

PRIVATE SECTOR PRIVACY LEGISLATION
&
EMPLOYEE INVESTIGATORS IN BRITISH COLUMBIA

By

Dean Parker Davison, BA, MBA¹

INDEX

I.	INTRODUCTION	2
II.	THE EVOLUTION OF PRIVACY LEGISLATION IN BRITISH COLUMBIA.....	4
III.	WHAT CONSTITUTES AN EMPLOYEE’S PERSONAL INFORMATION	7
IV.	EMPLOYEE’S PERSONAL INFORMATION AND PRIVACY LEGISLATION	10
V.	CONSENT.....	11
a.	COERCED CONSENT	14
b.	EXPRESS CONSENT.....	15
c.	IMPLIED CONSENT.....	16
d.	NECESSARY CONSENT TO ENSURE EMPLOYER COMPLIANCE	16
e.	INVESTIGATION EXEMPTIONS TO EMPLOYEE CONSENT	18
VI.	COLLECTION OF EMPLOYEE INFORMATION.....	19
VII.	USE OF EMPLOYEE INFORMATION	22
VIII.	DISCLOSURE OF EMPLOYEE INFORMATION.....	23
IX.	EMPLOYEE ACCESS TO THEIR PERSONAL INFORMATION	27
a.	LAW ENFORCEMENT EXEMPTIONS FOR INFORMATION ACCESS.....	28
b.	THIRD PARTY EXEMPTION TO EMPLOYEE ACCESS	31
c.	EXEMPTIONS TO EMPLOYEE ACCESS UNDER <i>FOIPPA</i>	34
d.	<i>FOIPPA</i> AND THIRD PARTY EXEMPTIONS TO EMPLOYEE ACCESS	38
X.	AN UNREASONABLE INVASION OF THIRD PARTY’S PRIVACY.....	40
XI.	WHEN AN EMPLOYEE AND THE EMPLOYER DISAGREE ON ACCESS.....	42
XII.	PERSON RESPONSIBLE FOR PRIVACY COMPLIANCE.....	43
XIII.	FINES	44
XIV.	WHAT PROTECTIONS WILL WHISTLEBLOWERS HAVE?	45
XV.	SECURITY	46
XVI.	ACCURACY	47
XVII.	AN OVERVIEW: Video Surveillance to Monitor Employees	48
XVIII.	CONCLUSION	53

¹ Dean Parker Davison is currently a third year Student of Law at the University of British Columbia. He has in-depth experience in management and training in corporate security. Additionally, he has extensively dealt with the area of employee investigations, primarily in the retail industry. He can be reached at davison_dean@hotmail.com

I. INTRODUCTION

Privacy concerns itself with the collection, use and disclosure of information. Information is a commodity that individuals, organizations and governments desire. As with all commodities, ownership is paramount in the determination of rights and responsibilities. If you cannot lay claim of ownership to information, then you cannot assert a right to protect, use or sell it. The right to claim an ownership interest over information has a long pedigree dating back to the origins of intellectual property law. In British Columbia, legislation and privacy orders suggest that personal information is for the most part the property of the person it describes. However, this is problematic, if all information concerning you is subject to your property interest then businesses and governments would spend an inordinate amount of resources acquiring permission to collect, use or disclose it. The goal of the privacy legislation is to find a balance between an individual's privacy rights and an organization's ability to function. As the definition of privacy evolves, so does the balance.

Privacy as an ideal also encompasses a person's right to be left alone and control those things that are inherently theirs. In the legislative context of British Columbia, privacy rights, afforded by statute, have primarily been concerned with eliminating the inherent imbalance between the individual and the state. For a variety of reasons, these concerns have leapt into the private sector. The first being technology, as it has created a need for regulation in the private sector. Organizations in the private sector can collect, use and disclose personal information with greater efficiency than every before, making information an even more attractive commodity to a capitalistic environment. Additionally, the Federal Government has passed *Personal Information*

Protection and Electronic Documents Act [hereinafter *PIPEDA*]² that will eventually regulate the private sector in each province unless the Provincial Legislatures enact substantially similar legislation prior to 2004. The Province of British Columbia has stated that they intend to enact legislation that will fulfill the requirements *PIPEDA* of the exemption.

What will be the characteristics of this proposed private sector privacy legislation? How will it affect employee and employer relationships? Will an employer be prohibited from investigating an employee for dishonesty or poor performance? As an employer, it is important to understand the building blocks of privacy legislation. When does an employer need their consent to collect, use or disclose an employee's personal information. Would implied consent suffice or does it always have to be explicit to be valid? When does coercion act to vitiate consent and are there any statutory exemptions available to employers? Moreover, are there exemptions that allow an employer to deny an employee access to their own personal information if it was collected in an investigation? These questions and more will be explored and answers, although not always conclusively, will be reviewed using a practical prediction of the private sector privacy legislation in British Columbia. This prediction will be created based on the current and proposed federal and provincial privacy legislation, as well as examining the practical effect of subordinate regulations and administrative orders. In conclusion, an example of video surveillance in an employee investigation will be used to examine the rights and responsibilities that employers may have once the new private sector privacy legislation is enacted in British Columbia.³ Thereby giving employers a framework of best practices to assist them in their

² S.C. 2000, c. 5.

³ It should be noted that currently PIPEDA does not envision private sector privacy rights for employees. As will be reviewed, this is more a function of jurisdiction than proper legislation and it is more than probable that the private sector privacy legislation enacted in British Columbia will envelope this area of the population.

attempts to resolve employee issues while continue to be law-abiding and proactive contributors in the area of employee investigations.

II. THE EVOLUTION OF PRIVACY LEGISLATION IN BRITISH COLUMBIA

The Dictionary of Canadian law describes privacy as something that “[M]ay be ... the right of the individual to determine for himself when, how and to what extent he will release personal information about himself”.⁴ This definition of privacy has evolved parallel to society and technology. Generally, privacy legislation concentrates, and thus defines that information within its scope, as that which allows a person to be identified. The inherent power imbalance between an individual and their employer and/or the government creates society’s thirst for these privacy protections. The practical aspects of privacy legislation can be found in the codified limits and exceptions and a functioning organizations needs to ensure understanding and compliance with these legislative roadmaps.

In 1993, the British Columbian *Freedom of Information and Protection of Privacy Act* [hereinafter *FOIPPA*]⁵ was enacted to make public bodies more accountable to the public and protect personal privacy. In 2001, the Federal Government enacted *PIPEDA*. *PIPEDA*, the Federal Governments attempt at privacy legislation, will extend its jurisdiction over all Provinces without similar legislation in 2004. Although, the federal legislative regime was originally drafted to separate privacy and access to information, the final form of *PIPEDA* amalgamated the right to protect and access personal information. *PIPEDA* was created to fulfill the *European*

⁴ *The Dictionary of Canadian Law*, 2nd ed., s.v. “privacy”.

⁵ R.S.B.C. 1996, c. 165.

Union's Data Protection Directive.⁶ In an attempt to try to standardize trade principles, the European Parliament and Committee drafted the *European Union Directive*. The *European Union Directive* states that countries inside the European Union cannot enter into international trade agreements with other countries unless they adhere to rigorous standards of information protection. Subsequently, the six major chartered banks in Canada and the Department of Industry pressed for the creation of *PIPEDA* to satisfy the standards. In January of 2002, it was determined that the legislative implementation of *PIPEDA* qualified Canada to trade information with countries in the European Union.

PIPEDA asserts government regulatory control over all private organizations that collect, use or disclose personal information in the course of commercial activity and that currently fall outside of the jurisdiction of the federal *Privacy Act*.⁷ Sections 26(2) (b) and s. 30 of the *PIPEDA* allow a province to be exempt if they enact substantially similar legislation prior to 2004. A large part of the *PIPEDA* and its ideology is contained in the Canadian Standards Association's *Model Code for the Protection of Personal Information* [hereinafter *CSA Privacy Principles*].⁸ It appears that any form of provincial legislation that would fulfill the *PIPEDA* requirements would have to be consistent with the *CSA Privacy Principles*. There are many reasons why the government of British Columbia is being pressured to enact similar legislation. For example, British Columbians want it⁹, the government has promised it¹⁰, international trade practices

⁶ EC, Council Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995], O.J.L 281 p. 31. [hereinafter *European Union Directive*].

⁷ *Privacy Act*, R.S. 1885, c. P-21 [hereinafter *Federal Privacy Act*]

⁸ CAN/CSA-Q830-96.

⁹ British Columbia, Legislative Assembly, "Information Privacy in the Private Sector Report" by Special Committee in Fourth Session, Thirty-sixth Parliament (2001) at p. 13 [hereinafter *British Columbia Special Committee*].

¹⁰ British Columbia, Office of the Information and Privacy Commissioner, *Budget Proposal 2003/2004* (British Columbia: Canadian cataloguing in Publication Data) at p. 4.

demand it and most importantly, society and technology has made it a necessity. The question, which most concerns private sector employers in British Columbia, is how the new legislation will affect their business practices. Will it mirror *PIPEDA*, be similar to *FOIPPA* or be a hybrid of both?

FOIPPA deals with the right to privacy and freedom of information inclusively. In the federal scheme, the *PIPEDA* amalgamated an individual's right to privacy and access to information within the health and private sectors. A *FOIPPA* style legislation will most likely be overseen by the Office of the Information and Privacy Commissioner of British Columbia and include the right to privacy and access to information regimes. If British Columbia is going to have private sector privacy legislation, what should it look like to comply with *PIPEDA* and how will this effect employer's investigations of employees.

