
Case Summary #309	s. 2(1)	Daycare	Commercial activity
Case Summary #340	s. 2(1)	Law firm	Commercial activity
Rodgers v. Calvert, 2004 CanLII 22082 (ON S.C.)	s. 2(1)	Non-profit	Commercial activity
Case Summary #345	s. 2(1)	School	Commercial activity

2. PIPEDA Beyond Canada			
Case	*PIPEDA*	*Industry*	*Issue*
Case Summary #313	Principle 4.1.3 and 4.8	Financial institutions	Cross-border outsourcing
Case Summary #333	Principle 4.1.3 and 4.8	Security	Sharing information with U.S. parent
Case Summary #365	Principle 4.1.3 and 4.8	Financial institutions	Cross-border outsourcing
Report of Findings (April 2, 2007)	s. 2 and 7(3)(c)	Financial institutions	PIPEDA and foreign entities
Lawson v. Accusearch Inc., 2007 FC 125	s. 2 and 12	Data broker	PIPEDA and foreign entities
3. Surveillance Phenomena			
Case	*PIPEDA*	*Industry*	*Issue*
Case Summary #114	s. 5(3) and 7(1)(b)	Railway	Security surveillance
Eastmond v. C.P.R., 2004 FC 852	s. 5(3) and 7(1)(b)	Railway	Security surveillance
Case Summary #265	s. 5(3) and 7(1)(b)	Railway	Employee surveillance
Case Summary #279	s. 5(3)	Internet service provider	Employee surveillance
Case Summary #264	s. 5(3)	Railway	Employee surveillance and swipe cards
Case Summary #290	s. 5(3) and 7(2)(a) and (b)	Food plant	Employee surveillance
Case Summary #269	s. 7(1)(b) and 7(2)(d)	Industry	Employee surveillance and private investigator
4. Emerging Technologies			
Case	*PIPEDA*	*Industry*	*Issue*
Case Summary #281	s. 5(3) and Principles 4.2, 4.3, 4.4, and 4.7	Telecommunications	Voice print biometric information
Turner v. TELUS Communications Inc., 2005 FC 1601	s. 5(3) and Principles 4.2, 4.3, 4.4, and 4.7	Telecommunications	Voice print biometric information
Wansink v. TELUS Communications Inc. (F.C.A.) 2007 FCA 21	s. 5(3) and Principles 4.2, 4.3, 4.4, and 4.7	Telecommunications	Voice print biometric information
Case Summary #351	s. 2, s. 5(3), s. 7(1), s. 7(2) and Principles 4.2, 4.2.3, 4.3, 4.3.5, 4.3.6, 4.4, 4.5, 4.7 and 4.8	Telecommunications	Global positioning systems (GPS)

5. Data Breaches and Security Measures			
Case	*PIPEDA*	*Industry*	*Issue*
TJX Companies Inc. / Winners Merchant International L.P.	Principles 4.2, 4.3, 4.3.3, 4.4, and 4.7	Retail	Data security breach
Case Summary #185	Principle 4.7	Railway	Technical security measures
Case Summary #226	Principle 4.7	Health	Security measures and staff qualifications
Settled Case Summary #25	Not applicable	Restaurant	Masking information on receipts for security
Case Summary #292	Principle 4.7	Airline	Authentication and security
Case Summary #289	Principle 4.7	Financial institutions	Security and stolen laptop
Case Summary #356	Principle 4.7	Financial institutions	Security and destruction of records
6. Careless Disclosures and Need for Ongoing Employee Training			
Case	*PIPEDA*	*Industry*	*Issue*
Case Summary #372	Principle 4.7	Telecommunications	Social engineering and pretexting
Breithaupt v. Calm Air (Federal Court No. T-2061-04)	Not applicable	Airline	Careless disclosure by employee
Incident Summary #1	Not applicable	Health	Misdirected faxes
Incident Summary #2	Not applicable	Financial Institutions	Misdirected faxes
Incident Summary #3	Not applicable	Financial Institutions	Misdirected faxes
Case Summary #332	Principles 4.3 and 4.7.1	Financial Institutions	Misdirected faxes
Case Summary #360	Principles 4.3 and 4.7.1	Financial Institutions	Misdirected email
Case Summary #242	Principle 4.7	Transportation	Staff qualifications and training for sensitive information
Case Summary #54	Principle 4.7	Telecommunications	Staff training regarding confidentiality
Case Summary #344	Principle 4.7	Financial Institutions	Careless disclosure by employee
Case Summary #200	Principle 4.3	Financial Institutions	Careless disclosure by employee
Settled case summary #27	Not applicable	Health	Careless disclosure by employee
Case Summary #270	s. 7(3)(b) and Principle 4.3	Financial Institutions	Careless disclosure by automated voicemail system
Case Summary #154	Principle 4.7	Financial Institutions	Mortgage documents mailed in unsealed envelope

