Privacy & Workplace Investigations

Research Project for Emerging Issues/Advanced Topics Course

Diploma in Investigative and Forensic Accounting Program

Prepared by Linda Lister

August 2, 2004

For Prof. Leonard Brooks

TABLE OF CONTENTS

Objectives

Marlon Brando once said: "*Privacy is not something that I'm merely entitled to, it's an absolute prerequisite.*" Many of us feel the same way. We believe we have a right to our privacy and that our privacy ultimately facilitates our freedom.

It is one of my objectives to obtain and impart a basic understanding of our privacy rights in Canada, particularly in reference to the relatively new *Personal Information Protection and Electronic Documents Act* (PIPEDA or the Act).

Towards this end, this paper will first explore the basics behind Privacy legislation in Canada and the effect on commercial organizations. A large part of this paper had been devoted to trying to understand what an investigative body is under the Act and what rights have been conferred on them.

The second objective is to understand the major issues that are raised in courts and tribunals regarding privacy. This paper will then focus on gaining and imparting an understanding of how the privacy legislation, the Charter of Rights and Freedoms and court rulings affects the manner in which organizations and forensic accountants conduct workplace investigations. How organizations collect, document and retain personal information on employees will be affected by the privacy legislation and could affect the outcome of potential criminal proceedings.

What causes people to perceive that their privacy rights have been violated? Do we have an absolute right to privacy or only an expectation of privacy based on the circumstances? Recognizing what causes people to perceive an intrusion on their

privacy will help us comprehend how to avoid potential unfavourable rulings and judgements.

Introduction

PIPEDA establishes a right to the protection of personal information collected, used or disclosed in the course of commercial activities, in connection with the operation of a federal work, undertaking or business or inter-provincially or internationally. It further provides for the Privacy Commissioner to receive complaints concerning contraventions of the principles, conduct investigations and attempt to resolve such complaints. Unresolved disputes relating to certain matters can be taken to the Federal Court for resolution[1].

PIPEDA was passed by the Senate of Canada in 1998 and given Royal Assent in 2000. As of January 1, 2004, it became law in any province that did not have their own substantially similar privacy legislation and applies to all commercial activities. Ontario is one such province.

The Act is based on the current *Canadian Standards Associations Model Code for the Protection of Personal Information.* If a company complies with this code, they can be sure that they are meeting the requirements of the Act. A summary of the 10 Principles of the Code can be found in Appendix C.

The original intent of the Act was to protect our privacy rights as individuals carrying out normal, everyday activities. People have long been complaining that they get unwanted

[1] Bill C-6, *Personal Information Protection and Electronic Documents Act*, Summary page 1, assented to April 13, 2000, located in the Summary

marketing calls or too much junk mail. Much of this came from mailing and phone lists being sold from one company to another. You signed up for driving lessons and find yourself on a mailing list for car dealerships in the area. The protection of personal information has become more important as technology has allowed others to more easily use your identity for criminal purposes such as social assistance fraud and credit card theft.

While the basic principles of the Act require the need for consent from individuals for the collection and use of their personal information, there are some notable exceptions that allow for the collection, use, and disclosure of information between parties under various circumstances. In trying to protect our privacy rights, a strict application of PIPEDA would restrict legitimate investigations. Exceptions were formulated to facilitate such enquiries. These exceptions have been highlighted in Appendix D (**Exceptions related to the Collection and Use of Personal Information**) and Appendix E (**Exceptions to the Required Consent for Disclosure of Personal Information**). It is imperative that forensic accountants understand these exceptions and they will be discussed in more detail.

We should also understand the concept of reasonability. Much of the Act is based on what a "reasonable" person would consider appropriate in the circumstances. This same concept is found throughout various laws, including contract law.

PIPEDA includes provisions for some organizations to be designated an "investigative body". See Appendix F for a complete list of organization that currently have this status. This status allows the investigative body to receive and disclose personal information

without knowledge or consent under some limited conditions. These conditions will be discussed further in the section of this paper entitled **Investigative Bodies.**

Research Scope

The primary focus of the research for this paper was on workplace privacy issues in relation to searches, surveillance and the gathering and sharing of personal information on employees. Case law was researched in an attempt to determine the position of the courts regarding the different circumstances in which an employee has a right to privacy or an expectation of privacy. Understanding the difference between a right and an expectation is essential to understanding scope limitations when conducting forensic audits.

Interviews were conducted with privacy experts to assist in gaining an understanding of the impact of the laws and how the laws may be evolving. Other interviews were conducted to obtain the viewpoints of various legal and accounting organizations in relation to the investigative body status. Part of this research paper was prepared based on these interviews. Appendix B is a listing of people interviewed.

To obtain as many views and opinions as possible on the current state of privacy laws, textbooks, research papers and numerous articles were read. A detailed list is included in the Bibliography.

A list of cases cited can be found in Appendix A. When possible, direct links to the applicable internet page have been included in the footnotes.

Summary of Findings

Much of the Act is still subject to interpretation but there are some common themes. While it is the responsibility of the organizations to ensure they have taken all necessary steps to protect an individuals' privacy, the burden of proof is on the individual to show that they had a reason to expect privacy in the first place. Once the individual has demonstrated that they had a right under the circumstances to expect privacy, it is up to the organization to show they had an overriding right to invade it.

Perhaps the easiest way to summarize what our rights as individuals are in relation to privacy is to assess when others have the right to invade our privacy. When can someone collect, use and disclose information about us that we deem is personal? As previously noted, the Act provides for exceptions to the consent rule that are discussed in detail further in this paper. The courts and tribunals have come up with similar conclusions. Basically stated, in order for an organization to invade the privacy of an individual, they must have a sufficient, supportable reason and they must be able to demonstrate that other, less intrusive means were not available to use.

The organization then has one final requirement. They must show that the information they collected, used or disclosed was appropriate under the circumstances. In other words, they only collected, used or disclosed what was necessary to meet the purpose, nothing more.

As technology increases the capabilities to collect information and human ingeniousness continues to find more creative ways to use it, the courts struggle to keep up with the

changes. Issues such as the monitoring of employees computer use are just beginning to be addressed by the courts.

Privacy legislation continues to evolve. Although PIPEDA just came into effect nationally on January 1, 2004, amendments to be made when the legislation is up for review in 2006 are already being discussed.

Definitions under the Act

In order to understand the provisions and exceptions under the Act, explanations of some of the key terms is required.

Commercial Activity

There is some ambiguity in determining what transactions are covered under the Act. The Act applies to any personal information collected, used or disclosed during commercial activity. Commercial activity under the Act applies to more than just what we think of those as being conducted by commercial organizations and could encompass charitable organizations as well as not-for-profit organizations. The definition in the Act[2] states that a commercial activity:

means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

It encompasses any activity that has the characteristics of a commercial transaction. Would the sharing of a list of subscribers to a religious magazine with a church to use for soliciting donations be in violation of the Act? There is uncertainty in the status the sharing of information between loosely related parties should be considered a commercial activity. It is also unclear as to whether activities carried out by entities such as professional organizations and credit unions[3].

Organization

A similar ambiguity exists when the Act refers to an organization. Under the Act, an

---

[2] Bill C-6, *Personal Information Protection and Electronic Documents Act*, Summary page 1, assented to April 13, 2000, Part 1, Protection of Personal Information in the Private Sector, Definitions

[3] Colin H. H. McNairn, Alexander K. Scott, *Privacy Law in Canada,* Butterworths Canada Ltd. August 2001, p. 106

organization *"includes an association, a partnership, a person and a trade union"* but as above, is not clear on whether not-for-profits, professionals or charities are included.

Personal Information

Personal information has also been loosely defined as:

...information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

When specifying an identifiable individual, corporations and other legal entities are definitely excluded.

Personal information generally includes name, address, telephone number, birth date, social insurance number, credit history, medical information, work history, school history, criminal records and anything else that you might consider belonging uniquely to you.

Publicly available

There are some exemptions that exclude personal information from five public sources specified in a regulation adopted pursuant to the Act. For each source, there are other requirements to be met before the information can be excluded, so some publicly available information still qualifies as being personal information under the Act. These requirements are designed to ensure that somewhere along the line, the individual gave consent to have his/her name and information included. For example, if the public source is a directory of telephone subscribers, the subscribers must have had an opportunity at some point to have their information excluded. Another requirement addresses the use of the information.

An individual may have given consent to have their information included but only for specific purposes. This is particularly true of information given for professional or business directories.

The directories and requirements as found in the regulations[4] are:

(a) personal information consisting of the name, address and telephone number of a subscriber that appears in a telephone directory that is available to the public, where the subscriber can refuse to have the personal information appear in the directory;

(b) personal information including the name, title, address and telephone number of an individual that appears in a professional or business directory, listing or notice, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the directory, listing or notice;

(c) personal information that appears in a registry collected under a statutory authority and to which a right of public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry;

(d) personal information that appears in a record or document of a judicial or quasi-judicial body, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document; and

(e) personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information.

Understanding Exceptions to the Rules

Exceptions related to the Collection and Use of Personal Information

Consent. The main principle behind the Act is the right of the individual to know what information is being collected on them and the manner in which the information will be used. Individuals have the right to determine whether or not they agree with the

[4] Regulations Specifying Publicly Available Information, SOR/2001-7

collection, use and disclosure of their personal information. We have a right to say no. However, as noted in Appendix D, there are some exceptions to the required consent for the collection and use of personal information. These exceptions allow a company to gather personal information on an individual without first informing them that the information is being collected or the purpose for which it is being used.

The most obvious exception is that related to the gathering and use of information that is publicly available. Obviously, information you have allowed to become public, such as your address and phone number (if not unlisted) is information that can be gathered and used without your further consent.

An exception is made for those instances where it is clearly in the best interests of the individual for the entity collecting the information to do so quickly. For example, if an individual was suffering from an allergic reaction and fell unconscious it would be reasonable to expect that a caregiver would try to obtain information on the individual concerning allergies. The same reasoning applies to the use of the personal information gathered. It would be useless for the caregiver to gather the information but then not be able to put it to use.

Another exception exists which allows for the collection and use of personal information without the individual's consent if the act of asking for the consent would lead to the information becoming unavailable, incomplete, inaccurate or false. This could happen if you are trying to obtain information for an investigation. If the person becomes aware you are investigating them or their activities, they could attempt to hide information that would tend to incriminate them. For example, banking, purchasing activity, e-mails

could become difficult to obtain. The actual wording of the Act under section 7(1)(b)[5] states:

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;

Note that the concept of reasonability is raised twice. There are actually two conditions being stated for this exception to be valid. First, if an individual is made aware that they are being investigated, that individual will attempt to inhibit the investigation by hiding or changing information about themselves and or their activities. Obviously, this will most often occur if they have been engaging in illegal activities.

The second part of the reasonability test is designed to protect the individual from having extraneous personal information gathered. An individual's health information is probably totally irrelevant to an investigation related to a breach of a contract.

Personal information can be collected without the individual's consent if it is to be collected for journalistic, artistic or literary purposes. A further exception encompasses the use of information for statistical research or study purposes that would not be accomplished without the information and it is impractical to obtain permission. Two conditions apply. First, it must be shown that the information is collected and retained in a manner that will ensure confidentiality and the Privacy Commissioner is notified prior to the actual collection.