The Ontario Government has recently created a draft of their private sector privacy legislation with the hopes that it will satisfy the criteria of *PIPEDA*. As for the Quebec, their privacy act was already deemed substantially similar in 2000 and thus fulfills the requirements of s. 30 of *PIPEDA*. Although, there is currently no similar type of privacy legislation in British Columbia, there has been a privacy committee created and they have, consequently, developed recommendations for the proposed legislation. These recommendations, along with *FOIPPA*, *PIPEDA*, the *CSA Privacy Principles*, Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector* [hereinafter *Quebec Privacy Act*]¹¹, and the draft of the Ontario

¹¹ R.S.Q. c. P-39.

Privacy of Personal Information Act [hereinafter *Ontario Privacy Draft*]¹², will assist in developing the proposed private sector privacy legislation in British Columbia. A comparison of these various legislative formats and policies will assist in determining best practices and suggestions for private sector employers when they are doing employee investigations. In particular, it will assist in determining how employers should collect, use and/or disclose an employee's personal information.

III. WHAT CONSTITUTES AN EMPLOYEE'S PERSONAL INFORMATION

To protect an employer's privacy through legislation, the legislation needs to establish a working definition of what is reasonably contemplated by the term "private". Clearly, such a definition cannot encompass every personal item of information regarding an employee, no matter how significant its connection may be to their personal expectation of privacy. As with all privacy legislation in Canada, the *Quebec Privacy Act* and the *PIPEDA* are concerned with personal information infractions and not with privacy as a right in your home or outside of commercial or government activity. The *Quebec Privacy Act* adds the term "natural person" to the definition to focus the protections on its citizens and not businesses. The *FOIPPA* additionally requires that the information was recorded or formed part of a permanent record to qualify as personal information and defines "recorded" as anything where information is recorded or stored (other than software or anything that produces records). Moreover, information is deemed personal, in *PIPEDA* and the *Ontario Privacy Draft*, if it could be used to identify an employee through reasonable deduction or manipulation¹³ whether spoken or written. If British Columbia's privacy legislation is going to fulfill the requirements to be substantially similar to *PIPEDA* its definition

¹² Ontario, Ministry of Consumer and Business Services, *Consultation on the Draft: Privacy of Personal Information Act, 2002*, online: <<http://www.cbs.gov.on.ca/mcbs/english/pdf/56XSMB.pdf>>

¹³ *Ontario Privacy Draft*, *supra* at p. 20

of personal information may not be restricted to recorded information. Therefore, information, recorded or not, that directly relates to an employee or could be used to identify a particular employee will, under the *PIPEDA* guidelines, be deemed personal information and thus have to be protected and regulated. Such regulations could potentially encompass videotape, audiotape, pictures, key strokes programs, access control programs and interview notes¹⁴, all of these tools may be used in employee investigations but are also used by most employers in normal daily activities.

Privacy legislations in Canada attempt to deal with this dichotomy with subtle differences. The differences relate to how specific the personal information has to be to be classified as such under the privacy acts. The *Ontario Privacy Draft* states that personal information includes anything that can be manipulated to allow identification of an employee. Because this legislation is in the draft stage, it does not have the benefit of a working commissioner's office or their decisions. If the *Ontario Privacy Draft* is passed in its current form, the Ontario Privacy Commissioner will regulate both Ontario's *Freedom of Information and Protection of Privacy Act* [hereinafter *FIPPA*]¹⁵ and the *Ontario Privacy Draft*. Therefore, one of the best indicators of how the Commissioner may rule on future issues is an examination of her prior decisions. Under the current privacy regime in Ontario, personal information has been determined to include what a person said, what people have said about that person and current employee information. She has concluded that even the number of laboratory tests a doctor has ordered within a year is that doctor's personal information.¹⁶ If an employer can contravene a privacy act through standard

¹⁴ *Refusal of employee access to records after sexual harassment case* (Ministry of Attorney General) (1997), B.C.I.P.C.D. No. 193 (193-97) at p. 4. [hereinafter *FOIPPA Employee Sexual Harassment*]

¹⁵ *Ontario*, Chapter F.31.

¹⁶ *Ministry of Health* (1994), p-778 at p.4.

operating procedures, like monitoring internet access, then how is an employer going to ensure compliance?

The proposed definition of personal information in the private sector privacy legislation for British Columbia may reflect the openness of the definition in *FOIPPA*, which includes not only what a person says, does or is said about them,¹⁷ but also information that can allow a reasonable person to deduce an employee's identity. This encompasses a large portion, if not all, of the information an employer may collect about an employee. For example, once a person is hired, an employer typically maintains an employee file that is kept with Human Resources or their manager. Anything in that file that could identify the particular employee is their information and theoretically, owned by them. Additionally, all of the information collected in an investigation would be the personal information of the employee. This could include written documentation, audits, video and audio surveillance, correspondence monitoring, and conversations with their peers, subordinates and superiors. However, privacy legislation concerns itself with the balance of fair collection, use, disclosure and access principles between an employee and an employer. An employee can easily prove that information in their file is theirs but for an employer to keep this information from the employee is considerably, more burdensome. The following sections will review the issues in privacy legislation as they may relate to an employee investigation in light of the proposed private sector privacy legislation in British Columbia.

¹⁷ *FOIPPA Employee Sexual Harassment, supra*

IV. EMPLOYEE'S PERSONAL INFORMATION AND PRIVACY LEGISLATION

As mentioned above, if the Provinces do not create substantially similar legislation prior to 2004, *PIPEDA* will regulate private sector privacy within those provinces. *PIPEDA* concerns itself with all organizations that collect, use or disclose personal information in the course of their commercial activities. An organization includes an association, partnership, a person or trade union.¹⁸ Notably, exemptions under *PIPEDA* include; any government institution regulated by the *Federal Privacy Act*, and all information that is categorized as a domestic, personal, journalistic, artistic or literary use of personal information. The *Quebec Privacy Act* and the *Ontario Privacy Draft* both specifically include all organizations outside the purview of their public sector privacy legislation. Thus, it is reasonable that most business would be regulated by *PIPEDA* or like provincial legislation. This creates a blanket of privacy legislation that ensures that in British Columbia most private sector employers will be regulated by privacy legislation.

Employees of federal works are currently protected by *PIPEDA* but in 2004, employees of private sector organizations will not be afforded these same protections. Federal legislation that only protects employees of federal works runs the risk of falling short of the *European Union Directive*. Certainly, privacy legislation is adopted, in many cases, to protect the rights of citizens from the imbalance of power in their relationships with government and corporations. One could argue that employees have an even greater power imbalanced relationship with their employers and in many situations; the only way to ensure their privacy rights are protected is through privacy legislation. In Ontario, the legislation attempts to treat employee information similar to a citizen's personal information, as reflected in a quote from the Ontario Privacy Commissioner's frequently asked question section of the privacy web page.

¹⁸ *PIPEDA*, *supra* at p. 2.

The proposed privacy legislation will impact employers and employees in Ontario because it will cover most personal information in the employment context. With a few exceptions, the legislation will not treat employment information differently from other types of personal information.¹⁹

Privacy legislation would and should give employees equal, if not more, privacy protection from their employers as compared to the protection citizens have from the government. Additionally, the *British Columbia Special Committee* found in an Ipsos-Reid survey that seventy percent of British Columbians believe it is very important to have privacy legislation that specifically addresses employee information protection.²⁰ This was third in importance behind financial and patient information, respectively. Thus, it appears politically unlikely that employee privacy rights will not be present in future British Columbia private sector privacy legislation.

V. CONSENT

Consent is one of the fundamental principles of privacy protection. It gives an employee control over their personal information. The privacy commissioners and privacy advocates would prefer a company did not collect or use information without consent but the question then turns to what constitutes consent. The Canadian Law Dictionary defines consent as “freely given agreement” and this is repeatedly echoed in Canadian privacy legislations. There are three issues to be considered when dealing with freely given consent by an employee to an employer. First, how much knowledge about the collection of their personal information does an employee have to possess before they can effectively give their consent and what responsibilities do employers have to supply this information. Second, if the initial consent to collection is given does that permit an employer to continue collection and use of that information indefinitely? Third, does

¹⁹ Ontario Privacy Commissioner’s “Frequently Asked Questions”, online: <http://www.ipc.on.ca/english/whatsnew/newleg/faqleg-e.htm#mean> (date accessed: November 21, 2002).

²⁰ *British Columbia Special Committee, supra* at p. 50.

the inherent imbalance in the employee / employer relationship vitiate an employee's consent, particularly when the consent is requested from a potential employer?

Before an employee can make an effective decision about consent, they must be informed. A person cannot give proper consent if they do not understand to what they are consenting. The *Quebec Privacy Act* says that for consent to be appropriate it must be "enlightened". *Section 8(1)(4)(a)* of the *Ontario Privacy Draft* also states that a person must understand the nature and consequences to give proper consent. Additionally, The *CSA Privacy Principle 4.3* in *PIPEDA* explicitly affirms that an employee must know or have knowledge of the nature of their consent for it to be valid. The *Ontario Privacy Draft* is more specific in its definition of consent, as it outlines for a person to give free and voluntary consent they must know what information is going to be collected, who will have access, how it will be used and when will it be disclosed. Although, this may seem an overly onerous burden on an employer, it does go to the heart of consent. An example of invalid consent may be the consent a person gives a film crew when being interviewed. The consent may be given for the footage to be used on the evening news but no one informed the subject that the coverage would be used as part of larger film outlining the ignorance of Canadian's or repeatedly aired in subsequent news broadcasts as a background to convicted child molester stories. Without complete disclosure of the actual use, the consent may be void. Consent obtained through partial truth or misleading information should not and does not fulfill the proper requirements for consent of personal information for collection, use or disclosure. Even if the request is truthful, it should be specific. The British Columbia Privacy Commissioner has deemed that the Workers Compensation Board of British Columbia was in contravention of *FIOPPA* when they started collecting employee's information as they applied

for benefits even though all employees signed a generic consent form. To amend the privacy infractions the WCB adopted the following commissioner's recommendations;

The WCB should amend the consent form that workers are required to sign to indicate the purpose for collecting personal information, the legal authority for collecting it, and the title, business address, and business telephone number of an officer or employee of the WCB who can answer the employee's questions about the collection pursuant to section 27 of the *Freedom of Information and Protection of Privacy Act*.²¹

Thus, a specific consent form or consent clause should be included with a hiring package. For it to be valid the consent request should include the information contained in the above quote and the person administering the consent should be able to adequately explain all aspects of the request. Notably, this does not create a continuing consent for all personal information collection, use or disclosure.