7. Collecting Too Much Information			
Case	*PIPEDA*	*Industry*	*Issue*
Case Summary #361	s. 5(3) and Principle 4.3.3 and 4.4	Retail	Photo ID for refunds and exchanges
Case Summary #169	Principle 4.3.3 and 4.4	Financial Institutions	Information to open accounts
Settled case summary #28	Not applicable	Retail	Photo ID to open an account
Settled case summary #19	Not applicable	Landlord/tenant	SIN for apartment lease
Case Summary #22	s. 5(3) and Principle 4.3.3 and 4.4.1	Telecommunications	SIN for Internet connection
Case Summary #280	s. 5(3) and Principle 4.3.3	Telecommunications	Photo ID to purchase equipment
Case Summary #368	Principle 4.3.3 and 4.4.1	Insurance	Collection on insurance claim form
Case Summary #257	Principle 4.4	Transportation	Sick leave certificates
Case Summary #233	Principle 4.4	Transportation	Sick leave certificates
Case Summary #135	s. 5(3) and Principle 4.4	Transportation	Sick leave certificates
Case Summary #235	Principle 4.3	Transportation	Contacting hospital about employee exam

8. Meaningful Access to Personal Information			
Case	*PIPEDA*	*Industry*	*Issue*
Case Summary #367	s. 8 and Principle 4.9	Law firm	Access
Vanderbeke v. Royal Bank of Canada, 2006 FC 651	Principle 4.9	Financial Institution	Form of access
Case Summary #352	s. 8, 9 and Principle 4.9	Airline	Access and litigation
Case Summary #285	s. 8, 9 and Principle 4.9 and 4.9.4	Not available	Access, litigation and fees
Case Summary #306	s. 9(3)(a) and 9(3)(d) and Principle 4.9	Health	Access, litigation and privilege
Rousseau v. Wyndowe, 2006 FC 1312	s. 9(3)(a) and 9(3)(d) and Principle 4.9	Health	Access, litigation and privilege
Case Summary #283	Principle 4.9.4	Financial Institution	Fees for access
Case Summary #354	s. 8(6)(a) and (b) and Principle 4.9 and 4.9.4	Not available	Fees for access
Case Summary #328	Principle 4.9.4	Health	Fees for access

9. Secondary Marketing Purposes			
Case	*PIPEDA*	*Industry*	*Issue*
Englander v. TELUS Communications Inc., 2004 FCA 387	s. 5(3) and Principle 4.2 and 4.3	Telecommunications	Consent
Case Summary #42	s. 5(3) and Principle 4.2 and 4.3	Airline	Consent
Case Summary #207	Principle 4.3	Telecommunications	Opt-out consent
Case Summary #192	Principle 4.3	Financial Institution	Consent
Case Summary #308	Principle 4.3.3 and 4.3.8	Financial Institution	Opt-out consent
Case Summary #299	Principle 4.7.1	Financial Institution	Safeguards in secondary marketing
Case Summary #78	Principle 4.2.3 and 4.3	Frequent buyer program	Opt-out consent
Case Summary #83	s. 5(3) and Principle 4.3	Financial Institution	Consent
Case Summary #91	Principle 4.2.3 and 4.3	Marketing firm	Consent