Employee Monitoring in the Private Sector:

In Search of a Balanced Approach to Privacy Rights and Consent

Ryan Leggett

Table of Contents

I. INTRODUCTION

The COVID-19 pandemic has rapidly changed the nature of how people work. Monitoring the activities of employees is not a new idea for employers, but employers may be exploring new avenues for monitoring their workforce in a world where the employment relationship is shifting, and remote work is more common. Employers must first recognize that employees generally have a reasonable expectation of privacy with respect to personal information in the workplace.[1] As a result, employers do not have unharnessed abilities to monitor their employees in any manner that they desire.

Consent is a cornerstone of current Canadian private sector privacy legislation. There is no dispute that allowing individuals to exercise control over the collection of their personal information is valued and valuable. Despite this point, individual rights to privacy are not absolute. With respect to monitoring employees through the collection and use of their personal information, Canadian privacy legislation that has eliminated the consent requirement in certain employment-specific situations has resulted in adequate privacy protection for employees, while balancing the needs of organizations to run effective businesses.

This paper will focus on the extent to which private sector privacy legislation allows employers to monitor their employees through collection and use of their personal information. Private sector privacy statutes in Canada provide rules for the collection, use, and disclosure of employees' personal information.[2] As will be discussed below, most forms of employee monitoring involve the collection and use of personal information. This paper will focus specifically on the relevant rules under the federal *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"),[3] and the *British Columbia Personal Information Protection Act* ("BC *PIPA*").[4]

Part II of this paper begins by laying out the legal frameworks of *PIPEDA* and BC *PIPA*, focusing specifically on laws concerning monitoring and surveillance of employees, and highlighting the similarities and differences between *PIPEDA* and BC *PIPA*. Part III will then assess how the law has been applied in practice and highlight how the differences in *PIPEDA* and BC *PIPA* have resulted in slightly different applications of the law. Part IV will discuss how allowing employers to collect personal information from employees without consent is reasonable. Such collection without consent also makes consent requirements in the legislation more clearly defined, thereby meeting the reasonable expectations of employees and employers. Lastly, Part V will assess whether monitoring benefits employers by assessing the impacts of monitoring and surveillance on employees. This paper posits that collecting employee personal information can be reasonable *at law*, depending on the extent of surveillance. Although employee monitoring can be reasonable, employers should recognize the potential effects of monitoring and surveillance on their employees, and ensure that they appropriately balance employee rights and desires for privacy with organizational efficiency.

---

[1] See *R v Cole*, 2012 SCC 53.
[2] See Michael Power, *The Law of Privacy*, 2nd ed (Toronto: LexisNexis Canada, 2017) at 241.
[3] SC 2000, c 5 [*PIPEDA*].
[4] SBC 2003, c 63 [*BC PIPA*].

II. LEGAL FRAMEWORK: FEDERAL *PIPEDA* AND BC *PIPA*

A. Introduction: General Similarities and Differences

The rules around the collection and use of personal information are similar in *PIPEDA* and BC *PIPA*. Currently, both BC *PIPA* and *PIPEDA* contain provisions that allow for the collection and use of employees' personal information without consent for limited purposes, which will be discussed below. This was not the case prior to 2015 when *PIPEDA* treated all personal information, including information of employees, identically ("Pre-2015 *PIPEDA*"). Relative to Pre-2015 *PIPEDA*, BC *PIPA* provided a broader scope for employers to collect and use employee personal information in managing the employment relationship. This provided greater clarity to both employers and employees with respect to how employers could monitor employees through collection and use of personal information. After the 2015 amendments, *PIPEDA* provides a similar scope for employee monitoring as BC *PIPA* ("Post-2015 *PIPEDA*").