It may not be realistic or practical to outline all possible uses of personal information at the onset of employment or a business relationship but employers do have some flexibility in obtaining consent when the original use of the information has been expanded. In the *CSA Privacy Principle 4.3.5*, the reasonableness of an employee's expectations is relevant to the expanded use of personal information. The *Ontario Privacy Draft* s. 8(1)(4)(c) says informed consent is what a reasonable person would expect in the circumstances. The definition of reasonable varies but in past *FOIPPA* orders, it has been an objective test defined as what a reasonable person would believe to be acceptable in this circumstance.²² For example, when a person is hired and they give consent for collection of their basic information for payroll and government deductions, it

²¹ Re Disclosing Personal information about injured workers to employers (WCB of British Columbia), (1996) B.C.I.P.C.D. No. 006 (p96-0006) at p. 21. [hereinafter *WCB disclosure*]

²² *WCB disclosure, supra*.

may be unreasonable for that employer to use the employee's information in an internal investigation without obtaining further consent.

a. COERCED CONSENT

Additionally, even if the consent is attained for a specific purpose it should not be in exchange for something or because of a threat. The *CSA Privacy Principle 4.3.3* outlines consent shall not be given as a condition of supply of a product or service beyond what is required for that service or product. Meaning, an employer cannot demand consent of a potential employee in exchange for hiring them unless the consent was for collection or use of information necessary for the position. The *Ontario Privacy Draft* also identifies that consent given because of undue influence by an employer will nullify the consent. This would again refer to what is reasonable. An employer would not be justified in requesting consent for a criminal record check on one employee and not another if they are applying for the same job, as it could be argued that the check is not required for the position and thus the consent is in exchange for being hired. Similarly, an employer would also not be justified in or if it was not standard practice for that position. A background investigation is common practice for high-level management positions or positions that have security clearance. How evasive can the investigation be even with consent? It is certainly arguable that the consent is given in exchange for opportunity to be considered for the position. Is the consent valid and who can have access to this information, particularly if the candidate is not successful? As will be shown, this investigation would not be exempt under the "law enforcement" category. It would initially appear that this common practice by employers is in contravention of standard privacy legislation.

Another problematic example of employee consent includes peer pressure and past practices. For example, if ten out of eleven employees give consent for locker checks, is the eleventh employee really giving consent freely or are they doing it because of peer pressure to conform or for fear of others thinking they have something to hide. In this scenario, what obligation does the employer have to alleviate this pressure to consent? Does an employer have to ensure an employee's consent is freely given and well informed or is their only responsibility to ensure that they do not create or contribute to the coercion that made the person consent?

b. EXPRESS CONSENT

Express and implied consent are two types of consent considered by the Federal Privacy Commissioner, in some of his recent orders. Express consent is specific and can entail something as basic as a signature, a verbal agreement or a check-off box but normally involves an action. According to the Federal Privacy Commissioner, express consent is the preferable way to ensure that an employee has consented to an employer's control of their information. The question then turns to the practicality of employers getting freely given and explicit consent from employees. The privacy legislation and orders attempt to attain a balance between an employee's privacy protections and a business's ability to be commercially effective. If express consent were required for all personal information, many businesses would cease to function. Sensitivity of the personal information appears to be the distinguishing characteristic between the need for express and implied consent. The more sensitive or potentially damaging the personal information is the greater the likelihood that express consent is required for its collection, use and disclosure.

c. IMPLIED CONSENT

The make-up of the personal information may allow for implied as opposed to express consent. The *Ontario Privacy Draft* states that implied consent may entail a standard action by the employee but it would need to be reasonably applied. An example of this may be, when an employee gives an employer their social insurance number it is implied that the use of this information is for payroll reasons. However, there is no such implied consent for an employer to do a credit check with the same social insurance number and such a check would be in contravention of an applicable privacy act. Using a lack of action to indicate express consent has fallen out of favor with the Federal Privacy Commissioner. In his decision on March 20, 2002, Air Canada's opt-out consent, requiring a customer having to do something to deny consent. "I have a very low opinion of opt-out consent, which I consider to be a weak form of consent, reflecting at best a mere token observance of what is perhaps the most fundamental principle of privacy protection."²³ He has also chastised Canada Post and their requirement of customers to write a letter to be excluded from mailing lists sold to advertisers.²⁴

d. NECESSARY CONSENT TO ENSURE EMPLOYER COMPLIANCE

Coerced consent will never be valid consent; therefore, an employer should never force, or even appear to force, an employee to consent to the collection, use or disclose of their personal information. Coercion is a subjectively assessment. Would a person in a particular position be able to freely consent to the privacy intrusion. As noted earlier many employers unintentionally coerce their employees into consenting but regardless, the consent is still void. A Judge,

²³ George Radwanski, "Air Canada's Aeroplan Frequent Flyer Program" (2002), online: Privacy Commissioner of Canada <http://privcom.gc.ca/media/nr-c/02_05_b_020320_e.asp> (date accessed: 20 December, 2002).

²⁴ George Radwanski, "Canada Post's Change of Address Notification" (2002), online: Privacy Commissioner of Canada <http://privcom.gc.ca/media/nr-c/02_05_b_020417_e.asp> (date accessed: 20 December 2002, 2002).

Commissioner or Arbitrator may look at the reasonableness of the consent. If all employees have consented to an intrusive bag check then the possibility of coercion certainly arises. The fact that no one has questioned the bag check lends itself to the determination that the employees are not allowed to decide and thus no consent is requested or freely given. For an employer to ensure an employee freely gives consent, they have to guarantee there are no penalties for repudiation or benefits for it being bestowed. However, if there is doubt as to whether the consent should be explicit or implied, it is always best to get explicit consent. In fact, the *Ontario Privacy Act* says in s. 8(1)(1) that if an employer is in doubt between the necessity of implicit or explicit consent, explicit consent is required. Furthermore, the *Ontario Privacy Draft* goes on to say that implied consent can only be used when the use, collection and disclosure is reasonably obvious, the employer can reasonably expect consent and the personal information is only used for the purpose it was consented. The *British Columbia Special Committee* and the *CSA Privacy Principles* also state that express consent is necessary for sensitive information. Thus, an employer should always determine the sensitivity of the personal information prior to deciding if implied consent is pragmatic. If the employer is unsure, it is always advisable to get express consent. Video surveillance of a person's activities at work in public or common areas could be unobtrusive information and implied consent may suffice, especially if the cameras were overt or in highly visible domes. However, someone's credit history, criminal record, health information, personal activities and friends or family could be deemed highly sensitive and would most likely require express consent to collect, use or disclose. Therefore, an employer would rarely be able to depend on an employee's implied or generic consent to allow them to conduct an in-depth internal investigation. An employer may be better served to look at the applicable exemptions under the privacy acts in order to ensure compliance.

e. INVESTIGATION EXEMPTIONS TO EMPLOYEE CONSENT

Once the information is classified as an employee's personal information, as in an investigation, it may not be realistic or plausible to acquire consent without affecting the validity or volume of the information. An employer should then look to exemptions to consent in the applicable privacy acts. These exemptions apply to collection, use, disclosure and access of personal information but may refer to each category separately. In regards to employee investigations, the exemptions for law enforcement may be the most practical. The *CSA Privacy Principles* and the *British Columbia Special Committee* are relatively silent as to law enforcement or criminal investigation exemptions; however, they both state that the any law enforcement exemption must be used in a reasonable fashion. The *Quebec Privacy Act*, *Ontario Privacy Draft*, *FOIPPA* and *PIPEDA* all include some type of law enforcement exemption and concur that for it to be valid it must be reasonable. The definition of reasonableness can be as elusive as the definition of privacy and in regards to an employee's protections, it is equally fundamental. In the Federal Privacy Commissioner's annual review, he makes a particularly relevant statement regarding "the reasonable person test"

That provision— "the reasonable person test" as it's known—is what makes the Act a true privacy protection statute, rather than just a code of fair information practices. It's particularly important in situations like employment, where there's a power imbalance between an employee and an organization that wants to collect, use, or disclose his or her personal information. The organization can't use its greater bargaining power to coerce the employee to consent. It has to be able to justify what it wants to do, and show that it's reasonable.²⁵

Thus with the power imbalance, how does an employer justify collection, use and disclosure without consent? Is consent always coerced, even when it is a minor privacy infraction for

²⁵ Canada, Privacy Commissioner of Canada, *Annual Report to Parliament 2000-2001* at part 3. online: Privacy Commissioner Homepage < http://privcom.gc.ca/information/ar/02_04_09_03_e.asp#002>.

productivity concerns? As consent in employee investigations is at best tumultuous, an employer would be better to look to law enforcement exemptions for justification. Collection, use and disclosure exemptions will be reviewed separately as some exemptions vary the information that can be collected and when the exemptions are valid.

VI. COLLECTION OF EMPLOYEE INFORMATION

Investigators in licensed organizations, in Quebec, do not have to obtain an employee's consent before they collect personal information, if they are reasonably trying to prevent, detect or repress a crime or statutory offence.