---

[5] Bill C-6, *Personal Information Protection and Electronic Documents Act*, Summary page 1, assented to April 13, 2000, Part 1, Protection of Personal Information in the Private Sector

This section has discussed the conditions under which an organization (or another individual) can collect and use personal information on another individual. What about giving the information you have on an individual to another party? The disclosure of personal information is covered under section 7(3)[6] of the Act (Appendix E). The same primary principle applies. Before you can disclose information on an individual, you should have their consent, but again, there are exceptions as discussed below.

Exceptions related to the Disclosure of Personal Information

Some of the exceptions to the required consent for disclosure are aligned with the same reasons as to why you can collect and use information without an individual's consent. These exceptions include the disclosure of information that is available publicly and information that was collected for statistical, study or research purposes and meets the same conditions as previously mentioned. Your organization can disclose personal information to your attorney or other legal representative. An organization can disclose personal information to another if they are trying to collect a debt that individual owes them. This is the only way you could have a collection agency involved. Other exceptions relate to the passage of time, the desire to protect historical records and the disclosure of personal information to government institutions in relation to national security issues or law enforcement and administration.

The exceptions that relate more specifically to our jobs as forensic accountants include the disclosure of personal information that is compelled by law or by a court of law

[6] Bill C-6, *Personal Information Protection and Electronic Documents Act*, Summary page 1, assented to April 13, 2000, Part 1, Protection of Personal Information in the Private Sector

through a warrant or a subpoena and, the disclosure either to or by an investigative body in connection with investigating a breach of an agreement or a contravention of a the laws of Canada or a province. Per section 7 (3) (d)[7] of the Act:

made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization

> *(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or*
>
> *(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;*

and section 7 (3) (h.2)

made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or

The act seems to be conferring more rights upon investigative bodies in the receiving and giving of personal information. It is important therefore, for us to understand exactly whom and what can be classified as an investigative body.

Investigative Bodies

Paragraph 7(3)(*d*) of the Act allows an organization to disclose personal information to a private investigative body in order to begin or assist with an investigation without the consent of the individual. Paragraph 7(3)(*h*.2) in turn, allows an investigative body to disclose personal information to another private organization (including the client organization and the organization for which they are conducting the investigation). The

[7] Bill C-6, *Personal Information Protection and Electronic Documents Act*, Summary page 1, assented to April 13, 2000, Part 1, Protection of Personal Information in the Private Sector

disclosures must be directly related to investigations of a breach of an agreement or a contravention of the law.

The ability to exchange information without the individual's consent raises concerns about which organizations can obtain investigative body status, how the personal information will be used and stored and how the use of the privileges granted under the act will be monitored.

Two organizations (Insurance Crime Prevention Bureau, a division of the Insurance Council of Canada and the Bank Crime Prevention and Investigation Office of the Canadian Bankers Association) obtained "Investigative Body" status in January of 2001[8]. *Regulations Amending the Regulations Specifying Investigative Bodies* published in the Canada Gazette[9] lists more organizations that have been accepted as Investigative Bodies under the Act as of March 30, 2004. See Appendix F for a list of these organizations. There are basically two types of organizations. Those that require the status in order to monitor their membership for adherence to professional regulations, conduct and codes and those organizations that conduct investigations concerning contractual breaches or the contravention of a law.

The Regulatory Impact Statement[10] issued by Mr. Richard Simpson, Director General, Electronic Commerce Branch, Industry Canada discusses the criteria that Industry

---

[8] Regulations Specifying Investigative Bodies, P.C. 2000-1776 13 December, 2000, http://laws.justice.gc.ca/en/P-8.6/SOR-2001-6/164713.html

[9] Government of Canada, Canada Gazette, Vol. 138, No. 8, April 21, 2004. http://canadagazette.gc.ca/partII/2004/20040421/html/sor60-e.html

[10] Government of Canada, Canada Gazette, Vol. 138, No. 8, April 21, 2004. http://canadagazette.gc.ca/partII/2004/20040421/html/sor60-e.html

Canada has set in order to assess whether or not an organization can be classified as an investigative body. The list of criteria is fairly extensive as they are designed to protect the privacy of individuals as much as possible. Not all criteria will be applicable to all investigative bodies but it should be noted that the criteria are closely aligned with the Canadian Standards Association's Model for the Protection of Personal Information – Privacy Code Principles. Industry Canada has indicated that in order to become an investigative body, the organization must address:

- What type of investigations they generally conduct, what laws and contract breaches they generally address.

- Specifically, what type of personal information they will be required to collect and disclose and why. For example, in addition to property searches (of public record), the investigator may need to gather other financial information such as investments, credit card use.

- Who will be receiving the information and what use will be made of it.

- How will the information be stored? Is it safe from being distributed to unauthorized parties, both internal and external? How long will the information be kept on file? How secure is it? When the investigative body is finished with the information, how will they dispose of it? Is there any kind of audit trail maintained to show how the information was collected and to whom it was given?

- To what extent does the organization try to comply with the Act prior to collecting the information? Do they consider consent? Is there a contract requiring the person to disclose the information?

- In relation to the investigative body itself, there should be some assurance that their members have gone through some sort of licensing requirement and there are policies and procedures in place (that are followed) to ensure the privacy of individuals is protected. Are there penalties or sanctions if the policies and procedures are violated? How is this monitored? The organizational structure including the identification of accountability centres should be clearly documented.

- How independent the organization is from others in the same industry and the client organization.

- Have individuals been informed about the nature of the organization, what they do and how to file a complaint about privacy issues concerning the organization.

Industry Canada representative have indicated that Industry Canada will monitor the activities of the organizations designated as investigative bodies and if it is determined that any organization has not complied with all of the regulations, their investigative body status could be withdrawn.

How Essential is the Investigative Body Status?

It is interesting to note that among the most recent organizations to be designated an investigative body is the Certified General Accountants Association of Canada (CGA)

and the territorial and provincial affiliates. It is the position of the CGA that the investigative body status is required to effectively carry out investigations particularly in relation to disciplinary actions.

The CGA applied for the investigative body status for their members of the Disciplinary Body and for CGAs in public practice.[11] In order to support their position, their submission addresses all of the criteria as set out by Industry Canada. In meeting the requirement for internal accountability, the CGAs stated:

"CGA further undertakes to adopt PIPEDA compliant personal information management practices in a timely manner but by no later than January 1, 2004. Such personal information management practices will include a Privacy Code, an appointment of Privacy Officers and Employee/Independent Contractor Agreements to account and enforce such personal information management practices."

They further assure that CGAs are bound by a Code of Ethical Principles and Rules of Conduct and that a model Privacy Code based on schedule 1 of the Act was developed and would be made available to Public Practitioners. Since then, the CGA has input a new section into their Public Practice Manual that was released early this year. The guideline discusses the Act and who and what it covers. In addition, a Privacy Code, a FAQ sheet and a checklist were developed to assist the Public Practitioners in becoming compliant with the Act.

Practice Inspections for CGA public practitioners are the responsibility of the provincial affiliates. The Disciplinary Committees are also governed by the provincial affiliates. CGA Canada is currently working with the provincial affiliates to harmonize the practice

[11] Certified General Accountants Association of Canada, Submission to Industry Canada for Designation as an "Investigative Body" Pursuant to the Personal Information and Electronic Documents Act (Canada), April 2003, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00206e.html

inspections across the country to possibly include compliance testing regarding the handling of personal information.

In his Regulatory Impact Analysis Statement, March 30, 2004[12], Mr. Simpson stated:

"In reviewing the application of the Certified General Accountants, the Office of the Privacy Commissioner noted that it consisted of two parts. The first part sought to designate the various disciplinary bodies of the provincial CGA's and the second part sought to designate the certified general accountants who are also public practitioners, i.e., registered CGA's who offer their services directly to the public (representing approximately ten percent of the total number of CGA's). The Commissioner's Office had no reservations concerning the designation of the CGA's provincial disciplinary bodies.

As regards the registered public practitioners, the Office noted that the number who would be specified as investigative bodies represented only about ten percent of the total number of CGA's. It also observed that public practitioners are required by the CGA to meet special standards of practice and that the option of obtaining consent was not available for many of the investigations that public practitioners undertake. The Office concluded that there was adequate justification for designating all registered public practitioners as investigative bodies."

Therefore, it does not appear there would be any objection to either the Society of Management Accountants Association or the Canadian Institute of Chartered Accountants (CICA) obtaining the same status for the same basic classes of members. The CICA have the same monitoring practices with their public practitioners as the CGA. The responsibility associated with the monitoring of their members resides with the provincial affiliates. However, as the CICA and the Society of Management Accountants have not applied for an investigative body status, they appear to have a different view on the necessity of being designated an investigative body. It is particularly interesting to note that the Alliance for Excellence in Investigative and

[12] Government of Canada, Canada Gazette, Vol. 138, No. 8, April 21, 2004. http://canadagazette.gc.ca/partII/2004/20040421/html/sor60-e.html

Forensic Accounting, a specialized group within the CICA, have not applied for this status either. The majority of their members work in the investigative or litigation fields.

The CICA does not believe the absence of the investigative body status will hamper their performance of any service for various reasons. The Alliance is not a self-contained separate entity within the CICA and as a result, does not have it's own disciplinary process or charter. The CICA does not have a federal code of conduct or disciplinary body and, as previously mentioned, relies on their provincial affiliates for monitoring purposes. As a result, they do not have a standard code or regulations that would have been required in order to apply for the investigative body status on a national basis.

The view was taken that there are very few instances in which a CA would require access to information that they would be prevented from getting under the Act. The majority of the information they seek is in areas where there is little or no expectation of privacy, including information already in the public domain related to business people or related to a criminal activity. There would be very few instances where they require information that would be compromised by obtaining consent. And finally, in regards to the investigation of a member, since this is not a commercial activity, the Act may not apply. They have also indicated that there has been little effect on the collection, use and disclosure of information from their perspective since the implementation of the Act.

A special issue of "The Balance Sheet" discusses the impact of Federal privacy legislation on investigative and forensic services[13]. [There is a disclaimer at the end of

[13] The Balance Sheet, Special Issue, February 2004, Alliance for Excellence in Investigative and Forensic Accounting

the article stating that it is a non-authoritative guidance only and has not "been adopted, endorsed, approved, disapproved or otherwise acted upon by the Alliance for Excellence in Investigative and Forensic Accounting or the Canadian Institute of Chartered Accountants."]

The article stated that while the IFA Alliance did consider whether to apply to Industry Canada to have CA•IFA's designated as an investigative body, they determined that the benefits derived by doing so were very limited and the organization could become accountable to Industry Canada for the individual CA's compliance under the legislation. The suggestion was made for any CA•IFA who felt that they should require the benefits associated with being part of an investigative body to consider becoming a licensed private investigator as the Council of Private Investigators has been granted an investigative body status.

A number of issues were discussed in relation to the collection and disclosure of personal information by a CA•IFA. Of particular interest is a reference to a speech given by the former Privacy Commissioner to private investigators[14] in relation to whether or not the communication of information to a client by an IFA would be a disclosure or a transfer. Per section 4.1.3 in Schedule 1 of the Act:

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.