A key element of private sector legislation with respect to employees' personal information is striking a balance between an employer's need to manage their workforce, and employees' individual privacy rights. Accordingly, interpretation of both *PIPEDA* and BC *PIPA* is informed by their legislative purposes. These purposes include the protection of individuals' personal information and commercial organizations' ability to collect, use, and disclose personal information for reasonable and appropriate purposes. As a result, interpreting both statutes requires striking a balance between individual privacy rights and organizational needs to collect and use personal information for commercial purposes.[5]

Lastly, both *PIPEDA* and BC *PIPA* contain the following general exclusions that are not covered by the legislation:

1. Personal information collected, used, or disclosed for purposes that are purely personal or domestic;[6]
2. Personal information collected, used, or disclosed for journalistic, artistic or literary purposes;[7]
3. Personal information to enable an individual at a place of business to be contacted;[8] and
4. Work product information related to an individual's employment that is prepared or collected by those individuals.[9]

---

[5] See *PIPEDA, supra* note 3, s 3; *BC PIPA, supra* note 4, s 2; see also Barbara von Tigerstrom, *Information and Privacy Law in Canada* (Toronto: Irwin Law Inc., 2020) at 296.

[6] See *BC PIPA, supra* note 4, s 3(2)(a); *PIPEDA, supra* note 3, s 4(2)(b) contains a similar exclusion, but applies only to the collection of information by individuals.

[7] See *PIPEDA, supra* note 3, s 4(1)(c); *BC PIPA, supra* note 4 s 3(2)(b).

[8] See *PIPEDA, supra* note 3, s 4.01; *BC PIPA, supra* note 4, s 1 "contact information," "personal information" (a).

[9] *BC PIPA* explicitly excludes work product information from the definition of "personal information." Conversely, *PIPEDA* allows for the collection of personal information without the knowledge or consent of an individual where it was produced by the individual in the course of their employment, business or profession and the collection is consistent with the purposes for which the information was produced. This operates as an exception from the knowledge and consent requirements under *PIPEDA*, but the effect is similar to the exclusion in *BC PIPA*. In *BC PIPA,* "work product information" is not subject to any sections of the Act. Conversely, in *PIPEDA,* this information

B. *PIPEDA*

i. Scope

Part 1 of *PIPEDA* governs the protection of personal information in the private sector but does not apply to all private sector employers in Canada. *PIPEDA* applies to private sector organizations that collect, use, or disclose personal information in respect of commercial activities, and to federal works, undertakings, or businesses. Federal works, undertakings, or businesses means any activity within the legislative authority of Parliament, including maritime navigation, interprovincial railways, airlines, airports, banks, broadcasting, telecommunications, interprovincial or international trucking, shipping or other transportation, and nuclear energy.[10]

Provinces that have enacted "substantially similar" private sector privacy legislation are exempt from the collection, use, and disclosure requirements under *PIPEDA*.[11] Despite these exceptions, *PIPEDA* still applies to any federal works, undertakings, or businesses in those provinces. Currently, only British Columbia, Alberta, and Quebec have implemented substantially similar legislation.[12] In the remaining provinces, no private sector privacy laws apply to private sector employment relationships that fall outside the scope of *PIPEDA*. Despite the absence of privacy laws, certain privacy issues may still be governed through other means such as collective agreements, employment standards legislation, and the *Charter*.

ii. What is Personal Information?

PIPEDA governs the collection and use of personal information that is "about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."[13] Three terms require further consideration to determine the scope of this provision: (1) "organization;" (2) "federal work, undertaking or business;" and (3) "personal information." An "organization" governed by *PIPEDA* is defined broadly to include, but is not limited to, an association, partnership, person and a trade union.[14] As explained above, "federal work, undertaking or business" means any activity within the legislative authority of federal Parliament.[15]

PIPEDA defines "personal information" as information *about* an *identifiable individual*.[16] This is similar to the definition in BC *PIPA*, except BC *PIPA* expressly includes employee personal information.[17] Information is "about" an identifiable individual where it reveals something about

---

would be subject to the Act, but could be collected or used without the employees' consent. *BC PIPA, supra* note 4, s 1 "personal information" (b), "work product information"; *PIPEDA, supra* note 3, ss 7(1)(b.2), 7(2)(b.2).

[10] See *PIPEDA, supra* note 3, s 1 "federal work, undertaking or business"; see also Power*, supra* note 2 at 242.

[11] See *PIPEDA, supra* note 3, s 26(2)(b).

[12] See *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374*; Organizations in the Province of Alberta Exemption Order*, SOR/2004-219; *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220.