A detective or security agency holding a permit issued under the Act respecting detective or security agencies (chapter A-8), or a body having as its object the prevention, detection or repression of crime or statutory offences and a person carrying on an enterprise may, without the consent of the person concerned, communicate among themselves the information needed for conducting an inquiry for the purpose of preventing, detecting or repressing a crime or a statutory offence. The same applies in respect of information communicated among persons carrying on an enterprise, if the person who communicates or collects such information has reasonable grounds to believe that the person concerned has committed, or is about to commit, a crime or statutory offence against one or other of the persons carrying on an enterprise.²⁶

Investigators, licensed or otherwise, that have as their objective to prevent, detect or repress crime can communicate an employee's personal information amongst himself or herself without contravening the *Quebec Privacy Act*. Additionally, if a person in an enterprise believes, on reasonable grounds, that someone has or is about to commit a crime they can collect and communicate personal information without consent. Meaning personal information cannot be collected, without an employee's consent, for a policy violation or anything less than a statutory

²⁶ *Quebec Privacy Act*, *supra* s. 18.

crime in Quebec and a policy infraction or monitoring for productivity would not qualify. Although, it may be arguable that policy violations could be investigated under the guise of implied consent if they were to take place in common areas or of an inherently minor nature.

Section 7(1) of PIPEDA and s. 33(1) of the Ontario Privacy Draft authorize more collection of personal information from an employee without their consent than the *Quebec Privacy Act*. For example, s. 7(1)(b) of *PIPEDA*, allows employee investigators to collect information if consent would reasonably be expected to compromise the investigation.

7. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the employee only if...

(b) it is reasonable to expect that the collection with the knowledge or consent of the employee 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; [emphasis added]

Section 7(1)(b) of *PIPEDA* and s. 33(1) of the *Ontario Privacy Draft* both appear to allow the collection of personal information for a breach of contract. Although, many employee investigations encompass criminal activities, in regards to *PIPEDA*, this is not a requirement. Assuming an employer has a standard or specific employment contract, misconduct could fall within the purview of s. 7(1)(b) and conversely allow for a reasonable investigation without the subjects consent. However, this does prima facie appear to be over reaching and counter-productive for privacy legislation.

Section 26 of FOIPPA states that no personal information may be collected unless it is expressly authorized, it relates directly and is necessary for the operating or activity of the organization or it is collected for the purposes of law enforcement. In FOIPPA,

law enforcement is defined as:

- (a) policing, including criminal intelligence operation
 - (b) investigations that lead or could lead to a penalty or sanction being imposed,
- or
- (c) proceedings that lead or could lead to a penalty or sanction being imposed;

As any employee investigation could lead to a penalty or sanction, it becomes plausible that almost any employee investigation would fall within the definition of law enforcement. In addition, once information is exempted under FOIPPA an employer may also collect the information surreptitiously without disclosing their purpose, legal authority and privacy officer information. Even though on first glance the legislation appears to allow investigators a carte blanche approach to using personal information, it depends ultimately on the reasonableness of the use on a case-by-case basis. Privacy legislation is developed to protect employees from having their privacy rights violated, particularly when there is an imbalance of power. Although, it would appear that employers could use the above clause in FOIPPA for surveillance of employee productivity, this specifically contradicts the purpose of their enactment. Thus, even if it were done in a reasonable manner it would be inconsistent with the legislation to allow an employer to use video surveillance.

VII. USE OF EMPLOYEE INFORMATION

The use of the law enforcement exemption to obtain and use an employee's personal information without their consent is similar to the exemption employed in collection without consent. The Ontario Privacy Draft and PIPEDA deem it to be a reasonable violation only after all relevant factors are taken into account. The Quebec Privacy Act demands that it be a criminal offence and thus productivity surveillance would not exempt an employer from the requirement of obtaining consent. However, s. 18 of the Quebec Privacy Act requires that a notation be placed in the employee's file outlining the use of the law enforcement exemption and as such increasing the transparency of the law enforcement exemption. Section 7(2)(a) of PIPEDA says that personal information for which an employer does not have consent and did not collect in an investigation of a crime or breach of contract has to be useful for an investigation of a crime before it can be used by an investigator. This creates a higher threshold use of extrinsic information collected and used for secondary purposes. For example, information in a personnel file may not be available for an investigator's use if it is not in regards to a criminal investigation. Thus, if an employer had a credit report file on a manager for a company gas card, they could not use that information to determine suitability for promotion unless they acquired further consent. Most privacy legislation requires additional consent when the original use has changed. Section 7(4) of PIPEDA allows for information that was collected under s. 7(2) to be used for subsequent purposes without consent, as long as the use undertaken is consistent with law enforcement or from which a law enforcement proceedings is likely to result.

VIII. DISCLOSURE OF EMPLOYEE INFORMATION

It has been shown that an employer can collect and use an employee's information without their consent for law enforcement or even to investigate a possible breach of contract. The disclosure of the collected information to third parties or other employees is even more problematic than impermissible use or collection. During or after an investigation it is common for an investigator to disclose an employee's information to a third party for assistance or further enforcement. The question then becomes what personal information can be disclosed and to which third parties. In regards, to the CSA Privacy Principles and the British Columbia Special Committee they again defer the qualifications for disclosure to a general statement of a need for balance between personal privacy and business interests. They do however mention that if an employer is going to collect and use personal information it should be discarded after use. Disposal requirements will be further explored subsequently but this does imply that an employer should not have personal information to disclose after its purpose has expired. Section 18(3) of the Quebec Privacy Draft, states that an employer may disclose personal information without an employee's consent if it is to an organization responsible, by law, for the prevention, detection, or repression of a crime or statutory offence. Disclosure is also permissible if a person requires the information to perform their duties and it is necessary for a prosecution of an offence in Quebec. This would most likely entail police and governmental agencies. Section 18(4) of the same act also allows for disclosure without consent to a person that requires the information in the performance of their duties as long as their duties are necessary under the law or a collective agreement. This empowers an investigator to disclose personal information to other investigators if disclosure is part of duties that are outlined in legislation or a collective employment agreement. This suggests that union

employees with this type of employment agreement are at a distinct disadvantage as compared to nonunion workplaces.

FOIPPA and the Ontario Privacy draft refer to law enforcement or a contravention of a law as they did in the collection and the use of personal information. Thus, if an employer was justified in the collection or use of personal information they are also justified in its disclosure under s. 33(c) of FOIPPA. Consequently, an investigator working on an employee's file who discloses information to a municipal police force to determine if there may be criminal charges laid, would be authorized to do so under FOIPPA s. 33(n) or the Ontario Privacy Draft. They would also be authorized to disclose the information that could lead to a penalty or sanction being imposed under statute. This may allow an employer to show a picture of an employee to a witness to determine if the employee was not in the correct place working. This appears prima facie to be an unreasonable invasion of an employee's privacy. However, s. 33(f) of FOIPPA also allows an investigator to disclose personal information as may be necessary for the performance of their duties. Thus, an employee at the motor vehicle branch may disclose a persons' driving record to their manager if the manager's job was to ensure the employee had a clean driving record. The PIPEDA has the most onerous qualifications for disclosure of personal information without consent. Section 7(3) states that;

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the employee only if the disclosure is...

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

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a Province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or...

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

(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a Province or a foreign jurisdiction that has been, is being or is about to be committed, or

(h.1) of information that is publicly available and is specified by the regulations;

(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

(i) required by law.

(4) Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection (2).

Section 3 outlines that no personal information may be disclosed without consent unless the disclosure fulfills one of these requirements. The most notable part of the exceptions is that they do not contain the expansive categories of law enforcement, breach of contract or contravention of any law. Thus, personal information can only be disclosed to an investigative body or a governmental institution. *PIPEDA* has to date only given the 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 the title of investigative body. A list of government institutions is found within *PIPEDA* but they are generally federal institutions or divisions of federal works. As mentioned above, either *PIPEDA* is going to become the privacy

legislation for British Columbia or similar legislation will have to be enacted. Thus, an investigator would not be able to give information about a crime to the local police department if they were not the RCMP. Thus, it is possible for an employer to release personal information without consent under *FOIPPA* and still not be compliant with *PIPEDA*. Therefore, the new British Columbia private sector legislation may make disclosure by an employer more tedious to ensure compliance with *PIPEDA*. An employer would be best served to disclose only an employee's personal information without consent to further a significant employee investigation. The motto "need to know" would be a prudent policy when it comes to disclosure of personal information. In fact, many employers have stopped giving references and communicating any personal information to third parties, including the police, unless they are directed to do so by the law. This may be primarily out of fear of being sued for defamation but it is also prudent to privacy considerations.

It should also be noted that disclosure policies could be contravened by giving information to other employees within an organization. If an investigation is inconclusive or absolves the accused, should the information be disclosed to their supervisor? The current legislation suggests that once the investigation is resolved it is no longer exempt under the "law enforcement" exemption. A law enforcement investigation is not endless. Once the investigation is complete, regardless of outcome, the information should not be allowed to be disseminated any further. Thus, it would likely be in contravention of the legislation for an investigator to inform a supervisor of the results of an investigation in order to allow the supervisor to review other employment concerns. In fact, it is difficult to imagine a situation where an investigator would be permitted to disclose any personal information from an investigation to a person's supervisor.