---

[14] George Radwanski Privacy Commissioner of Canada, *The PIPED Act and private investigators.* General Meeting of the Private Investigators Association of British Columbia. March 20, 2003 Vancouver, British Columbia.
http://www.privcom.gc.ca/speech/2003/02_05_a_030320_e.asp

Simply put, if information exchanged between a client and an IFA is considered to be a transfer of information to a third party for processing rather than a disclosure, an investigative body status may not be required. To further support this view, in his speech, Mr. Radwanski states:

"As well, investigative body status isn't all it's cracked up to be. People sometimes have an exaggerated idea of what it permits. It doesn't remove an organization from the application of the Act. *Having this status only allows disclosures to, and by, an investigative body in specific limited circumstances. It doesn't, for example, allow an organization to collect information without consent.*

I also would have reservations about recommending that an entire industry or an industry association be granted investigative body status. Unlike the two investigative bodies designated to date-the Insurance Crime Prevention Bureau and the Bank Crime Prevention and Investigation Office-your industry is made up of a large number of generally small companies. Designating these companies as a single investigative body raises a lot of issues, such as ensuring that these companies do not abuse their investigative body status.

So those are some of the problems with investigative body status. But the real reason that I don't think it's a good avenue for you to follow is that it's not necessary. You don't need investigative body status to operate within the Act. *I believe that the* Act *has to be interpreted flexibly and reasonably, and I think that the principal way that the* Act *applies to private investigators is through what can be called the 'agency' concept."*

In Norman Groot's[15] article[16] discussing the speech given to the Private Investigators Association of British Columbia by the former Privacy Commissioner on March 20, 2003, it was his position that the view taken by Mr. Radwanski is not that of Industry Canada and, as it is Industry Canada that is setting the policy, it is advisable to apply for investigative body status. He stated that Industry Canada's position is reflected in the

[15] Norman Groot is a litigation associate at McCague Peacock LLP where his practice is devoted to civil fraud recovery litigation, criminal and civil defence of police, private investigators and security personnel, and privacy litigation and compliance. He authored Canadian Law and Private Investigations. He is also the creator of /www.cdn-pi-law.com, has authored numerous articles on privacy issues and is a Certified Fraud Examiner (CFE).

[16] Norman Groot, *Private Sector Investigations in Light of Recent Policy Statements on PIPEDA,* March 31, 2003

document entitled "Regulation Specifying Investigative Bodies – Regulatory Impact Analysis Statement"[17] where it was stated (emphasis mine):

Many investigations into frauds and breaches of agreement are conducted by private sector organizations, either acting as or making use of independent, ***non-governmental investigative bodies****. Should the investigation reveal grounds for suspecting that a fraud has been committed or a law contravened, the organization may then turn the findings over to a police or other law enforcement agency for further action or (as in the case of professional regulatory bodies such as the Law Societies and the Colleges) may take appropriate disciplinary action pursuant to its own statutory authority. Paragraph 7(3)*(d) *allows an organization to disclose personal information, without the consent of the individual, to a* ***private investigative body*** *in order to instigate or facilitate an investigation. Paragraph 7(3)*(h.2) *allows* ***an investigative body*** *to disclose personal information to another private organization, including the client organization on whose behalf it is conducting the investigation. The disclosures are circumscribed as they must be related to investigations of a breach of an agreement or a contravention of the law and be reasonable.*

Paragraph 7(3)(h.2) *completes the exception provided in paragraph 7(1)*(b) *for collection without consent for the purposes of the prevention of fraud by extending it to disclosure. Collection alone would be of limited use to those combatting fraud and other breaches of agreement, unless the information could be disclosed to the parties that need the information. However, without paragraph 7(3)*(h.2)*, the flow of information could only go in one direction — from the organization to the investigative body.* ***The investigative body would be unable to disclose the results of its investigation back to its client or other interested parties without consent.***

Further to this, there is some controversy around the issue of agency. Could an investigator be considered an agent of the organization by which they were hired thus supporting the idea of the information being transferred rather than disclosed? This is subject to interpretation. Some are of the opinion that if you are an agent, you cannot be an independent third party. As forensic accountants, much of our work depends on the fact and perception of independence.

[17] Regulation Specifying Investigative Bodies – Regulatory Impact Analysis Statement, Canada Gazette, Vol. 138, No. 8 — April 21, 2004

The perception of not being considered independent if you are acting as an agent was somewhat supported by a recent Ontario Court ruling involving the challenge to the admissibility of evidence using PIPEDA.[18] The case involved a person who was suing her doctor for professional negligence during an operation that she claims caused irreparable damage to her left wrist. It was the plaintiff's contention that a video taken by a private investigator hired on behalf of the defendant and submitted as evidence should be inadmissible as it was in contravention of the Act in that it was private information collected in the course of commercial activity without the consent of the plaintiff and that the *Act* prohibits the collection of such information or its use or distribution. The video shows the plaintiff using her left wrist in a manner she had stated she could no longer do.

As part of his interpretation of the Act, Justice Dawson wrote:

One way to avoid this result, and I conclude it is the correct interpretation of the Act, is to apply the principles of agency. On this analysis it is the defendant in the civil case who is the person collecting the information for his personal use to defend against the allegations brought by the plaintiff. Those whom he employs, or who are employed on his behalf, are merely his agents. On this analysis s. 4(2)(b) of the Act governs. That section reads as follows:

4(2) This part does not apply to

(b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose;

The defendant through his representatives was employing and paying an investigator, to collect information for him. It is the defendant's purpose and intended use of the information that one should have regard to in determining the applicability of the Act. On the basis of this analysis I conclude that the defendant is not collecting or recording personal information in the course of commercial activity. He, through his agents, was

---

[18]Denise Ferenczy v MCI Medical Clinics and Dr. Gary Weinstein, Ontario Superior Court of Justice April 14, 2004, para. 30,
http://www.canlii.org/on/cas/onsc/2004/2004onsc11110.html

collecting information to defend himself against the lawsuit brought by the plaintiff. This is a personal purpose in the context of the civil action brought against him by the plaintiff. In my view, this conclusion is consistent with the overall purpose of the Act which is aimed primarily at information collected as a part of commerce.

His conclusion that an agency relationship exists was different from those discussed by Mr. Radwanski. Justice Dawson's key point was that the investigation was not a commercial activity and therefore an agency relationship existed. He then went on to state that, even without the agency status, the video did not contravene the Act because of the exceptions allowed in section 7(1)(b) of the Act (previously discussed). Justice Dawson indicated that he was given an article and some internet resources to read regarding PIPEDA and it was these resources he used to make his determination. At no time did he reference Simpson's Regulatory Impact Analysis Statement in relation to the Act or how it should be interpreted, so it is not clear as to how much credence should be given to his determination. In Englander v. Telus Communications Inc.[19], Justice Blais in his ruling, constantly referred to the Regulatory Impact Analysis Statement for his decisions and stated:

Even if the parties have different views on what weight should be given to such "Impact Analysis Statement", nevertheless, those are a strong indication of the purpose of such regulations.

The Englander v. Telus case involved an individual who had initially put in a complaint to the Privacy Commissioner about the publication by Telus of customers' personal information in its directories. He also claimed that the Act restricted Telus from charging a fee for the provision of the unlisted service. The Privacy Commissioner determined that his complaint was not well-founded. The individual then decided to pursue the issue in a court of law.

[19] Englander v. Telus Communications Inc., [2003] F.C.J. No. 975, para 46

In spite of the assurances given in the speech that private investigators do not need investigative body status to perform their jobs, the Council of Private Investigators – Ontario on behalf of private investigation companies across Canada submitted an application for investigative body status on June 16, 2003 and was granted this status at the same time as the Certified General Accountants Association (March 31 2004).

The Position of Financial Institutions

The following is an excerpt taken from the TD Privacy Code on the TD Bank Financial Group web-site[20] (emphasis mine):

When we release your information

We must give information in response to a valid demand, search warrant or other legally valid enquiry or order. We may disclose information to help us collect a debt owed to us by you. ***We may also disclose information to an investigative body*** *in the case of a breach of agreement or contravention of law - this helps prevent fraud, money laundering or other criminal activity.*

I presented a scenario to a few financial institution privacy officers and legal representatives regarding the investigative body issue. What if a member of a disciplinary committee came to your institution looking for information on one of their members? They had received a complaint from an individual that a member of their professional organization was negligent in the handling of their investments. Was it negligence or theft? What assets does the member have? Would the financial institution release any information on the member to the disciplinary committee? All interviewed first gave a disclaimer in that they have not had a request similar to the above and therefore have not done any research on the issue. Nonetheless, they also all indicated

[20]TD Bank Financial Group, TD Privacy Policy, When we release your information, accessed July 2004 http://www.td.com/privacy/index.jsp#f

that they would not release the information to the disciplinary committee unless it was required or specifically allowed under law or statute. Therefore, the general consensus was that they might release the information to a member of a CGA disciplinary committee without a warrant but not a CICA disciplinary committee member.

Due Diligence

In an attempt to further clarify whether or not an investigative body status is required in order to facilitate workplace investigations, I spoke with representatives from Industry Canada as well as the Office of the Privacy Commissioner of Canada. Both agreed that the Act is not clear on when an investigative body status is required and as to whether or not information is being appropriately disclosed is subject to interpretation. Industry Canada is currently looking at possible amendments to the Act or could be providing clarification with regards to what constitutes a transfer of information to a third party versus a disclosure of information. They are also considering clarifying what is considered personal information as opposed to what is information of business people in the process of conducting business. This distinction is important because if the information can be considered business information rather than personal, it may not be subject to the same restrictions on collection, use and disclosure as personal information.

This distinction is particularly relevant to those of us in the forensic accounting field as well as professionals involved in areas such as mergers and acquisitions. For instance, when conducting a due diligence exercise, how much information can you obtain and disclose on the Directors of the company being purchased before you are crossing the fine line between business and personal? What happens if you have obtained this

information, passed it on to potential purchasers but then the deal falls through? Is there an implied consent by virtue of the Directors knowing that due diligence will be conducted?

The provinces of British Columbia and Alberta have both passed their own substantially similar legislation regarding privacy and have both addressed the issue of mergers and acquisitions. Alberta's legislation section 22[21] deals specifically with "Disclosure respecting acquisition of a business, etc." and basically states that the collection and use of relevant personal information is acceptable although consent should be obtained when possible. It also addresses what should happen if a business transaction does not proceed:

(4) If a business transaction does not proceed or is not completed, the party to whom the personal information was disclosed must, if the information is still in the custody of or under the control of that party, either destroy the information or turn it over to the party that disclosed the information.

The Act is up for review in 2006 and amendments will probably be considered at that time to include some of the concepts currently found in the above provincial legislation as well as possible clarifications to the transfer vs. disclosure of information.

Responsibilities under the Act

There is a perception that the lack of inspection and enforcement of the Act is rendering it ineffectual. A recent article[22] by Michael Geist discusses the lack of enforcement and direction in relation to whose responsibility it is to protect personal information. He references a finding by the Assistant Privacy Commissioner regarding a fax that was

[21] Personal Information Protection Act, S.A. 2003, c.P-6.5
[22] Michael Geist, *Weak enforcement undermines privacy law, the Toronto Star*, April 19, 2004

inappropriately read by a manager[23]. An employee sent a fax related to union matters without a cover page. When the receipt was printed by the machine it contained the body of the letter faxed because no cover sheet was used. The employee was not present when the receipt was printed and a manager was in the process of reading the letter when the employee returned to the fax machine. The manager ignored a request by the employee to stop reading the receipt. While the Assistant Privacy Commissioner acknowledged that the manager should have stopped reading the fax when asked, she determined that the complaint instigated by the employee was not well-founded because he did not take the appropriate steps to protect his own information. It is Mr. Geist's point of view that this approach is not supported by the law.