[13] *PIPEDA, supra* note 3, s 4(1)(b).

[14] *Ibid* s 2(1).

[15] *Ibid.*

[16] *Ibid.*

[17] See *BC PIPA, supra* note 4, s 1 "personal information."

the individual's identity, characteristics, or activities.[18] Personal information is about an "identifiable individual" "where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information."[19] This definition means that even information that does not directly identify individuals can be personal information if it can identify individuals in combination with other accessible information.[20]

Personal information about employees can exist in a variety of forms. The Office of the Privacy Commissioner of Canada has found the following information, among other forms, to constitute personal information about an employee:

1. Performance appraisals;[21]
2. Internal investigation files;[22]
3. Employee number and employee voices;[23]
4. Video footage; [24] and
5. GPS in a company vehicle.[25]

The 2015 amendments to *PIPEDA* made a key change with respect to the collection and use of employees' personal information. The addition of section 7.3 brought Post-2015 *PIPEDA* in line with BC *PIPA*. Section 7.3 reads as follows:

> 7.3 In addition to the circumstances set out in section 7, for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, a federal work, undertaking or business may collect, use and disclose personal information without the consent of the individual if
>
> (a) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the federal work, undertaking or business and the individual; and

---

[18] See von Tigerstrom*, supra* note 5 at 302; see also *British Columbia Hydro and Power Authority v British Columbia (Information and Privacy Commissioner)*, 2019 BCSC 2128 at para 67 (this case concerns "personal information" under the BC *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, which defines "personal information" in a similar manner as in *PIPEDA*).

[19] *Gordon v Canada (Minister of Health),* 2008 FC 258 at para 34 (this case incorporates the definition of "personal information" from the *Privacy Act,* RSC 1985, c P-21, which is virtually identical to the definition of "personal information" in *PIPEDA*.

[20] See von Tigerstrom, *supra* note 5 at 305.

[21] See *Employer accused of wrongful disclosure, PIPEDA* Case Summary #2003-198, 2003 CanLII 44917 (PCC).

[22] See *Telecommunications company asked to adopt consistent retention practices*, *PIPEDA* Case Summary #2002-73, 2002 CanLII 42331 (PCC).

[23] See *Individual denied access to personal information*, *PIPEDA* Case Summary #2003-149, 2003 CanLII 42240 (PCC).

[24] See *Eastmond v Canadian Pacific Railway*, 2004 FC 852 [*Eastmond*].

[25] See *Use of personal information collected by Global Positioning System considered, PIPEDA* Case Summary #2006-351, 2006 CanLII 42313 (PCC) [*PIPEDA GPS Case*].

> (b) the federal work, undertaking or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.

Unlike Pre-2015 *PIPEDA*, federal employers can monitor employees without their consent only where it is performed for the purpose of establishing, managing, or terminating an employment relationship. Subsection (b) requires the employer to provide notice of the collection or use.

iii. Valid Collection and Use: Reasonableness Requirement

Reasonableness "is a guiding principle that underpins the interpretation of the various provisions of *PIPEDA*."[26] Employers must collect and use personal information in accordance with the rules in Part 1 of *PIPEDA*, and Schedule 1 to the Act. Subsection 5(1) of *PIPEDA* reads "Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1."

A key principle guiding employer conduct is that organizations must collect, use, and disclose personal information only for reasonable and appropriate purposes, and only to the extent necessary to fulfil those purposes.[27] This obligation is in addition to consent requirements. Further to the reasonableness requirement, the collection of personal information must be limited in type and amount to what is necessary to fulfill the organization's identified purposes.[28] This means that collection or use beyond the scope of the employer's reasonably identified purposes will be invalid. Collection may be excessive, and therefore beyond the extent necessary to fulfill the organization's stated purposes, where the collection is not effective in meeting the stated purpose, or where the purposes could be achieved using less information, or less sensitive information.[29] Employers must therefore limit monitoring so as to only collect information necessary to achieve their objectives.