IX. EMPLOYEE ACCESS TO THEIR PERSONAL INFORMATION

The right of an employee to access his or her own personal information is consistent throughout all Canadian privacy legislation, enacted or proposed, and may be akin to natural justice. As we have previously discussed, personal information is the information of the subject and therefore theirs to access. In an Ipso-Reid poll, eighty-four percent of British Columbians believed that a person should have access to their personal information and be able to make any corrections.²⁷ No matter why an employee requests access, an employer should be aware of what type of information can be requested and when must an employer comply. When an employer receives a request for access from an employee, they must reply. The privacy acts all have the same requirements for an access request. First, they must respond within thirty days unless they apply for another thirty-day extension. Generally, extensions are only given if the employer does not have care and control of the record, they cannot get it within thirty days or getting it within thirty days would cause an unreasonable strain on the organization. If they do not properly notify the applicant within thirty days, it is the same as if the employer has refused the request and the employee can act accordingly. An employer also has a duty to assist the employee upon their request. An employer has to make a copy of the record or allow for access to the records with little or no charge. The *CSA Privacy Principle* number nine states that an employee has the right to their own personal information with only a few specific exceptions, security being one of them. All of the legislation contemplates law enforcement in one regard or another but they individually expand on its usage. Additionally, third party information and concern for damage to third party privacy rights is also a disclosure exemption that may be applicable in an employee investigation. As most employee investigations entail surveillance of the subject and their

²⁷ *British Columbia Special Committee, supra* at p. 50.

interaction in common areas, an investigation may have third party information and some of it may be personal and damaging to other employees. Thus, the law enforcement and third party exemptions to requestor access for their information will be reviewed in the context of the relevant privacy legislations in Canada.

a. LAW ENFORCEMENT EXEMPTIONS FOR INFORMATION ACCESS

Law enforcement and third party exemptions to consent will be assessed with the *PIPEDA*, *Quebec Privacy Act*, and the *Ontario Privacy Draft* respectively. *FOIPPA* will be used to review these exemptions as well as a few more exemptions separately, as it is believed that these exemptions may be very applicable in the new private sector privacy legislation in British Columbia.

PIPEDA once again refers to s. 7(1)(b) for the definition of the law enforcement exclusion and the right of an employee to demand access of their personal information. It should be noted that in a past order of the Federal Privacy Commissioner he allowed an ex-employee of the Royal Bank to see their personnel files.²⁸ The order does not review why the employee wanted to see the file or why the employer attempted to deny access but it could be assumed that it was in regards to an alleged misconduct. As mentioned earlier, misconduct may be enough to qualify under the breach of a contract clause but as the Commissioner's orders show, it may not be applicable for employee files. If all breaches of employee / employer contracts created reasonable exemptions to disclosure then virtually all information in an employee's file would be

²⁸ *Bank accused of withholding information on former employee* (April 2002), Order #44 (O.P.C.C.) online: < http://privcom.gc.ca/cf-dc/cf-dc_020408_e.asp > (date accessed: 20 December 2002). [hereinafter *Bank and Former Employee*].

exempt and this would be patently unreasonable and inconsistent with the purpose of *PIPEDA*.²⁹ Therefore, if an employee wants access to their file and no charges were laid or contemplated, an employer would likely have to release it to the employee. *PIPEDA* also blends the law enforcement and third party exemptions in s. 2.4. *Section 2.4* states that if an organization disclosed personal information to a government institution for a particular investigative use then the organization may have to apply to the government institution for permission to acknowledge the disclosure. If the government institution denies access, the organization may not admit the existence of the record or that it was disclosed to anyone. This appears to, at worst, directly defy the *CSA Privacy Principles* 4.9.1 or at best, put the Federal Government above privacy laws and citizen's privacy rights.

However, s. 39 of the *Quebec Privacy Act* does speak to internal security or conduct on behalf of an employer when access would be likely to hinder the prevention, detection or repression of a criminal or statutory offence³⁰ or a judicial proceeding where either party has an interest.³¹ In both of these instances, the act allows for refusal but again does not demand it. This appears to deal with employees requesting their personal information when it was collected for an internal investigation and the access may be detrimental to the investigation. It does not however allow for the refusal of an employee's personal information when there was only a misconduct investigation or review unless it led to a current or future judicial proceeding. No matter the severity or result after an internal investigation, whether the police were involved or not, an employee would be able to access their personal information unless it could be shown the disclosure would harm the investigation. Thus, under the *Quebec Privacy Act* an organization

²⁹ *PIPEDA*, *supra* s. 3.

³⁰ *Quebec Privacy Act*, *supra* s. 39(1)

³¹ *Quebec Privacy Act*, *supra* s. 39(2)

may be able to deny disclosure of an open, active investigation but could not afford the same protections to a closed or stalled one.

The *Ontario Privacy Draft* outlines “law enforcement” very similar to *PIPEDA* so only the differences will be reviewed. The legislation outlines many different possibilities for reasons to allow exemption to access under s. 56(1). Some of these exemptions are overlapping and overbearing as the Federal Privacy Commissioner mentions in his review of the proposed legislation.

Subsection 56(1)(a) allows access to be refused if the information relates to the security or defence of Canada or the conduct of international affairs. Subsection 56(1)(b) allows access to be refused if the information relates to an investigative body enforcing or investigating the enforcement of a law or by-law. While I understand the intent of these two provisions, they raise certain concerns. First of all, I question how an organization will determine if information falls into these categories. A retailer, a charity or a health care practitioner is unlikely to have the expertise to determine if releasing certain information will threaten national security. If the information has been disclosed to a law enforcement agency or an investigative body, then subsections 56(1)(c) and 56(8) would allow access to be withheld and these provisions would not be needed.

It would appear from some of his recent speeches and orders that the Federal Privacy Commissioner is attempting to pare down some of the privacy legislation to be more reflective of the *CSA Privacy Principles*. It is not clear if the “breach of an agreement” clause in the law enforcement definition will be interpreted with a common language definition or a more specific and limiting interpretation as with Commissioner’s orders.³² The Retail Council of Canada has recently mentioned the same concern ‘Sections 33, 35 and 37 of PPIA [proposed privacy legislation in Ontario] allow for the collection of personal information where there is breach of

³² *Bank and Former Employee, supra.*

the agreement. However, “agreement” has not been defined and thus does not necessarily include an implied employment contract”³³ If the *Ontario Privacy Act* were to include an employment contract as a contract under the act then for all practical purposes it would be of little force and effect in regards to protecting employee’s privacy rights. Thus, it can be reasonably assumed that even if the British Columbia privacy draft has a similar clause, it will not exempt all information amassed that could lead to a breach of an employment contract.

b. THIRD PARTY EXEMPTION TO EMPLOYEE ACCESS

In a typical investigation, there may be interviews, video surveillance and spot checks or audits. On many occasions, the information attained is relevant to the investigation but also includes other employee’s’ or customers’ personal information. *Section 9(1) of PIPEDA* does not mention that the third party personal information has to be harmful or even reasonable to be excluded, but s. 9 falls under s. 5(1) and consequently the *CSA Privacy Principles*. Therefore, an employee’s right to access their information has to be balanced with a third party’s right to keep their information private.³⁴ This would have to be decided on a case-by-case basis and as many commissioners have decided, taking into account the sensitivity of the information and the severity of the possible consequences. Thus, it is plausible that a third party may have some of their personal information disclosed to ensure that the requestor applicant is able to adequately protect their rights. For example, if an employee was going to lose or did lose their job, their needs may take precedent over a third party’s fear of being embarrassed or ridiculed when if of their information is disclosed.

³³ Sharon E. Maloney, “Submission, Ontario Privacy of Personal Information Act”(2002) online: Retail Council of Canada Homepage < http://www.retailcouncil.ca/govrelations/ontario/submission_privacy.asp> (date accessed: 5 December 2002).

³⁴ *PIPEDA*, *supra* s. 9(2)(a)(i)

Whether *PIPEDA* directs or allows an employer to give an employee access to their personal information, the employee still has obligations under the *PIPEDA*. The various Canadian privacy legislations contain similar obligations and for that reason will only be evaluated once. Regardless if the employer is ordered or allowed to keep the information requested confidential, the employer has to write to the applicant explaining why the request was denied, under what authority it was denied and whom in the organization the employee can speak to about the denial. The employer also has to hold onto the information for as long as is necessary for the employee to exhaust any recourse.³⁵ Although, none of the legislation speaks to how long this entails, it could vary from thirty days to a year depending on the circumstances. It should be noted, that this has to be balanced with the fifth *CSA Privacy Principle*, which requires that the information should be destroyed after its original use has expired. Additionally, employers should create policies and procedures to ensure compliance. It is not enough for an employer to say that they have policies: an employer has to show that they enforce those policies.

Section 18 of the *Quebec Privacy Act* begins by stating that any employer with a file on an employee must acknowledge its existence to the applicant and communicate any personal information concerning him or her. Moreover, s. 39 of the *Quebec Civil Code*³⁶ on which the privacy legislation is based, expands of an employee's right of access to their information by stating;

39. A person keeping a file on a person may not deny him access to the information contained therein unless he has a serious and legitimate reason for

³⁵ *CSA Privacy Principles, supra.*

³⁶ *Civil Code of Quebec, S.Q., 1991, c. 64.*

doing so or unless the information is of a nature that may seriously prejudice a third person.³⁷

This only allows for denial of access for serious and legitimate reasons, as all legislation should reflect, such as serious harm to a third person.

Section 56(1)(i) of the *Ontario Privacy Draft*, states that information cannot be given to a requestor even if they are requesting their own personal information if the release of the information is likely to harm a third party's interests. This section ensures that an employer can only deny access to a employee's own information if the third party information cannot be severed. *Section 56(9)* then goes on to state that the employer has to write the employee stating that they received the request, what information was requested and that they will not be releasing the information to them without the third party's consent. Additionally, s. 57(17) asserts that if an employee is given their personal information, they should also be given the use and disclosure to other agencies with the file. This appears to be a practical attempt to balance the employee's rights to view their personal information with the third party's right to protect theirs.