Currently, there is no requirement for investigative bodies to monitor the compliance of their classes with the Act. Overall, the concept of whose responsibility for ensuring personal information is protected is unclear; however, it is generally understood that in relation to personal information gathered by an organization, it is ultimately the company's responsibility to ensure the information is used solely for the purpose for which it was gathered. In other words, if a company were to release information to another individual or organization that was not designated as an investigative body and the release of this information did not fall under any of the other exemption categories, the company could be held responsible under the Act. At all times, the company that has the personal information in their possession should have an agreement in place with any

[23] Commissioner's Findings, PIPED Act Case Summary #251, A question of responsibility, December 12, 2003,
http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031212_04_e.asp

other organization stating specifically to what purpose the information can be used and ensure it is clear that it is not for any other purpose.

While the Office of the Privacy Commissioner has the authority to conduct audits and investigations, compliance is being assessed on a reactive rather than a proactive basis. This further substantiates the perception that there is a lack of enforcement.

An excerpt from *A Guide for Businesses and Organizations*[24], a publication specifically formulated as a guide in complying with the Act, states:

The following are examples of circumstances that may lead the Commissioner to audit the personal information management practices of an organization:

- *a group or series of complaints about a particular organization's practice(s)*
- *information provided by an individual under the whistleblower provision*
- *an issue receiving media attention.*

When complaints are received, the commissioner will investigate and make a ruling as to whether or the not complaint is "well-founded" (the organization did violate a section of the Act) or not "well-founded". The Privacy Commissioner can then make recommendations to correct situations going forward.

If a plaintiff takes their case to court claiming invasion of privacy and seeking damages, awards tend to be nominal unless they involve extremely personal issues such as videotaping in a bedroom or bathroom. Damages awarded in Insurance Corp. of British Columbia v. Somosh[25] are typical of those awarded for invasion of privacy in relation to inappropriate investigations. An insurance company hired a private investigator to

---

[24]Government of Canada, *A Guide for Businesses and Organizations*, Your Privacy Responsibilities Canada's Personal Information Protection and Electronic Documents Act http://privcom.gc.ca/information/guide_e.asp#016

[25] Insurance Corp. of British Columbia v. Somosh [1983] B.C.J. No. 2034

determine the assets and income of a couple from whom they were trying to recoup insurances losses. During the course of his investigation, the Justice determined that the private investigator asked inappropriate and unnecessary questions about Mr. Somosh and stated at paragraph 59:

The plaintiff had no legitimate interest in the personal habits of Mr. Somosh and in fact had no claim against him arising out of the accident. That being so, Mr. Somosh is entitled to some damages, even though it appears that no damage resulted from these inquiries. There was, in my view, an invasion of his privacy and accordingly I award him nominal damages of $1,000.00.

Although the commissioner's office generally does not have the authority to assess damages or apply penalties and any awarded by the courts tend to be low, most companies are anxious to comply with the Act because the commissioner's office does have the authority to make the name of the organization public. There is a perception that having the company name in the paper in relation to potential privacy violations will result in lost business. At a February 2003 conference, Peter Cullen[26] gave a presentation on privacy and managing client expectations. In his presentation, he stated that:

Privacy accounts for an estimated 14% of overall Brand Value and 7% of overall Shareholder Value indicating that Privacy is more important to the brand than to driving business

His conclusion being that the proper managing of privacy matters is a business opportunity and, if not managed effectively, can be a threat.

[26] Peter Cullen, *Privacy by Design, Managing Your Brand and Trust*, power point presentation at p. 24 http://www.mser.gov.bc.ca/FOI_POP/Conferences/Feb2003/ConfPresentations/PeterCullen.pdf

Commissioner's Findings to Date

The majority of the privacy concerns addressed by the commissioner relate to personal information being inappropriately disclosed by banks. One case of interest arose in 2001 and addressed the issue of whether or not there was a violation of the Act when a teller wrote a person's bank account number on the back of a cheque being cashed[27] without the customer's consent. The complainant contended that by placing his bank account number on the back of the cheque, this information could potentially be inappropriately disclosed to a third party, specifically, the party who wrote the cheque. I found this particularly interesting because during an investigation a number of years ago, I discovered the existence of a shell company by comparing "deposit to account number" information found on the back of the company's cashed payables cheques to the employee's bank information on file for payroll deposits. The Commissioner found the complaint to be not well-founded as it is a reasonable practice and a reasonable customer should expect the practice to occur. Therefore, there is an implied consent and no contravention of the Act.

Privacy concerns in the workplace tend to be centred on video surveillance issues. Two such cases have been discussed in more detail under "**What the Courts Have Decided**".

Surprisingly, the issue of what constitutes a reasonable expectation of privacy in computer use at work is one issue that does not appear to have been addressed yet by the Office of the Commissioner although it has been addressed in the courts. While the

---

[27] Commissioner's Findings, PIPED Act Case Summary #9, Bank teller writes account number on cheque, August 14, 2001, http://www.privcom.gc.ca/cf-dc/cf-dc_010814_02_e.asp

concept of an employer monitoring an employee's technology use (internet usage, e-mails etc.) is outside the scope of this paper, those interested in pursuing this topic are directed to an excellent article entitled "Privacy issues in the workplace: Employer monitoring of employee technology use"[28].

As indicated in the Ferenczy v MCI Medical Clinics and the Englander v Telus Communications cases previously discussed, there are instances where a complaint originally submitted to the Privacy Commissioner could end up in a Canadian court of law. Generally, the Privacy Commissioner attempts to negotiate with both parties to arrive at an equitable solution; however, if a complainant is unsatisfied with a ruling and wants to appeal, or if the complaint was well-founded and they are seeking damages, they could take the case to court. The Privacy Commissioner also has the right to use the courts. Due to the cost and effort this would entail, it would only be done if the issue had a large public interest with further ramifications and therefore a critical determination was warranted from the courts. While the courts have determined that some deference should be given to the Commissioner's Findings, they acknowledge that they do not have to agree.

In Eastmond v. Canadian Pacific Railways [29], Lemieux J. noted:

A proceeding under section 14 of PIPEDA is not a review of the Privacy Commissioner's report or his recommendation. It is a fresh application to this Court by a person who had made a complaint to the Privacy Commissioner under PIPEDA and who, in order to

---

[28] Melanie C. Samuels and Sara Gregory, Privacy issues in the workplace: Employer monitoring of employee technology use, August 21, 2001, www.cle.bc.ca

[29] Eastmond v. Canadian Pacific Railway, 2004 FC 852, June 6, 2004, T-309-03, para. 118, www.canlii.org/ca/cas/fct/2004/2004fc852.html

obtain a remedy under section 16, bears the burden of demonstrating CP violated its PIPEDA obligations.

And in the case of Englander v. Telus Communications Inc.[30] it was stated that:

The present hearing is therefore not an appeal of the Commissioner's report, nor is it an application for judicial review in an administrative legal sense.

Accordingly, I am required to exercise my own discretion de novo.

Therefore, once a case is taken to court, it is not considered an appeal, but rather an action of the first instance.

There are basically four findings defined in the Act that the Commissioner uses.

Discontinued

The investigation is abandoned before the complaint has been fully investigated. A complainant could withdraw the allegations or information necessary to making a determination is unavailable.

Resolved

The investigation substantiated the allegations brought forth by the complainant but the organization has agreed to take correction action that will satisfy the Office of the Privacy Commissioner.

Well-Founded

The investigation substantiated the allegations brought forth and the organization did violate the rights of the complainant under the Act. At the time of the issuance of the findings and recommendations, the organization had not taken corrective action.

[30] Englander v. Telus Communications Inc., [2003] F.C.J. No. 975, para. 29 - 30

Not Well-Founded

The Office of the Commissioner determined that there was no (or not enough) evidence to show that the complainant's privacy rights under the Act had been violated.

Following are summaries of some of the workplace related issues addressed by the Office of the Privacy Commissioner to date. All were obtained from the Office of the Privacy Commissioner of Canada's web-site[31] under "Commissioner's Findings".

Not Well-Founded

PIPED Act Case Summary #65[32]

Thirty-five employees of a company's nuclear products division complained that the company was pressuring them to consent to a security clearance check. If they did not submit, they were threatened with job loss or transfer. The Commissioner concluded that a reasonable person would consider it appropriate to collect personal information for these purposes and that the company had given them sufficient notice and opportunity to switch jobs if they declined.

---

[31]Office of the Privacy Commissioner, http://www.privcom.gc.ca/cf-dc/index_e.asp

[32] PIPED Act Case Summary #65, Employer accused of forcing consent to security screening, August 14, 2002, http://www.privcom.gc.ca/cf-dc/cf-dc_020814_e.asp

PIPED Act Case Summary # 68[33]

An individual complained that the bank refused him access to personal information he had requested, had been late in providing other personal information and had exceeded their authority in collecting information without his consent for the purpose of a fraud investigation. The Commissioner's "not well-founded" decision was based on the conclusion that the bank had met all requirements and that the complainant's knowledge and consent could have compromised the availability and accuracy of the information.

PIPED Act Case Summary #84[34]

A former employee complained that a bank had refused him access to his personal information, specifically the file pertaining to an internal investigation that the bank had conducted in his regard. The Commissioner concluded that the bank's collection of the personal information had been for reasonable purposes and that the complainant's knowledge and consent could have compromised the availability or accuracy of the information.

---

[33] PIPED Act Case Summary # 68, Bank accused of withholding personal information related to fraud investigation, August 30, 2002
http://www.privcom.gc.ca/cf-dc/cf-dc_020830_e.asp

[34] PIPED Act Case Summary #84, Bank cites exemption to deny former employee access to personal information, October 10, 2002
http://www.privcom.gc.ca/cf-dc/cf-dc_021010_3_e.asp

PIPED Act Case Summary #264[35]

This case actually consisted of four complaints. Three were determined to be not well-founded and only one to be well-founded. The complaints were focused on the collection and use of personal information through the installation of video surveillance and swipe cards. The Commissioner found the claims regarding the collection of personal information through the use of video equipment and swipe cards to be not well-founded. She determined that the company had sufficient reason to use this technology, that they were collecting it for appropriate reasons and that the policy statements of the company in this regard were clear. She also determined that when the company used the technology to discipline an employee for information obtained through the course of an investigation, they did not require the consent of the individual.

What the Commissioner determined to be well-founded was the complaint about one of the uses of the information. In addition to the use as per the original intention (security concerns), an employee was inappropriately distributing the photos of certain individuals by showing the pictures to other staff.