A contextual approach that balances the individuals' and organizations' interests is necessary when determining whether an organization's purposes are reasonable or appropriate and whether the collection or use is justified.[30] *Eastmond v. Canadian Pacific Railway* established a legal framework for determining whether collection or use of personal information is reasonable, integrating the balance between individual and organizational interests, as follows ("*Eastmond*"):

1. Is the measure demonstrably necessary to meet a specific need?
2. Is the measure likely to be effective in meeting that need?
3. Is the loss of privacy proportional to the benefit gained?
4. Is there a less privacy-invasive way of achieving the same end?[31]

---

[26] *R v Spencer*, 2014 SCC 43 at para 43.
[27] See *PIPEDA, supra* note 3, s 5(3).
[28] *Ibid,* Schedule 1, cls 4.4 and 4.4.1.
[29] See von Tigerstrom, *supra* note 5 at 346.
[30] *Ibid* at 343.
[31] See *Eastmond, supra* note 24, at para 127; see also *PIPEDA GPS Case, supra* note 25.

iv. Valid Collection and Use: Consent Requirement

The knowledge and consent of individuals being monitored must be obtained to collect or use personal information, "except where inappropriate."[32] Exceptions to consent are only available if an enumerated exception in section 7 is met.[33] Consent must normally be obtained at or before the time of collection, and there is an onus on organizations to make a reasonable effort to advise individuals of the purposes for which the information will be used. The purposes must be stated in a manner that allows the individual to reasonably understand them.[34] Consent must be meaningful in the sense that consenting employees must understand specifically what they are consenting to.

Organizations may obtain consent in different ways, depending on the circumstances and the type of information collected. Organizations should obtain express consent when information is likely to be considered sensitive. Conversely, organizations can obtain implied consent when the information is less sensitive.[35] In obtaining consent, the reasonable expectations of the individual are also relevant.[36] In the context of implied consent, this principle suggests that consent should only be implied for the purposes which the employee could reasonably expect that the information would be used.[37]

As mentioned above, the 2015 amendments to *PIPEDA* introduced an exception to consent when personal information is obtained to establish, manage or terminate an employment relationship.[38] This exception did not exist under Pre-2015 *PIPEDA*. As a result, organizations governed by Pre-2015 *PIPEDA* had to obtain consent or meet the broad exceptions to consent under section 7. These exceptions apply to the collection and use of all personal information. Few exceptions under section 7 appear to be directly applicable to situations where employers may wish to monitor the performance of their employees.

Two section 7 exceptions that have been used to collect employees' personal information are as follows:

1. The collection or use is clearly in the interests of the individual and consent cannot be obtained in a timely manner;[39] and
2. Collection or use without consent for the purposes of an investigation where obtaining consent is reasonably expected to compromise the investigation. The relevant investigation must be of a "breach of an agreement or a contravention of the laws of Canada or a province."[40]

In the first exception, the Federal Court of Appeal has interpreted "in a timely manner" to suggest that the exception only applies in exceptional and temporary circumstances, such as where the

---

[32] *PIPEDA, supra* note 3, Schedule 1, cl 4.3.
[33] *Ibid,* ss 7(1) and 7(2); see also *Eastmond, supra* note 24 at paras 183-186.
[34] See *PIPEDA, supra* note 3, Schedule 1, cls 4.3.1 and 4.5; Schedule 1, cl 4.3.2.
[35] *Ibid,* Schedule 1, cl 4.3.6.
[36] *Ibid,* Schedule 1, cl 4.3.5.
[37] See *PIPEDA GPS Case, supra* note 25.
[38] See *PIPEDA, supra* note 3, s 7.3(a).
[39] *Ibid,* ss 7(1)(a) and 7(2)(d).
[40] *Ibid* ss 7(1)(b) and 7(2)(d).

individual cannot be contacted prior to collection of personal information.[41] It would be rare to categorize employee monitoring under this exception. The second exception requires some evidence or a reasonable belief that a breach of an agreement or laws may occur or have occurred, rather than mere suspicion, before collection of personal information without consent can be justified.[42] This exception appears applicable in the context of disciplinary action against an employee, but is generally not applicable to monitoring employees for other purposes.