The new private sector privacy legislation in British Columbia will presumably fall within the s. 30 exemption of *PIPEDA*. Presumably, it will also adopt many of the exemptions in *FOIPPA*, and thus *FOIPPA* will be examined with greater depth than the other Canadian privacy regimes. The purpose of the *FOIPPA* is to protect the privacy rights of British Columbians and to make public bodies more accountable for these protections while allowing them to be efficient.³⁸ This is done through legislative exemptions that balance an employee's rights with the public bodies'

³⁷ *Quebec Privacy Act, supra* s.39.

³⁸ *FOIPPA, supra* s. 2(1)(a) and s. 4(1)

need to function. *FOIPPA*, in the following sections, does not distinguish between the right of an employee to access their own information and the right of an employee to access someone else's personal information. This discussion is only concerned with exemptions that allow an employer to deny an employee's or potential employee's right to access their own information.

c. EXEMPTIONS TO EMPLOYEE ACCESS UNDER *FOIPPA*

Section 15 of *FOIPPA* allows a public body to refuse an employee access to information if they can fulfill the requirements of the subsections. Only the subsections that are applicable to an employee investigation will be reviewed. The applicable portions of s. 15 are

15(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

- (a) harm a law enforcement matter,...
- (c) harm effectiveness of investigative technique and procedures currently used, or likely to be used, in law enforcement,
- (d) reveal the identity of a confidential source of law enforcement information,
- (f) endanger the life or physical safety of a law enforcement officer or any other person,...
- (g) reveal any information relating to or used in the exercise of prosecutorial discretion,
- (l) harm the security of any property or system, including a building, a vehicle, a computer or a communications system.

Section 15(1)(a) is an exemption clause that encapsulates all possible criteria in law enforcement. However, this is a harm-based test and will be implemented as such. Law enforcement is defined by *FOIPPA* as anything where an employee can be assessed a penalty or fine. Obviously, this

includes criminal offences, but it does not necessarily include a breach of a contract or agreement. Under the current privacy regime, this could mean an employer may be authorized to deny an employee's request to access their personal information. The second part of s. 15 (1)(a) states that the law enforcement matter has to be harmed. Past *FOIPPA* orders have stated that in a harm-based test, harm diminishes the longer the investigation is closed. Even if the investigation is not closed, there has to be a substantial link between the disclosure and the harm to law enforcement. Thus, the subject of an internal investigation may be able to gain access to their file and investigation information, after the matter has been resolved.

The next provision in s. 15(1) of *FOIPPA* that may allow for refusal of access applicable to an internal investigation would be s. 15(1)(c). This provision allows an employer to deny access if it can be reasonably be expected to harm techniques and procedures of law enforcement. Assuming that the internal investigation is law enforcement, and then any disclosures that could hurt the techniques or procedures of the employee investigation could be denied access. This is also a harm-based test, and as such, the same application applies as with s. 15(1)(a) of *FOIPPA*. The *FOIPPA* Commissioners' orders have stated that for techniques and procedures to be exempt they have to be of a secret and/or a technical nature. For example, interviews have not fallen under this exemption even if the investigator used a specific interrogation technique.³⁹ It can be concluded that investigators' use of video equipment would not apply because it is common knowledge. An example, of an exemption under this subsection may include a DNA extraction technique used to catch criminals. Under s. 15(1) (d) of *FOIPPA*, any information that could reveal an investigator's confidential sources can be refused access. This could include, for example, a manager who revealed a confidential statement, or anything in a file that could allow

³⁹ *FOIPPA Employee Sexual Harassment, supra* at p. 8.

someone to identify an employee that was the subject of an investigation. *Section 15(1)(d)* and *(f)* are relatively straight forward exemptions. However, *s. 15(1)(g)* does not allow for an employer to refuse access to information unless it is the used for prosecutorial discretion. This has been deemed by the *FOIPPA* Commissioner to mean discretion under the *Crown Counsel Act*.⁴⁰ In other Provinces, it may include police officers as they have charge approval status, but in British Columbia only individual empowered as crown counsel can decide to charge, and thus only their reasons for approval or denial of a charge are included in *s. 15(1)(g)* of *FOIPPA*.

Information in an employee investigation file that could give insight into how to circumvent the security of an employer or its property can be denied access under *s. 15(1) (i)* of *FOIPPA*. This may include covert video surveillance if the employer could show that the location of the cameras could be surmised from viewing the videotape, and the location of the cameras is important to the security of the building or company. Notably, this is also test where the employer must prove that there is harm and that the harm wanes over time.⁴¹ Additionally, the head of a public body may refuse to disclose information to an employee if the information in the law enforcement record would reasonably be expected to expose the person who wrote information in the record or the person who was quoted or paraphrased to civil liability.⁴² Therefore, if someone was to utter a defamatory or negligent statement, the employer may be authorized to refuse access of the requested information.

⁴⁰ R.S.B.C. (1996). C. 87

⁴¹ *FOIPPA*, *supra* s. 57(1)

⁴² *FOIPPA*, *supra* s. 2(a)

However, a public body must allow access to their reasons not to prosecute if, after the police have finished their investigation, one of the involved parties makes such a request.⁴³ Involved parties could include employees, employees' friends, supervisors, peers, witnesses, and victims. This situation could arise when an employee has been fired and charged for theft and the police close the file or pass it on to Crown Counsel with neither pursuing it. This file can now be accessed by any of the interested parties listed or the public if the incident has become public knowledge. Notably, public knowledge can come from court records, organizational newsletters or the media.

Section 16 of FOIPPA pertains to the denial of access if the information would likely harm intergovernmental agency relationships. This is applicable because *FOIPPA* regulates public bodies and the act stipulates that public bodies' interaction should not be jeopardized by improper disclosure of records. It is realistic that private sector employers also enjoy relationships with public bodies or governmental agencies, and it may be necessary for employers to continue these relationships. Therefore, it is plausible that there may be a similar clause in the new legislation to mirror s. 16 of *FOIPPA*. This may well mean that any information an employer shares with other organizations or police agencies may be protected if allowing access could jeopardize the relationship. It should be noted that s. 19(1) (a) of *FOIPPA* contemplates refusal for access of information to an applicant if it may cause a threat to anyone's safety or anyone's mental or physical health. In many employee investigations, there is shock, disbelief, stress and anger created from the knowledge that a co-worker was dishonest. This is usually because the other employees knew the dishonest co-worker as a peer and could not imagine anyone doing such a thing. Although, these worries and emotions are real and should be

⁴³ *FOIPPA, supra* s. 15(4)(a)

addressed in a workplace, they do not allow an employer to refuse access to information. The *FOIPPA* Commissioners have repeatedly stated that the threat contemplated in s. 19(1)(a) has to be substantial. They specifically mention that stress and discomfort do not qualify as substantial threats to mental health.

d. *FOIPPA* AND THIRD PARTY EXEMPTIONS TO EMPLOYEE ACCESS

Privacy legislation has to attain equilibrium between competing interests. It is commonly between the employee's rights to control their information and the business needs of an employer that this equilibrium has to be maintained. In regards to third party information, however, the harmony that the legislation attempts to attain is between people and the use of their information. If both parties have the right to decide how to use their information, then what is the result when the information is indistinguishably intermingled? The legislation appears to look at the severity and sensitivity of the information and through this, the harm suffered by its approved access compared to its remaining confidential. Notably, the orders appear to err on the side of continued confidentiality for two reasons. First, if they are to err, they should do so in a way that can be corrected and avoid situations where once the information is accessed, it cannot be made confidential again. Second, privacy protection seems to take precedents over freedom of information rights. Ideally, privacy protection is the right to be left alone and freedom of information is the right to take control of something that is inherently yours. In light of this, the *FOIPPA* has adopted stringent restrictions on an employee getting access to their personal information when it is mixed with a third party's.

If the head of a public determines that allowing access to information would be an unreasonable invasion of a third party's personal privacy, it must be kept confidential.⁴⁴ Notably, the burden of proof is switched to the applicant and they have to prove that the access would not be an unreasonable invasion of a third party's privacy. As previously mentioned, the head of a public body has the responsibility of considering all relevant factors prior to making their decisions. The head of a public body may err on the side of caution in regards to releasing third party information. *Section 22(2)* of *FOIPPA* lists factors that the head of the public body must consider when deciding to allow access of a third party's information, including;

- 2) In determining under subsection (1) or (3) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether
 - (c) the personal information is relevant to a fair determination of the applicant's rights,
 - (f) the personal information has been supplied in confidence,
 - (h) The disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant,

If the information falls under s. 22(2)(c) and the access requested is relevant to an employee's rights then this information should be reviewed when assessing the request for access. The employee may be going through a hearing or applying for worker benefits, and the access could assist them in proving their case. In *FOIPPA* orders the Privacy Commissioner has deemed that an investigator cannot guarantee an informant's confidentiality; only the Commissioner and

⁴⁴ *FOIPPA, supra* s. 22(1)

FOIPPA can speak to this issue. However, the intentions of the interviewer's promise and the interviewee's belief are heavily weighed. When the promise of confidentiality is given, it does create a rebuttable presumption. *Section 22(2)(h)* of *FOIPPA* may arise in an investigation when a person who was interviewed comments on another employee and that comment may unfairly damage the third party's reputation. In the workplace, people have to see each other every day and rumor or innuendo can quickly damage a person's reputation. The key to this section is that the information must "unfairly" damage a person's reputation and is another variable that the head of a public body must take into account when deciding to allow an employee access to a third party's personal information.