PIPED Act Case Summary # 268[36]

Three employees realized that their conversation was being taped in a smoking room. The Commissioner determined that the complaint concerning the inappropriate collection

[35] PIPED Act Case Summary #264, Video cameras and swipe cards in the workplace, February 19, 2002 http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_01_e.asp

[36] PIPED Act Case Summary # 268, Electronic monitoring does not yield any information, but practice is strongly discouraged, April 12, 2004 http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040412_e.asp

of personal information by the company was not well-founded. This determination was made not because the company stated they did so for investigative purposes, but because during the commissioner's investigation, it was determined that the tape was erased and therefore there was no evidence that the complainants' personal information had been inappropriately collected. As part of the findings under a section entitled "Further Considerations" the Commissioner did address the inappropriateness of what the company attempted.

PIPED Act Case Summary #269[37]

The complaint concerned an individual who complained that his personal information was collected and used inappropriately without his consent after he was dismissed when a video surveillance showed that he had misrepresented the state of his health. The company hired an investigator after multiple refusals of cooperation from the individual in relation to accepting jobs he could do under his constraints and in supplying required updated medical information. He had refused to attend an independent medical assessment and he refused a rehabilitation program. The Commissioner determined that while the company had definitely collected and used the personal information without the individual's consent, the reason, method, reliance and purpose for doing so was appropriately supported.

[37] PIPED Act Case Summary #269, Employer hires private investigator to conduct video surveillance on employee, April 23, 2004
http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040423_e.asp

Well-founded

PIPED Act Case Summary #114[38]

A union representative filed a complaint about new digital camera system installed by the company. This case is discussed in detail in the section of this paper entitled "**Video Surveillance – Federal Court**". See also case #265 below.

PIPED Act Case Summary #233[39]

An employee registered a complaint after her company insisted that a medical diagnosis be included on her doctor's certificate to validate her sick leave. Prior to the issuance of the Commissioner's "well-founded" finding, the company revoked its policy requesting medical diagnosis.

PIPED Act Case Summary #235[40]

In another medically related case, an employee filed a complaint when he found out that another employee called the hospital where he had had a medical examination. The complainant had requested sick leave and had submitted a medical certificate. Another

---

[38] PIPED Act Case Summary #114, Employee objects to company's use of digital video surveillance cameras, January 23, 2003
http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp

[39] PIPED Act Case Summary #233, An individual challenged the requirement to provide the medical diagnosis on her doctor's certificate for sick leave, October 3, 2003
http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031003_e.asp

[40] PIPED Act Case Summary #235, Individual challenges employer's refusal to grant sick leave, November 7, 2003
http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031107_03_e.asp

employee then called the hospital to ask further questions about the examination without the consent of the complainant. Unquestionably a well-founded complaint.

PIPED Act Case Summary #265[41]

This involves the same company as discussed in case #114 later in this paper. In addition to the cameras trained on the doors for security purposes, they have digital zoom cameras monitoring train movement in the yards. The security cameras trained on the doors taped the activity whereas the digital cameras in the yards do not. The union has agreed that the cameras in the yard are necessary for the purpose of monitoring train activity.

In this second complaint, two employees complained that the cameras had been used inappropriately to determine that they had left the premises during work hours. The company then took disciplinary action against them. The company contended that the use of the camera to see if the employees left the premises could not be considered collecting personal information since the employees' actions were not recorded. The company then went on to state that even if they were considered to be collecting personal information without consent, it would have been justified because the employees were in breach of their employment agreement.

The Commissioner stated:

Where an employer suspects that the relationship of trust has been broken, it can initiate the collection of information for the purposes of investigating that breach without the consent of the individual. The only evidence that the company presented to suggest a possible breach in the relationship of trust was the fact that the employees in question were entering a private vehicle on this occasion. The company admitted that the

[41] PIPED Act Case Summary #265, Video cameras in the workplace, February 19, 2004 http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_02_e.asp

employees might have been leaving the site with the permission of their immediate supervisor, and that the manager who used the camera only determined after the fact *that the employees left the work site without such permission. The Assistant Commissioner remarked that cameras are highly privacy intrusive, and cautioned that a decision to use them, even in the circumstances set out in Paragraph 7(1)(b), must be taken with great care and deliberation. Where there is a less intrusive method of achieving the same result, it should be the first avenue of recourse.*

This finding highlights two major thrusts of the Act. The company must have sufficient, supportable reasons for violating employee privacy and they must have made every attempt to find less intrusive methods of getting the same results.

What the Courts Have Decided

The Influence of the Charter of Rights and Freedoms

In the following April 23, 2004 decision by Justice Clackson[42], he acknowledged the influence of the Charter in all situations by stating:

"... that does not mean that there is no privacy protection available to employees. Clearly, in cases where the Charter applies there may be an expectation of privacy which requires a reasonableness of search analysis. As well, a reasonable expectation of privacy exists in a situation where the Charter has no application, the Charter's values may still require a reasonableness of search analysis."

The influence of the Charter of Rights and Freedoms is strong and is often considered in conjunction with existing privacy legislation.

While the next case does not discuss PIPEDA, it involves a surveillance issue and discusses an employee's right to privacy versus an expectation of privacy. This case was heard in an Alberta court to review a decision made by an arbitration board. A grievance was heard by the board in relation to an employee's dismissal from the City of Edmonton. The three-person board dismissed the grievance.[43]

---

[42] Clackson J., *Amalgamated Transit Union Local No. 569 v. Edmonton (City)*, [2004] A.J. No. 419, at para. 111

[43] *Amalgamated Transit Union Local No. 569 v. Edmonton City*, [2003]A.G.A.A. No. 69

The employee had been off work on disability due to various conditions that he claimed prevented him from working. The employee was dismissed after a video surveillance (taken outside of a local greenhouse) showed the employee performing physical tasks he had said he could not do. The employee was contending that a video taken of his activities violated his of right of privacy.

In addition to some questions regarding the applicability of the Charter of Rights and Freedoms, as part of Justice Clackson's analysis[44], he addressed three questions:

i. What standard should be used for reviewing the arbitration board's decision regarding the reasonable expectation of privacy.

ii. Did a reasonable expectation of privacy exist.

iii. Do employees have a right of privacy independent of the Charter of Rights and Freedoms?

It was his conclusion that because the respondent is a government agency, albeit a municipal one, the Charter should apply. What is really interesting and applicable to our industry is his discussion on whether or not a right of privacy exists in favour of employees in all circumstances and is summarized in paragraph 115 of the ruling as follows:

As I have said, the Charter which provides constitutional protection of our rights and freedoms, does not recognize a general right to privacy. Therefore, I find it inconceivable that employees would have such a right when other Canadians do not. I appreciate that employer-employee relations create unique circumstances because of the nature of being employed and because the tools of the job may be the very means by

[44] *Amalgamated Transit Union Local No. 569 v. Edmonton City*, [2004] A.J. No. 419, April 13, 2004

which an intrusion on privacy is affected. That unique relationship is what prompted labour relations legislation and the various dispute resolution processes common to the filed. However, it does not compel recognition of the right to privacy.

This distinction is important in that a general right to privacy would prohibit the collection of any photos, candid or surveillance, without the express consent of the individual. His determination in this regard was based on the review of multiple rulings, including one by Justice Cory of the Supreme Court of Canada who said that a person's expectation of privacy will vary with the circumstances.[45] Justice Clackson determined that no reasonable expectation of privacy existed either since the surveillance occurred in a public place in a business that was also open to the public, the employee was engaged in public activities, there were no obvious steps taken by the employee to protect himself from observation and he was not physically searched.

No discussion on privacy would be complete without referencing some of the cases that set precedents and are still being referenced in the courts today. While they do not specifically address workplace issues or PIPEDA, they do discuss the basics of the expectations of privacy in various circumstances. These are important for us to understand, as they are part of the determination as to whether or not information and evidence we gather will be accepted in a court of law.

Hunter v. Southam (1984)[46], R. v. MacKinlay Transport (1990)[47], Regina v. Plant (1993)[48], and R. v. Edwards (1996)[49] are four such cases.

---

[45] Supreme Court of Canada, M.R.M. (1998), 3 S.C.R. 393, p. 276

[46] Hunter et al v. Southam Inc. (1984) 14 C.C.C. (3d) 97

[47] R. v. McKinlay Transport (1990), 55 C.C.C. (3d) 530, (S.C.C.)

[48] R. v. Plant (1993), 84 C.C.C. (3d) 203 (S.C.C.)

One of the issues discussed in Hunter v. Southam[50] is an individual's reasonable expectation of privacy as reflected in the following statement discussing s.8 of the Charter of Rights and Freedoms:

Moreover, s. 8 is not restricted to the protection of property but rather guarantees a broad and general right to be secure from unreasonable search and seizure which at least protects a person's entitlement to a reasonable expectation of privacy.

Other cases then continue to define what a reasonable expectation of privacy entails.

Regina v. Plant[51], discussed whether or not a person has a reasonable expectation of privacy in relation to information being held by places of business such as utilities. At issue, were records from a hydro company used as evidence of excessive hydro usage to grow illegal plants. Per McLachlin J.:

In determining whether or not the accessing of the utilities commission computer was an unreasonable search in violation of s. 8 of the Charter, it must be determined whether there was a reasonable expectation that the information would be kept in confidence and restricted to the purposes for which it is given.

In this instance, the Supreme Court did find that there was a reasonable expectation of privacy since a "reasonable person" looking at the facts would conclude that the records should be used only for the delivery and billing of electricity. Further, as discussed previously in relation to the case involving the faxed union file, the onus is apparently on the individual claiming the violation to show that they had an expectation of privacy and that the expectation was reasonable.

---

[49] R. v. Edwards (1996) 104 C.C.C. (3d) 136

[50] Hunter et al v. Southam Inc. (1984) 14 C.C.C. (3d) 97, p. 652

[51] R. v. Plant (1993), 84 C.C.C. (3d) 203 (S.C.C.) , p. 205

The concept of the accused needing to show they had a reasonable expectation of privacy is further clarified in R. v. Edwards[52] where the Supreme Court of Canada determined that there were a number of principles to be applied when determining whether or not s. 8 of the Charter applied. After listing the principles to be considered the Justices stated that:

Taking all the circumstances into account, the accused had not demonstrated that he had an expectation of privacy in his girlfriend's apartment. Apart from a history of use, the accused could not comply with any of the other factors.

This supports the position that it is up to the accused to demonstrate they had a reasonable expectation of privacy. The circumstances to which they are referring are in themselves, interesting and an understanding of them is important. Taken directly from R. v. Edwards[53]:

(1) a claim for relief under s. 24(2) of the Canadian Charter of Rights and Freedoms could only be made by the person whose Charter rights have been infringed...

(2) s. 8 is a personal right which protects people and not places...

(3) the right to challenge the legality of a search depends upon the accused establishing that his personal rights to privacy have been violated;

(4) as a general rule, two distinct inquiries must be made in relation to s. 8: first, has the accused a reasonable expectation of privacy, and second, if so, was the search by the police conducted reasonably;

(5) a reasonable expectation of privacy is to be determined on the basis of the totality of the circumstances...

(6) The factors to be considered in assessing the totality of the circumstances may include, but are not restricted to, the following:

i. presence at the time of the search;

ii. possession or control of the property or placed searched;

---

[52] R. v. Edwards (1996) 104 C.C.C. (3d) 136, p. 138

[53] R. v. Edwards (1996) 104 C.C.C. (3d) 136, para. 45

iii. ownership of the property or place;

iv. historical use of the property or item;

v. the ability to regulate access, including the right to admit or exclude others from the place;

vi. the existence of a subjective expectation of privacy; and

vii. the objective reasonableness of the expectation.