C. BC *PIPA*

i. Scope

BC *PIPA* applies to private sector "organizations" within the province, which include a person, unincorporated association, trade union, trust or not for profit, and explicitly excludes a public body.[43] Any collection, use, or disclosure of personal information to which *PIPEDA* applies is excluded from BC *PIPA*'s scope.[44]

ii. What is Personal Information?

Personal information means information about an identifiable individual, including employee personal information, but does not include contact information or work product information.[45] In *Re Schindler Elevator Corporation* ("*Schindler*"), the BC Privacy Commissioner adopted the following interpretation of the meaning of personal information:

> "...'personal information' is information that is reasonably capable of identifying a particular individual, either alone or when combined with other available sources of information, and is collected, used or disclosed for a purpose related to the individual."[46]

The Privacy Commissioner also noted that personal information is not restricted to information about an individual's personal life, and can encompass information about the individual in their employment or professional capacity.[47]

iii. Employee Personal Information

BC *PIPA* and Post-2015 *PIPEDA*'s unique treatment of employee personal information marks a significant departure from Pre-2015 *PIPEDA*'s legislative framework. BC *PIPA* defines "Employee personal information" as follows:

> personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment

---

[41] See *Wansink v Telus Communications Inc*, 2007 FCA 21 at para 27 [*Wansink*].
[42] See von Tigerstrom, *supra* note 5 at 361.
[43] See *BC PIPA, supra* note 4, s 1 "organization."
[44] *Ibid,* s 3(2)(c).
[45] *Ibid,* s 1 "personal information."
[46] *Re Schindler Elevator Corporation,* Order P12-01, 2012 BCIPC 25 (CanLII) at para 85, [2012] BCIPCD No 25 (QL) [*Schindler*].
[47] *Ibid* at paras 83-84.

> relationship between the organization and that individual, but does not include personal information that is not about an individual's employment.[48]

In Order P06-04, the BC Privacy Commissioner established the following framework for determining if information qualifies as employee personal information:

1. The information must be "personal information";
2. The personal information must be collected, used or disclosed "for the purposes reasonably required" to establish, manage or terminate an employment relationship between the organization and that individual;
3. the personal information must be collected "solely" for those purpose(s); and
4. The personal information must not be "personal information that is not about an individual's employment".[49]

Employers have the right to collect and use employee personal information without consent for the purposes of establishing, managing or terminating an employment relationship between the organization and individual.[50] If an employer chooses to collect or use employee personal information for those purposes, they must notify an individual that it will be collecting or using the information, and advise the individual of the purposes for collection or use prior to proceeding without consent.[51] Valid notice requires outlining the types of information to be collected or used with some specificity so that employees are aware of the types of information being collected, uses for that information, and purposes for collection and use.[52]

iv. Collection and Use of Employee Personal Information: Reasonableness

The dominant criterion with respect to the collection of employee personal information is reasonableness. Collection and use must be interpreted in accordance with section 4(1), which requires organizations to "consider what a reasonable person would consider appropriate in the circumstances."[53] Sections 13(2)(b) and 16(2)(b) also require collection and use of employee personal information without consent to be "reasonable" for the purposes of establishing, managing or terminating an employment relationship. The BC Privacy Commissioner established the following framework for evaluating whether collection and use of employee personal information is acceptable:

1. Is the information "about an identifiable individual" within the meaning of "personal information" as defined in section 1 of *PIPA*?
2. Is the information "work product information" as defined in s.1 of *PIPA*?
3. Is the information "employee personal information" as defined in s.1 of *PIPA*?

---

[48] *Ibid,* s 1.
[49] See *Re Twentieth Century Fox Film Corporation,* Order P06-04, 2006 CanLII 37938 at para 38, [2006] BCIPCD No 35 (QL).
[50] See *BC PIPA, supra* note 4, ss 13(1, 2), 16(1, 2).
[51] *Ibid* ss 13(3, 4), 16(3, 4).
[52] See *Re KONE Inc,* Order P13-01, 2013 BCIPC 23 (CanLII) at para 80, [2013] BCIPCD No 23 (QL) [*KONE*]; see also *Re ThyssenKrupp Elevator (Canada) Limited,* Order P13-02, 2013 BCIPC 24 (CanLII) at para 76, [2013] BCIPCD No 24 [*ThyssenKrupp*].
[53] See *Schindler, supra* note 46 at para 139.