X. AN UNREASONABLE INVASION OF THIRD PARTY'S PRIVACY

After all of the relevant factors have been reviewed, s. 22(2) of *FOIPPA* notwithstanding, the head of the public body has to review what is presumed to be an invasion of a third parties privacy as per s. 22(3):

22 (3) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if

- (b) the personal information was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent disclosure is necessary to prosecute the violation or to continue the investigation,...
- (d) the personal information relates to employment, occupational or educational history,
- (f) the personal information describes the third party's finances, income, assets, liabilities, net worth, bank balances, financial history or activities, or creditworthiness,

- (g) the personal information consists of personal recommendations or evaluations, character references to personnel evaluations about a the third party,
- (h) the disclosure could reasonably be expected to reveal that the third party supplied, in confidence, a personal recommendation or evaluation, character reference or personnel evaluation,...

This section of the *FOIPPA* outlines presumptions and but not sureties. If third party information falls within one of the above categories, it only creates a rebuttable presumption that can be refuted. However, as with all information in s. 22, the employee has the burden of proof and any presumptions makes access more onerous. For the most part, s. 22(3) of *FOIPPA* is self-explanatory. However, in s. 22(3)(a) a violation of law is a much more finite category than “law enforcement”, and so a misconduct investigation would not make access a presumed invasion of a third party’s privacy rights. This means that if there was information collected for the investigation of a crime, it would be presumed that access by an employee would be denied if the information was about a third party. It should be emphasized again, that this only creates a presumption and does not definitively mean that the information cannot be released.

Section 22(4) of *FOIPPA* categorizes instances when the access of information is not an unreasonable invasion of a third party’s personal privacy. There are two applicable subsections. First, subsection (a) allows for access in regards to a third party’s consent. Second, subsection (e) states that information regarding a third party’s position, function or remuneration as an employee would be subject to access. This could be in relation to a co-accused or a manager and the handling of a situation regarding one of their peers or subordinates. Lastly, *Section 22(5)* demands that an employer that does not allow access to personal information supplied in

confidence to an employee under s. 22, must supply the employee with a severed copy of the record unless it cannot be prepared without revealing the identity of the third party in question.

XI. WHEN AN EMPLOYEE AND THE EMPLOYER DISAGREE ON ACCESS

An investigator or a manager of investigators should know the possible consequences that an employer may suffer when an employee complains to the Privacy Commissioner about the lack of access. There will most likely be an independent authority overseeing the privacy sector and the private sector's compliance to the privacy legislation. Currently, an independent authority is necessary to comply with *PIPEDA* and *FOIPPA* and; seventy one percent of British Columbians believe it is important that it is part of the new legislation.⁴⁵ In *FOIPPA*, the Commissioner can order audits, seizures and fines to employers that are being investigated or are non-compliant. There is also an opportunity to appeal the Commissioner's ruling in court but only on a matter of law or jurisdiction, not fact. For example, if a privacy commissioner denies use of video surveillance or witness testimony but does so by using the proper judicial test, this ruling may not be subject to appeal. There are two different ways that privacy commissioners exercise their powers of compliance. The first is through an ombudsman format without powers to order compliance. The second way is through an officer of the legislature who can order compliance. The Federal Privacy Commissioner is an ombudsman and therefore cannot order compliance. If an employer does not comply with his orders and he feels that the issue is worthy, he can take them to Federal Court. The Federal Courts can award damages for privacy intrusions and humiliation. As there has not yet been a ruling that has awarded damages, there is no way to determine how large the awards may be. Although, the Federal Privacy Commissioner is

⁴⁵ *British Columbia Privacy Committee, supra.*

achieving a relatively large rate of compliance it would seem that the Provinces, particularly British Columbia, are inclining towards extending the provincial privacy model into the private sector. Thus, the Privacy Commissioner will most likely be an officer of the legislature. Whichever, format is used, there are certain standards that will be similar throughout. They include responsibility of an employer, fines, whistleblower protection, security, and accuracy.

XII. PERSON RESPONSIBLE FOR PRIVACY COMPLIANCE

All of the privacy legislation in Canada codifies the responsibility of an employer to designate a person responsible for ensuring that the employer complies with privacy requests. This person does not have to fulfill all of the requirements of the legislation but must ensure compliance. Additionally, the *FOIPPA* and Ontario *FIPPA* designate responsibilities and decision-making powers to the head of the public body to which they can delegate authority. For internal investigators, this may become relevant to how they conduct investigations. Before the Privacy Commissioner sees a privacy complaint, the employee is required to apply to the employer for access to their records and be denied. The person who will most likely make the access decision is the Privacy Manager. As anyone who has worked in a large organization, particularly in an investigation department, can attest to, different departments have different mandates. In some organizations, everyone works to one common goal, and in others, departments work against each other in an environment of “competitive decentralization”. For example, a human resources manager may not agree with an internal investigator in regards to the amount of information in an employee’s file that may be confidential and thus denied access. In fact, if an organization does not create a new privacy officer position, the duties will most likely be relegated to a human resources manager. The Privacy Manager may not understand or agree with the investigator’s

request to deny access, particularly, when the statute demands that the access be allowed. Therefore, when a section of privacy legislation allows for employee access, an investigator would be ill served to assume that their privacy officer would deny access of any information to applicant.

XIII. FINES

Provincial Privacy Commissioners are empowered to resolve privacy disputes through mediation and tribunals. However, when decisions are handed down, an employer must comply or risk being fined. The Quebec Privacy Commissioner can currently fine an employer up to ten thousand dollars for a first offence and up to twenty thousand dollars for any subsequent offences. The *FIPPA* or *FOIPPA* Commissioners can give fines up to five thousand dollars per offence. Notably, the *Ontario Privacy Draft* allows for employee fines up to fifty thousand dollars and non-employees fines up to two hundred and fifty thousand dollars. All employees that manage an organization can be held liable for the fifty thousand dollar fine, even if the organization is found not guilty of an offence under the act. Thus, it is reasonable to presume that the new British Columbia privacy legislation will emulate the provincial model as opposed to the federal model, and, as a result, the fines will be much higher than what is currently available. The large amounts that can be awarded under the *Ontario Privacy Draft* appear to be of a punitive or deterrent nature. The Federal Privacy Commissioner, in his critique of the draft, did not make any mention of the fines being disproportionate to offences under the act.⁴⁶ If, however, the British Columbia private sector privacy legislation does mirror the federal model

⁴⁶ George Radwanski, "A Consultation on the Ontario Draft Privacy of Personal Information Act" (2002) O.P.C.C.

then the large damage awards could come from the Federal Courts. *Section 16(6) of PIPEDA* allows for the courts to award damages for humiliation and; currently this is open to a wide interpretation. If the courts wanted to be punitive or create deterrents to noncompliance, the awards could be very large, especially if a large employer has humiliated an employee and the employee had to quit. The inherent imbalance of power in this relationship and the potential for humiliation to be widespread lends itself to a large amount of damages being awarded.

XIV. WHAT PROTECTIONS WILL WHISTLEBLOWERS HAVE?

Provincial privacy legislations are silent to whistle blowing protections. However, s. 27 of *PIPEDA* ensures confidentiality and protection of employees who disclose contraventions or refuse to contravene the privacy act. The employer is prohibited from dismissing, suspending, demoting, disciplining, harassing or generally disadvantaging any employee who is doing or the employer believes the employee will do any of the afore-mentioned actions.⁴⁷ In *PIPEDA*, the term employee also includes independent contractors.⁴⁸ If a person knowingly contravenes this section, obstructs the commissioner or destroys a record that is the subject of a request, they can be found guilty of an indictable offence and can be fined up to one hundred thousand dollars. This ensures that co-workers would be able to pass on information that could not be conclusively proved to the Commissioner, without the fear of retribution from their employer, regardless of the confidentiality of the information. The *Ontario Privacy Draft* also states that an employee cannot be disadvantaged for doing or not doing anything, they believe would be in contravention of the act. If an employer does disadvantage a whistle blower, they are subject to the above-mentioned fifty thousand dollar fine. It is most likely that the proposed private sector privacy

⁴⁷ *FOIPPA* s. 27.1(1)

⁴⁸ *PIPEDA* s 27.1(3)

legislation for British Columbia will include a whistleblower clause for employees or at least a fine for disadvantaging a person who acts on behalf of the statute. However, the *Quebec Privacy Act* does not have a protection for employees that take action on behalf of the legislation and it has been approved as substantially similar to *PIPEDA*. Therefore, the British Columbia privacy legislation may not include compliance protection but for practical reasons will probably have some form of whistleblower protection.

XV. SECURITY

An employer is responsible to ensure that all personal information under their control is secured from unauthorized access. As per *CSA Privacy Principle 4.7.3*, these protections should include

- (a) physical measures, for example, locked filing cabinets and restricted access to offices;
- (b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
- (c) technological measures, for example, the use of passwords and encryption

The *Ontario Privacy Draft* and the *Quebec Privacy Act* also reflects the measures in principle 4.7.3. Additionally, the amount of security that is needed depends on the type of information and particularly the sensitivity of the information. It also falls to an employer to ensure that the information they give to a third party under contract is kept as secure as if it was still under the care and control of the originating employer. Furthermore, an employer must ensure that all of their employees are aware of the security procedures and make certain of the confidentiality of information⁴⁹ and that only employees that require access to the information for the performance

⁴⁹ *PIPEDA*, *supra* Schedule 1.

of their duties are permitted access.⁵⁰ If an employer does not have adequate arrangements with sufficient communications, they could be found in contravention of the privacy legislation and subject to fines.⁵¹

XVI. ACCURACY

Regardless of why an employee wants to ensure that their personal information remains accurate, an employer has to accommodate them. Employers make life-altering decisions about employees everyday and these decisions are based on information that employers have. Inaccurate information can be seriously damaging to an employee. An employer has a responsibility to ensure that all information they use or disclose is accurate. In s. 11 of the *Quebec Privacy Act* states that everyone who has control of a employee's file must ensure that it is up to date and accurate prior to accessing it. The *Ontario Privacy Draft* demands that an employer take reasonable steps to ensure that it does not have or use inaccurate information.⁵² It also states that an employer shall not update an employee's file unless updating is required in order to fulfill the purpose in which it was collected unless the employee requests it is updates.⁵³ This creates a situation where an investigator must either have a file open for a specific reason, or the file should be closed and not accessed until another specific incident arises. However, it is also a mandate of some privacy regimes that once personal information has been used and is not currently needed, it should be destroyed. Hence, when an employer ceases to use personal information, it should be destroyed after the use is completed; or if action was taken because of

⁵⁰ Ibid.