(7) if an accused establishes a reasonable expectation of privacy, the inquiry must proceed to the second stage to determine whether the search was conducted in a reasonable manner.

The Supreme Court has made it clear that it is the person seeking relief that must show they had a reasonable expectation of privacy and all the surrounding circumstances must be considered. This expectation must be a personal one and not simply associated with a place.

In R. v. McKinlay Transport[54], Justice Wilson was addressing government intrusion specifically but has since been referenced in many other types of cases involving the expectation of privacy. At p. 542 – 543 she said:

Since individuals have different expectations of privacy in different contexts and with regard to different kinds of information and documents, it follows that the standard of review of what is "reasonable" in a given context must be flexible if it is to be realistic and meaningful.

In summary, the vast majority of rulings focus on the reasonableness of the expectation of privacy and that the expectation of privacy is generally lower in a work environment or in a public venue that it would be at home.

Computer Usage

This concept of a lower expectation of privacy is further acknowledged in Milsom v.

[54] R. v. McKinlay Transport (1990), 55 C.C.C. (3d) 530, (S.C.C.)

Corporate Computers Inc.[55]. Mr. Milsom was terminated for non-performance although the company initially terminated him without cause. After termination and during negotiations, the company discovered there was a large volume of non-work e-mails he processed each day. The company then used them as evidence of Mr. Milsom's poor performance and inattention to his job. In his findings, Veit J states at para. 40 - 41 :

Even where an e-mail policy is published within a workplace, and even where the published policy outlines some privacy rights for an employee, an employee may not have a reasonable expectation of privacy when the contents of the employee's e-mail is of an unprofessional nature, offensive, or where access by the employer is in furtherance of investigating illegal activity, in which case the employer's interests would outweigh any claimed privacy right...

Where there is no e-mail policy in place, an employee has no reasonable expectation of privacy in relation to e-mails received and sent in the workplace on the employer's time and equipment.

The expectation of privacy in relation to e-mails both in the office and at home has not been extensively explored even in the courts. R v Weir[56] is a case involving a person charged with the possession of child pornography after an ISP provider found e-mails on his home computer while doing repairs. Justice P. Smith discussed whether or not e-mail carries a reasonable expectation of privacy and stated:

In summary, I am satisfied e-mail via the Internet ought to carry a reasonable expectation of privacy. Because of the manner in which the technology is managed and repaired that degree of privacy is less than that of first class mail. Yet the vulnerability of e-mail requires legal procedures which will minimize invasion. I am satisfied that the current Criminal Code and Charter of Rights protections are adequate when applied in the e-mail environment.

---

[55] Milsom v. Corporate Computers Inc.[55], [2003] A.J. No. 516

[56] R v. Weir [1998] A.J. No. 155, para 55 – 77

There is an interesting case that involved an employer securing the rights to have their employees home computers searched. This is from the United States but Canadian case law often refers to or quotes US court decisions.

Northwest Airlines secured a search warrant allowing them to search the home computers of 21 of their flight attendants who were suspected of orchestrating an illegal work stoppage from their homes[57]. The Judge authorized Ernst & Young (E & Y was retained by Northwest Airlines) to act as an intermediary. It was E & Y's job to image the machines and review the material to determine if there was anything pertinent to the case. They had to ensure that Northwest Airlines did not get access to any information that:

1. was not specifically related to the work stoppage (i.e. chequing account information, web-surfing habits) , and
2. was not protected by some privilege (i.e. some correspondence with Union representatives may have been considered privileged under the collective agreement).

Twelve flight attendants were dismissed and five subsequently quit after it was determined that they did orchestrate the work stoppage.

Video Surveillance – Federal Court

PIPED Act Case Summary #114[58] addressed a complaint filed on January 17, 2002 by an employee (CAW Union representative) of a railway that the company's use of digital video surveillance cameras was in violation of the Act because by using these cameras,

[57] Northwest Airlines vs. Teamsters,Griffin, Reeve Civil No. 00-08 (DWF/AJB), (2000)

[58] Commissioner's Findings, PIPED Act Case Summary #114, January 23, 2002, www.privcom.gc.ca/cf-dc_-3-123.asp

the company was collecting personal information of employees without their consent. The company had placed the cameras at various locations in the rail yard to reduce vandalism, theft, and liability for property damage and to minimize threats to staff. The company did inform the employees of the systems, why they were using it and where the cameras were located. The employees were specifically referring to the ability of the company to monitor the employee's conduct and work performance and use that information in disciplinary actions although the company had stated that the cameras were not intended to be used to monitor employee productivity and they were not aimed at any work areas. The company and the Union disagreed on the necessity for the cameras.

When assessing the appropriateness of the use of the cameras, the Commissioner indicated that there were actually two things to consider. First, whether or not the reason for wanting to use the cameras was reasonable, second, whether or not the circumstances warranted the use of the cameras. It was the Commissioner's belief that a reasonable person would not consider these circumstances to warrant the use of cameras and the employee had a valid complaint due to:

1. The low incidents of vandalism and theft did not sufficiently demonstrate the existence of a real problem.

2. The effectiveness of the system was questionable. He felt that the lack of any incidents since the installation of the cameras could have been from warning signs that could also have serve as a deterrent.

3. The perceived loss of privacy it created in the employees was not offset by any benefit.

4. The Commissioner did not believe that other methods that could have been just as cost effective (such as more lighting in the area) were not explored in sufficient detail.

The Commissioner recommended the removal of the cameras.

On behalf of the employees and based on this ruling, the Union representative took the issue to the Federal Court[59] as allowed under subsection 14(1) of the Act. Specifically, they were requesting a court order for the removal of the cameras, a court order to have any records generated by the use of the cameras to be destroyed and costs of the court action to be paid by the company. This is one of the first cases heard in the Federal court involving PIPEDA.

On June 11, 2004, Justice François Lemieux issued his ruling on Eastmond v CP Rail[60]. While he agreed with the Privacy Commissioner's assessment of what the salient points were, he did not agree with the commissioner's conclusions regarding those points as follows:

1. He was convinced that the evidence established the need for the cameras. CP identified numerous past incidents that justified the need to have the cameras in

[59] Eastmond v. Canadian Pacific Railway, 2004 FC 852, June 6, 2004, T-309-03, www.canlii.org/ca/cas/fct/2004/2004fc852.html

[60] Eastmond v. Canadian Pacific Railway, 2004 FC 852, June 6, 2004, T-309-03, www.canlii.org/ca/cas/fct/2004/2004fc852.html

place including past thefts and complaints from female workers regarding their safety.

2. He felt that "on a balance of probabilities, the cameras are effective". In this, he disagreed with the Commissioner because he felt that the warning signs would not have been enough – the cameras and the warnings signs work hand-in-hand.

3. It was his belief that the loss of employee privacy was minimal and proportional to the benefit gained since the recordings are never viewed unless an incident requiring an investigation occurs.

4. He was satisfied that the company did assess alternatives and came to a reasonable conclusion as to the most cost-effective, viable option.

His conclusions were based on various arbitration cases and additional evidence produced by the company that had not been available to the Privacy Commissioner.

The last point the Justice made is especially worthy of note. The question was asked as to whether or not consent was required to collect the information (use the cameras). It was the Justice's finding that (at paragraph 188):

There is no CP official looking at the monitor at the time the cameras are capturing a person's image. Rather, that person's image is recorded on videotape. The recording is never viewed unless there is a triggering event. The recording is wiped out after 96 hours with the result that person's image is never seen if there is no event.

In this context, I accept CP's argument collection of the person's information takes place when CP officials view the recording to investigate an incident. Assuming the recording captured an individual committing an act of theft asking for his/her permission to collect the information would compromise the availability of the information for the purpose of investigation.

It was his conclusion that CP did not require consent to use the cameras.

As noted earlier, the story involving CP and their cameras continues. The system discussed above is trained on their doors and is used for security purposes. All activity is taped. The second system is a digital camera with zoom capabilities but no tape. As discussed under this paper's section entitled "**Commissioner's Findings to Date**", a complaint filed by two employees regarding the inappropriate use of the digital cameras was determined to be well-founded[61].

And it doesn't end there. This case is currently in labour arbitration. Other labour arbitration rulings will now be discussed.

Video Surveillance – Labour Arbitration Cases

There are two other interesting cases that address video surveillance and involve decisions by labour arbitrators. The first is highlighted on the Canadian Association of Special Investigation Units (CASIU) web-site[62]. CASIU is an organization of insurance investigators specifically geared to addressing insurance fraud through education, training and investigative services. Late in 2003, they posted an article focused on a decision by Arbitrator P.J. Brunner of the Canadian Labour Arbitration Board regarding the Act and employee related surveillance. In Ross v Rosedale Transport[63], Mr. Ross claimed he was wrongfully dismissed after his employer hired an investigator who took a video of him

---

[61] PIPED Act Case Summary #265, Video cameras in the workplace, http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_02_e.asp

[62]Canadian Association of Special Investigations Units, http://www.casiu.ca/president.html

[63] Ross v. Rosedale Transport Ltd. [2003] C.L.A.D. No. 237

lifting heavy chairs etc. when he was moving his family. Mr. Ross had been on modified duties at work due to a work-related lower back injury. In this particular case, the Arbitrator found that Mr. Ross's expectation to privacy as protected under the Act were violated and the company could not use the video as evidence to justify dismissal. His decision was based on his belief that the gathering of personal information in this manner and under these circumstances was not reasonable. He strongly believed that there were other methods through which this information could be collected. In paragraphs 35 and 36 he states[64]:

If the employer really thought that Ross was malingering or pretending that he was not yet fully able to resume the duties of a driver/associate, it was open for Rosedale to ask for an independent medical examination a matter that was conceded by Topping. His failure to do so was left unexplained. This is a case, where an employer, without any evidence that the employee was malingering or had made misrepresentations or spread disinformation as to his physical abilities, orders a surreptitious video surveillance in the hope of trapping the unsuspecting employee during the course of moving furniture at his place of residence at a time and place that he had voluntarily disclosed to his employer. In this respect, the words of Arbitrator M. G. Picher in Canadian Pacific Ltd. and Brotherhood of Maintenance of Way Employees, (supra), are very appropriate:

'as a general rule, (the employer's interests) does not justify resort to random video surveillance in the form of an electronic web, cast like a net, to see what it might catch. Surveillance is an extraordinary step which can only be resorted to where there is, beforehand, reasonable and probable cause to justify it. What constitutes such cause is a matter to be determined on the facts of each case'.

In my opinion, this is exactly what Topping attempted to do, namely, to cast an electronic web to see whether he could catch Ross while moving his family on April 6, 2002. In my view, the collection of this personal information in the form of the video surveillance tape was not reasonable for any purpose related to the investigation of a breach of the employment agreement. Its collection without the knowledge and consent of Ross violated Section 7(1)(b) of the Act. It was for these reasons that I ruled on the first day of the hearings that the videotape was not admissible in evidence.

---

[64] The quote by Arbitrator P.J. Brunner is from Canadian Pacific Ltd. and Brotherhood of Maintenance of Way Employees (1996), 59 L.A.C. (4th) 111 (M. G. Picher)

This is an interesting concept that is relatively exclusive to the Act. Previously, while the concept of reasonability was applied, the consideration of other less intrusive means to obtain the same information was not generally considered.

In another arbitration case, Arbitrator K. Whitaker thoroughly analyzed the applicability of PIPEDA in the workplace as well as the concept of reasonableness and appropriateness of video surveillance. In Teamsters, Local 419 v Securicor Cash Services[65], an armoured truck employee was dismissed for abusing his sick leave after the employer obtained a video taken outside of the employee's house showing the employee was well. The employer had requested the surveillance because the employee had been under suspicion involving some missing cash and had called in sick two days in a row. The employer was concerned that the employee may be leaving the area. The employee knew he was under investigation. Beginning at paragraph 51 and through to paragraph 53, the Arbitrator acknowledged that video surveillance was an invasion of privacy on par with a physical search when he stated:

...In my view, employee surveillance depending on the circumstances, can be understood to be an intrusive inquiry into the private realm of the employee, just as much as a physical search, a drug or alcohol test, a medical exam or the search of a locker or coverall pockets. Whether it is a drug test or surveillance, the employer is conducting an investigation for the purposes of obtaining information that it believes is necessary to run its business. The type of information being sought is usually not of any concern to the employer in the normal course of business and is understood generally to be within the realm of the employee's private life. Absent a special or unusual concern (for example a suspicion of theft or sick leave abuse), an employer would not be interested in what an employee carries in his or her pockets, whether they are in good health or what they might be doing when standing in front of their home when not at work. In the normal course, this type of information would be understood to be part of the sphere of the employee's private life and of no legitimate interest to an employer.

[65] Teamsters, Local 419 v Securicor Cash Services65 (Mehta Grievance) [2004] O.L.A.A. No. 99

For these reasons, the same type of analysis which applies to searches or medical examinations should apply to the issue of surveillance - which is that a collective agreement should be read to include an implicit term that such intrusive inquires are only permitted if reasonable in the circumstances. In other words, the exercise of management's rights to undertake inquiries that intrude into the sphere of what would in the normal course be considered to be an employee's private affairs, are constrained to only those inquiries which are reasonable.

A finding that a collective agreement otherwise silent on the issue of intrusive employer inquiries should be read to include an implicit term that requires such inquiries to be reasonable, is significantly buttressed where the nature of the inquiry may infringe on common law and statutory rights to privacy.

In spite of this view, his conclusions were:

- there is a common law right to privacy in some circumstances;
- there is a statutory right to privacy which applies to this workplace by virtue of PIPEDA;
- management's rights must be exercised in a manner consistent with common law and statutory rights to privacy;
- the collective agreement between the parties contains an implicit term which restricts employer inquiries which intrude into what would normally be considered the private affairs of employees, to those inquiries which are "reasonable";
- the surveillance of the grievor in this case is an inquiry to which the implicit term applies;
- the application of the implicit term has the effect of restricting employer surveillance of employees to circumstances which are "reasonable";

- where surveillance occurs in a public place, that is a factor to take into consideration in determining "reasonableness";
- the surveillance in this case is reasonable and therefore admissible.

Employee Searches

The majority of the guidelines in the area of employee search come from labour arbitration decisions. The best way to approach the answer to the question of whether or not an employer can search personal or company property is to describe the conditions under which the employer has been deemed by arbitrators to have the right and those conditions under which they have been found not to have the right.

Have the right

Most of the Arbitrators agree that the right to perform searches must be clearly laid out in the collective agreement. If there is no collective agreement, the right of the employer to search personal property should be clearly laid out in the policies that the employee reads and accepts. In United Auto Workers, Local 444 and Chrysler Corp. of Canada Ltd.[66] the board of arbitration stated that:

...a company can only justify spot checking of employees who are in no way suspected of theft, and who do not consent to a search of their person (includes property such as purses), by either an express or implied term of the employment.

An implied term of employment would include those instances where searches have been conducted in the past and remain unchallenged by the union or employees.

[66] United Auto Workers, Local 444 and Chrysler Corp. of Canada Ltd (1961), 11 L.A.C. 152, para. 1

This case and Amalgamated Electric Corp. Ltd. (Markham) and International Brotherhood of Electrical Workers, Local 1590[67] both address the concept of balancing the employee's rights to privacy with the employer's right to protect itself against theft and other threats. In Amalgamated, the dissenting Arbitrator states:

The company's right to conduct such searches is an inherent one and in any event falls within the company's exclusive function under art. 2 "to maintain order, discipline and efficiency". Of course, if an employee were to be disciplined as a result of refusing to open his lunch box, a grievance relating to such discipline would be a proper matter before an arbitration board and the board quite properly would inquire into the nature of the search and decide whether or not the employee was entitled to refuse.

In Drug Trading Co. Ltd. & Druggists Corp. Ltd. and Energy & Chemical Workers, Local 11[68], the arbitrator found that although the collective agreement provided the company an implied right to search employees' lockers and personal effects, the searches had to be done in such a manner as to ensure that the employees were not singled out and embarrassed in front of other employees and the search should therefore take place in privacy. On the same issue, in 1981, the arbitrator in the University Hospital v. London & District Service Workers Union, Local 220[69] dispute stated that any searches should be done on a universal basis so that all employees in a given work area are searched or a selection process should be used that is random and does not appear to single out individuals.

---

[67] Amalgamated Electric Corp. Ltd. (Markham) and International Brotherhood of Electrical Workers, Local 1590, (1974), 6 L.A.C. (2d) 28

[68] Drug Trading Co. Ltd. & Druggists Corp. Ltd. and Energy & Chemical Workers, Local 11 (1988), 32 L.A.C. (3d) 433

[69] University Hospital v. London & District Service Workers Union, Local 220 (1981), 28 L.A.C. (2d) 294

No right

Even if the employee agrees to the search, it may be found to be unjustified if the courts find that there was an implied threat of action being taken against the employee if they did not agree to the search. This concept was clearly stated by the majority of the Arbitration board in Amalgamated Electric Corp. Ltd. (Markham) and International Brotherhood of Electrical Workers, Local 1590[70]:

As indicated earlier we find that the company did not actively attempt to enforce its request. However, in view of the fear of suspicion which likely would be felt by those who refused to submit to the form of investigation or search conducted by the company, we find that even though the company may not have been improperly motivated, the company's actions would transgress the fundamental right of personal freedom described in the Chrysler[71] case.

If there are no policies in place or the right to search is not part of the collective agreement and the employer cannot justify the search on the basis of a reasonable suspicion of wrongdoing or there is no immediate danger, the ruling has been[72]:

..the preservation of the right of privacy with respect to personal effects ought to be jealously preserved

In Canada Post Corp. and CUPW[73], the arbitrator found that while Canada Post did have the right to do a visual search of the lockers of employees, they did not have the right to search personal effects. As to what constitutes personal effects, the Arbitrator stated:

I do not intend to attempt to define further what might be included in such a definition but it would obviously extend to a woman's handbag, carried as a normal appurtenance, and almost as a part of her clothing, to hold her usual personal effects. It would also

---

[70] Amalgamated Electric Corp. Ltd. (Markham) and International Brotherhood of Electrical Workers, Local 1590, (1974), 6 L.A.C. (2d) 28

[71] United Auto Workers, Local 444 and Chrysler Corp. of Canada Ltd (1961), 11 L.A.C. 152,

[72] Re Amalgamated Electric Corp. Ltd. and International Brotherhood of Electrical Workers Local 1590 (1974), 6 L.A.C. (3d) 28 p32, 33

[73] Canada Post Corporation v. C.U.P.W. (1990), 10 L.A.C. (4th) 361, page 391

attach to a similar container carried by a man. It would attach while personal effects are with the employee, and also when they are left in the locker.

Due to the diverse circumstances of each occurrence, there are no clear-cut rules as to when an employer can or cannot search an employee's personal belongings. There is one particular case that is constantly quoted and has attempted to set some parameters on when the invasion of privacy of an employee may be acceptable. In Lumber & Sawmill Workers Union, Local 2537 and KVP Co. Ltd.[74], the Arbitrators summarized the rules regarding employee searches:

A rule unilaterally introduced by the company, and not subsequently agreed to by the union, must satisfy the following requisites:

1. *It must not be inconsistent with the collective agreement.*
2. *It must not be unreasonable.*
3. *It must be clear and unequivocal*
4. *It must be brought to the attention of the employee affected before the company can act on it.*
5. *The employee concerned must have been notified that a breach of such rule could result in his discharge if the rule is used as a foundation for discharge.*
6. *Such rule should have been consistently enforced by the company from the time it was introduced.*

The conclusion reached by Arbitrator R. D. Howe in Teamsters Local Union No. 419 and Loomis Armored Car Service Ltd.[75] recognizes that there are times when the company has legitimate reasons for conducting the searches:

---

[74] Lumber & Sawmill Workers Union, Local 2537 and KVP Co. Ltd., 16 L.A.C. 73, pg 85

[75] Teamsters Local Union No. 419 and Loomis Armored Car Service Ltd., [1997] C.L.A.D. No. 33 p. 67

It is also clear from the foregoing review of the pertinent arbitral jurisprudence that arbitrators in both Canada and the United States have recognized employee privacy as an important right to be protected against unwarranted intrusions. However, they have also recognized that this right is not absolute and that it may legitimately be infringed upon to some extent in some circumstances, such as where what would otherwise be a violation of employee privacy has been expressly or implicitly consented to by the employee or the employee's bargaining agent, or where it is imposed by an employer rule or policy necessitated by legitimate countervailing interests of the employer (such as the need to curb a real and significant theft problem) and fulfilling the KVP requirements.

Anton Pillar Orders

An Anton Pillar Order is a private search warrant that can be obtained if you can convince a judge that there had been a breach and that evidence will be destroyed if you don't seize it. Such an order has been categorized as an invasion of privacy as stated in some cases highlighted below.

As times goes on and the granting of Anton Pillar orders becomes more and more frequent, there is a tendency to forget how serious an intervention they are in the privacy and rights of Defendants.

The order derives its name from the case of Anton Pillar KG v. Manufacturing Processes Ltd.,[76]. Guidelines on the use of an Anton Pillar Order were set out at page 784:

There are three essential preconditions for the making of such an order, in my judgment. First, there must be an extremely strong prima facie case. Secondly, the damage, potential or actual, must be very serious for the plaintiff. Thirdly, there must be clear evidence that the defendants have in their possession incriminating documents or things, and that there is a real possibility that they may destroy such material before any application inter partes can be made.

There is a parallel between these three tests and the exceptions for the collection use and disclosure of personal information under the Act. Obviously, the best way to ensure that an Anton Pillar order will be granted and not set-aside at a later date is to ensure that the

---

[76] Anton Pillar KG v. Manufacturing Processes Ltd.,[76] [1976] 1 All E.R. 779 (C.A.), page 784

three tests are met. If you can prove that, you will also be meeting the guidelines for the exceptions to the collection, use and disclosure of personal information under section 7 of the Act.