⁵¹ *Collection and Use of Electronic Signatures by Courier Company* (September 2002), Order #71 (O.P.C.C.) online: < http://privcom.gc.ca/cf-dc/cf-dc_020905_e.asp > (date accessed: 20 December 2002).

⁵² *Ontario Privacy Draft*, *supra* s. 49(1)

⁵³ *Ibid* s. 49(2)

the information then the employer should wait until the employee has had a reasonable time to request the access of the information.⁵⁴

XVII. AN OVERVIEW: Video Surveillance to Monitor Employees

In the modern era, everything can be videotaped. The “caught on tape” and reality shows beam pictures and stories around the world. Videotaping has become very intrusive, particularly in the workplace where the subject cannot avoid the unblinking gaze of the video camera. Many facets of the proposed private sector privacy legislation will affect how an employer runs its employee investigations. The pertinent privacy legislation in Canada has been used to predict how a private sector privacy statute may affect employers collecting, using, disclosing and allowing access when they are doing employee investigations. The use of video surveillance by employers in employee investigations allows for an overview of best practices and an amalgamation of the practical ramifications of private sector privacy legislation in British Columbia. The review will focus on video surveillance of employees, but many of the principles are universal to all types of evidence acquired in investigations and can be applied as such.

Firstly, as outlined in the *Alberta Wheat Pool v. Grain Workers' Union, Local 333* [hereinafter *Alberta Wheat Pool*]⁵⁵, video surveillance in the workplace, without consent, has been considered invasive and requires special consideration and due diligence.

In reference to the employee/employer relationship, there is a line of authority from both judicial and arbitral jurisprudence which generally holds that conducting surveillance on an employee and videotaping his or her conduct without knowledge or consent will amount to a breach of the employee's right to privacy, unless such

⁵⁴ *Ibid* s.52(1)

⁵⁵ (1995), 48 L.A.C. (4th) 332. at p. 7.

intrusive conduct can be demonstrably justified by the employer.
The onus of establishing that justification rests with the employer.

If an employer is going to collect, use or disclose records of an employee they have to first decide what type of consent is necessary. In many situations, there may be implied consent if the records are collected as part of a standard, non-intrusive practice. For example, consent can be reasonably implied if an employee parks a company car in the company parking lot under constant and overt video surveillance. The employee would most likely welcome the protection for the company automobile and themselves since they are parking under the camera by choice. If, however, an employer had a private investigator follow the employee around videotaping them while they were making sales calls in the company car, the employer could not suggest that the employee consented to being videotaped by driving the company car or not complaining, particularly since they were not aware of the intrusion. Additionally, some employers believe that videotaping an employee for productivity reasons is not intrusive and that by working, the employee consents to being taped. This would most likely not qualify as consent for a variety of reasons. First, video surveillance has been consistently found by the courts to be highly intrusive and sensitive, particularly in an environment where an employee has little choice but to work. Thus, to get an employee's consent for overt video surveillance, an employer would likely have to get the employee to agree to the exact type, duration and use of the video. To say that someone consented because they did not quit or complain is reverse onus consent and frowned upon by privacy commissioners.

Another way an employer could attempt to deal with the problem of consent when videotaping employees could be to use specific consent forms within a union or employment contract, which included the specific type of surveillance. This still may be deemed unsatisfactory for the

purposes of consent because even if it is knowledgeable consent, it has to be freely given. As mentioned above, there is an inherent imbalance between employee and employer, particularly when a person is applying for a position. This imbalance may be alleviated by making the consent optional (although, it could be argued that a person may consent for fear of repercussions) or as part of a union contract where the two parties, employer and union, are equal. The *Ontario Privacy Draft* attempts to legislate this principle by stating that consent cannot be given in exchange for a product or service and particularly the service of employment. Therefore, it may be difficult for an employer to get valid consent to surreptitiously videotape their employees. Especially since most employees would prefer not to be monitored if given a real choice.

As mentioned above, an employer may not be able to collect, use or disclosure an employee's personal information unless there is an exemption to consent. The "law enforcement" exemption is relatively large and will likely include employee investigations. However, even if the exemption does fall under the exemption, it still must meet the reasonable person test. A reasonable rationale for video surveillance may include ensuring proper safety procedures, deterring external theft or robbery, deterring vandalism and in some cases increasing productivity. There have to be valid reasons for productivity surveillance or every inch of a workplace could be under constant video scrutiny. The question is when can an employer use video surveillance to protect their assets? A camera does not distinguish between significant events, like theft and constant intimidation through observation. Moreover, when is an employer justified in putting up a camera? If they are justified, how many cameras are justified and for how long? If there are legitimate reasons that can be understood by employee and employer alike

then there is no reason an employer cannot get the consent of an employee. An employer needs to be profitable to survive and an employee requires a place to work. If video surveillance can be explained and justified to the reasonable employee, then getting consent should not be a problem. However, in the real world, some employees are dishonest and some employers are paranoid. That is why consent is rarely going to be given for video surveillance and privacy legislation has exemptions to getting consent.

The former British Columbia Privacy Commissioner, David Flaherty, and the current Federal Privacy Commissioner use specific criteria that have to be met to ensure video surveillance is used reasonably. This criterion was developed through arbitration cases involving video surveillance and employee dishonesty. In his speech on Feb. 13, 2002, the Federal Privacy Commissioner outlined the four specific criteria for proper video surveillance. First, prior to use of video surveillance, it has to be shown that it is demonstrably necessary to address the specific problem. This means that video surveillance should be used discriminately or not on a “fishing trip” to see what evidence can be gathered after an incident has occurred. Thus, if an employee charged that an employer contravened a privacy act while performing an investigation, the employer would have to supply substantial evidence as to why they put up a camera, especially a covert camera, to comply with the privacy act. A gut instinct would not suffice. For example, if a manager of a warehouse noticed that stock of a particular expensive part was missing, he would most likely be in contravention of the privacy legislation if he put up a covert camera over the night watchman’s break area. There is no evidence to justify this intrusion. The part could have gone missing in the daytime, or it could be a clerical error. Second, the employer would have to show that the video is likely to be effective. This means that the employer would have to show

that the camera could catch the employee's dishonesty or stop the vandalism. The camera over the night watchman would not be an effective use of video surveillance. If the watchman is taking the parts, there is no reason to believe he would take them out on his break and get caught on camera. The camera is not even a good deterrent to theft because it is covert. Third, the invasion of privacy has to be proportional to the security benefit derived. As covert video surveillance of an employee is a highly intrusive invasion of a person's privacy, the benefit to security or the employer has to be great. Attempting to catch a person committing minor misconduct through covert video surveillance may be deemed a contravention of their employee's privacy rights. Is the videotaping of the guard on his break an invasion disproportionate to the loss of stock? It may not be, but it could be argued that the guard has a reasonable expectation of privacy on his break. There is no reason to believe that the video surveillance would be successful. Lastly, and most problematic, an employer must show that there is no less invasive measure available. In the example with the night watchman, when the employer noticed the parts missing they may not have been justified in using video surveillance if increasing the protection of the missing goods is an option. Additionally, if an employer has evidence that an employee is being dishonest, the employer's first course of action should be to talk to the employee or to eliminate his or her opportunity to be dishonest.⁵⁶ It is a legal requirement that entrapment not be used as a substitute for a thorough and proper investigation.⁵⁷ This may be a good rule of thumb for video surveillance as well. The balance between the privacy rights of an employee and the needs of an employer is not equal and as per the Commissioner's criteria, an employer should ensure that they only invade an employee's privacy for specific, justifiable purposes and in the least obtrusive manner possible. In regards to

⁵⁶ *Alberta Wheat Pool*, *supra* p. 8.

⁵⁷ *R. v. Mack* (1988), 44 C.C.C. (3d) 513.

disclosure, an employer should only disclose video evidence to the parties that are necessary to achieve the ultimate “law enforcement” goal. Lastly, it would appear from privacy orders that an employee is permitted access to video that contains their personal information after the investigation is complete. This could be very important for an employer to remember when installing cameras. Videotape is a record of a person and that person can request access to the tape and once they have the tape they can show to whomever they like, including the media or judiciary. As an investigator, it is a good rule of thumb to assume that an employee will eventually have access to an investigation file and act accordingly.

XVIII. CONCLUSION

In conclusion, information about a person belongs to them and should be treated as such. An employer who collects, uses or discloses an employee’s personal information should be cognizant of this and the need to acquire an employee’s informed consent without coercion. It would appear that consent in regards to employee investigations is always going to be questionable. The private sector privacy legislation in British Columbia will have to permit the employer to function efficiently, and this will most likely be achieved through exemptions from consent requirements. Law enforcement exemptions are most likely going to be the exemptions most commonly used to allow employers to investigate employees and still comply with the legislation. A law enforcement exemption from consent requirements must be exercised with due caution if it is to be held valid. As with all good legislation, reasonable use and application is the essential element. If an employer is truly empathetic to the needs and concerns of their employees and use common sense, they will most likely comply with the new private sector privacy legislation in British Columbia.