In Netsmart Inc. v. Poelzer[77], the plaintiff claimed that the defendant did not meet the three requirements and the evidence obtained when the Anton Pillar Order was executed and any decisions based on the results of the search should be set aside. As part of his finding in this case, Belzil J. remarked:

It bears noting that the execution of an Anton Pillar Order is never a pleasant situation and certainly for any party who is the subject of such a seizure, it is considered to be an invasion of privacy, which indeed it is. As noted above, such orders are granted in exceptional circumstances and are to be carried out with a minimum of disruption. This was accomplished in this case.

And a final word to be noted on privacy and the use of Anton Pillar orders taken from the case of Polesystems Inc. v. Martec Mfg. Ltd.[78]:

Conclusions - Learning from the Research

The majority of the responsibility to ensure that the rights of their employees are not contravened belongs with the organization and therefore, the suggestions below are geared to organizations.

As forensic accountants retained by the organization to assist with any investigation or proceedings that may result in criminal charges or litigation, we can and should be providing guidance in tandem with the organization's legal counsel.

---

77 Netsmart Inc. v. Poelzer, [2002] A.J. 1122, para. 42

78 Polesystems Inc. v. Martec Mfg. Ltd.*78* (1989), 67 Alta. L.R. (2d) 159 at pp. 162 and 163:

Strategies for Conducting Surveillance

Hidden, On-Site Surveillance

To ensure that any surveillance information can be used for disciplinary action, prior to conducting a surveillance of an employee or group of employees without their knowledge, the employer should be able to demonstrate[79]:

- There is a substantial problem and there is a strong probability that surveillance will help solve the problem.
- The surveillance is not in contravention of any collective agreement terms.
- All other methods have been exhausted and there is nothing else less intrusive that can be done.
- The surveillance will be done in a systematic manner and not discriminatory.
- That it was reasonable to request surveillance. For example, if the problem is a first occurrence, it is not reasonable to immediately conduct surveillance. Also, you could not conduct a surveillance simply because a person has a record of disciplinary action taken against them. You would need to show a connection between the disciplinary action and the problem.

Off-Site Surveillance

Reasonable grounds for off-site surveillance could include:

- independent evidence from co-workers or others that the subject employee is engaged in other forms of work (while on sick leave)
- evidence provided by a medical practitioner that the employee may be faking injuries claimed

[79] Norman J. Groot, *Canadian Law and Private Investigations*,Irwin Law , 2001

- prior record of damaging company product or equipment

Overall, the longer a person has been employed by the company, the greater the employer's duty to confront them personally for an explanation. Surveillance should be the last resort.

Strategies for Conducting Searches

1. Ensure the right to search is implied in the collective agreement or other policies or there has been a practice in the past of conducting searches.
2. Let the employees know the reason for the search – i.e. Individuals are not being targeted, it is for better security for all.
3. The search should be as unobtrusive as possible.
4. The search should include everyone or be an obviously random sample.
5. The employees should be given prior warning where possible.
6. It should be made clear what the consequences will be if the employee is found with company property in their possession.
7. Prior to conducting a search, if the employer has reason to believe that an employee has company property in their possession, the employer should request police assistance.

Additional Considerations

There is an article that was published by the Information and Privacy Commissioner of Ontario (IPC) in November of 1993[80] that still applies today and addresses some elements considered as fundamental components to ensure workplace privacy for all

[80] Information and Privacy Commissioner/Ontario (IPC), *Workplace Privacy: The Need for a Safety-Net*, November 1993

employees. They also need to be considered when conducting workplace investigations and include:

- No mandatory genetic testing, drug testing and HIV/AIDS testing either pre-employment or in the workplace.
- The well-being of employees should be considered.
- Generic screening or monitoring of employees in the workplace or pre-employment should only be done if the individual volunteers to be tested and has control over the use of the information.
- A mechanism for conflict resolution and mediation should be created.
- The evaluation of a worker's ability to perform in his/her job should be drawn from a performance test rather than from a drug test designed to measure impairment.
- Explicit language on employees' and employers' rights should be included.
- Unless there are extraordinary circumstances, and there is demonstrable and reasonable cause of guilt, covert surveillance devices should not be used to monitor employees.
- Any overt monitoring should be strictly controlled through established standards. Policies and procedures should be developed to ensure all employees are notified as to the purpose and methods of electronic monitoring taking place or anticipated. This would include the monitoring of phone calls, computer use, e-mails etc.

If the people who run the organizations keep in mind how they would like their own personal information handled, the test of the "reasonable person" should be easily met. All of the provisions of the Act and, more importantly the employees will be respected.

Ayn Rand[81] summed up the issue of privacy well when he said:

> *Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men.*

As a society, have we made any progress on protecting the privacy rights of individuals? It is becoming increasingly easier for personal information to be found on the internet. I contacted most of the people I interviewed for this paper through the internet. If I did not find them through a search engine, the simplest way to locate them was to send an e-mail to their company's customer service or information departments and ask that they forward my request for an interview. In one instance, the service department did not forward my request until they had done some research on me! It was interesting to see that, along with my written request for an interview, the service department forwarded information on me they obtained from the Association of Certified Fraud Examiners Toronto Chapter web-site. As I am a Board member, my qualifications and place of employment are listed. I am grateful though, that everyone I asked responded.

For many years now, prospective employers have not been able to ask personal questions about your age, marital status and religion. While this was to reduce discrimination practices on hiring employees, it also served to enhance our privacy rights. Yet, at the same time, employers are asking employees to take polygraph tests and want them to

[81] Ayn Rand (1905 - 1982), *The Fountainhead,* Harper Collins (1943)

submit to drug tests. In some cases, they are being granted these rights, particularly if the employer can show that there is reasonable justification as stated by Picher in Canadian Pacific Ltd. and United Transportation Union (1987)[82]:

In addition to attracting discipline, the refusal of an employee to undergo a drug test in appropriate circumstances may leave that employee vulnerable to adverse inferences respecting his or her impairment or involvement with drugs at the time of the refusal. On the other hand, it is not within the legitimate business purposes of an employer, including a railroad, to encroach on the privacy and dignity of its employees by subjecting them to random and speculative drug testing. However, where good and sufficient grounds for administering a drug test do exist, the employee who refuses to submit to such a test does so at his or her own peril.

The use of polygraphs can be found in businesses with a high risk of cash losses such as armoured car services. The employee generally signs a statement acknowledging the use of polygraphs in certain circumstances and stating that they understand that if they refuse to participate, disciplinary action will be taken. An employee had a grievance denied and lost his job as discussed in Loomis Armored Car Service Ltd. and Canadian Auto Workers, Local 4266A at page 323[83]:

I find that the requests by the Employer were clear and specific; that they were not unreasonable in view of the circumstances; that the grievor was well aware in advance there could be repercussions from failure to submit to the testing; that he was in no doubt as to the seriousness with which the Employer viewed the matter or the extent to which it might react in response to his refusal to comply. If, indeed, the refusal was a true "matter of principle" for the grievor, this ought to have been raised by him by way of a policy grievance while he held official status with the Union.

There are other areas in which we seem to have made little or no progress. Due to 9/11 and more recent threats of terrorism, our privacy rights have been outbalanced in some

[82] Canadian Pacific Ltd. and United Transportation Union (1987), 31 L.A.C. (3d) 179 at pg. 7

[83] Loomis Armored Car Service Ltd. and Canadian Auto Workers, Local 4266A, 57 L.A.C. (4th) 305

circumstances by the need to increase security. This has greatly affected the way in which our funds are handled in financial institutions and the information we are required to give when travelling.

What about the Act itself? Has it improved our privacy? One of the goals was to prevent the selling of our information to others such as telemarketers, for commercial purposes. Our household still receives phone calls almost daily to either purchase something or donate to a charity, so I don't see any improvement. Perhaps it has allowed us to feel that we have some control over who gets our information and how it is used. Provided none of the many exceptions apply. Those in the public eye probably do not appreciate the exception to obtaining consent for journalistic or artistic purposes.

There may have been some progress but until such time as responsibilities are further defined and penalties are increased, any Act or legislation will be perceived to be ineffectual.

Bibliography

Alliance for Excellence in Investigative and Forensic Accounting, *The Balance Sheet*, Special Issue, February 2004

Canadian Association of Special Investigations Units, President's Message on Privacy, accessed July 2004, http://www.casiu.ca/president.html

Canadian Charter of Rights and Freedoms, Enacted as Schedule B to the Canada Act 1982 (U.K.) 1982, c. 11, which came into force on April 17, 1982

Certified General Accountants Association of Canada, *Submission to Industry Canada for Designation as an "Investigative Body" Pursuant to the Personal Information and Electronic Documents Act (Canada),* April 2003

Cullen, Peter, *Privacy by Design, Managing Your Brand and Trust*, power point presentation, 2003

Emond-Harnden, LLP, *Video surveillance: Invasion of privacy or reasonable response to misconduct?*, accessed July 2004, http://www.emond-harnden.com/jan99/videosur.html

Geist, Michael, *Weak enforcement undermines privacy law*, the Toronto Star, April 19, 2004

Government of Canada, *A Guide for Businesses and Organizations*, Your Privacy Responsibilities, Canada's Personal Information Protection and Electronic Documents Act

Government of Canada, Canada Gazette, Vol. 138, No. 8, April 21, 2004.

Gregory, Sara and Samuels, Melanie C. *Privacy issues in the workplace: Employer monitoring of employee technology use*, August 21, 2001

Groot, Norman J., *Application for "Investigative Body" Status Under PIPEDA,* 2003

Groot, Norman J., *Canadian Law and Private Investigations*, Irwin Law, 2001

Groot, Norman J., *Private Sector Investigations in Light of Recent Policy Statements on PIPEDA,* March 31, 2003

Immen, Wallace, *Workplace privacy gets a day in court*, Globe & Mail, April 28, 2004

Information and Privacy Commissioner/Ontario (IPC), *Workplace Privacy: The Need for a Safety-Net*, November 1993

McNairn, Colin H. H.and Scott, Alexander K., *Privacy Law in Canada,* Butterworths Canada Ltd. August 2001, p. 106

Miller, Jeffrey, *Workplace Phone Calls Protected by Privacy Law?*, July 6, 2001, http://www.globeandmail.workopolis.com/servlet/Content/rprinter/20010706/lw-privacy

Personal Information Protection Act, S.A. 2003, c.P-6.5

Personal Information Protection and Electronic Documents Act, Summary page 1, Bill C-6, assented to April 13, 2000

Radwanski, George, Privacy Commissioner of Canada , *The PIPED Act and private investigators.* General Meeting of the Private Investigators Association of British Columbia. March 20, 2003 Vancouver, British Columbia.

Rand, Ayn, (1905 - 1982), *The Fountainhead,* Harper Collins (1943)

Regulations Specifying Publicly Available Information, SOR/2001-7

Regulations Specifying Investigative Bodies, P.C. 2000-1776 13 December, 2000,

Regulation Specifying Investigative Bodies – Regulatory Impact Analysis Statement, Canada Gazette, Vol. 138, No. 8 — April 21, 2004

Swartz, Mark, *Does your boss have the right to spy on you?*, unedited version of an article run in the Toronto Star, accessed July 19, 2004 (no longer available on-line)

TD Bank Financial Group, *TD Privacy Code, When we release your information*, accessed July 2004

Wu, Elaine, Labour and Employment Newsletter, *Video Surveillance and PIPEDA*, Lawson Lundell, Barristers and Solicitors, Summer 2004