4. Is the collection and use "reasonable" pursuant to sections 13(2)(b) and 16(2)(b) of *PIPA*?
5. Pursuant to sections 11 and 14 of *PIPA*, would a reasonable person consider the collection and use appropriate in the circumstances?
6. Has the employer met the requisite notice requirements pursuant to ss. 13(3) and 16(3) of *PIPA*?[54]

In determining whether collection or use of employee personal information is *reasonable* under step 4 above, the following non-exhaustive factors must be considered:

1. Sensitivity of the employee personal information;
2. Amount of personal information;
3. Likelihood of effectiveness;
4. Manner of collection and use of the personal information;
5. Less privacy-intrusive alternatives; and
6. Other relevant factors given the circumstances.[55]

v. Valid Collection and Use: Default Position

As in *PIPEDA*, BC *PIPA* allows for the collection and use of personal information, outside the scope of *employee* personal information, with the consent of the individual whose information is being collected.[56] Consent is necessary, but not sufficient for the employer to take any desired action. The collection or use must also be for purposes that a reasonable person would consider appropriate in the circumstances.[57] As in *PIPEDA*, employers may be able to collect and use personal information about individuals, including employees, without consent in specifically enumerated circumstances under sections 12(1) and 16(1). For example, BC *PIPA* contains an exception similar to section 7 of *PIPEDA* where an employer may collect personal information without consent where consent may compromise the availability or accuracy of personal information reasonably necessary for an investigation.[58]

Aside from the limited exceptions to consent under section 12(1) and 16(1), there are likely many other situations where an employer may wish to monitor the activities of their employees outside the scope of, for example, an investigation or proceeding. BC *PIPA* and Post-2015 *PIPEDA* better equip employers to manage these situations because they contain provisions dealing specifically with the collection and use of employee personal information, a subset of personal information.

III. APPLYING THE LAW: THE SCOPE OF EMPLOYEE MONITORING

A. Employee Personal Information and Consent: Practical Effects

In theory, employers possess a broader scope to monitor their employees under BC *PIPA* and Post-2015 *PIPEDA* because employers can collect or use *employee personal information* without consent where it is reasonable for managing the employment relationship, in addition to their rights

---

[54] *Ibid* at paras 4, 68.
[55] *Ibid* at paras 123-166; see also *KONE, supra* note 55 at para 45; *ThyssenKrupp, supra* note 55 at para 48; *Re Teck Coal Limited,* Order P20-04, 2020 BCIPC 24 (CanLII) at para 39, [2020] BCIPCD No 24 [*Teck Coal*].
[56] See *BC PIPA, supra* note 4, s 6.
[57] *Ibid,* ss 11, 14.
[58] *Ibid,* s 12(1)(c).

to collect and use *personal information* without consent in accordance with the broader exceptions. Conversely, employers collecting or using personal information under Pre-2015 *PIPEDA* had to either obtain employees' consent, or rely on the narrow exceptions under *PIPEDA* sections 7(1) and 7(2). As discussed above, few exceptions under section 7 are directly applicable to situations where employers may wish to monitor employees.

Consent is a key operating principle in both BC *PIPA* and *PIPEDA*.[59] As a result, some employees may believe that allowing employers to collect employee personal information without consent grants too much latitude for collection and use without consent, and vitiates employees' ability to consent. If this were the case, Pre-2015 *PIPEDA* may be understood to have better protected employee privacy rights by prohibiting employers from collecting personal information without consent. In practice, by restricting employers' rights to monitor employees without consent, Pre-2015 *PIPEDA* created unintended consequences that resulted in unclear applications of the law and defeated the reasonable expectations of employees subject to Pre-2015 *PIPEDA*. These unintended consequences will be elaborated upon below after assessing employee monitoring cases under BC *PIPA* and Pre-2015 *PIPEDA*.

B. GPS Tracking

i. GPS Tracking and Personal Information

The following section will compare the reasonableness of GPS monitoring by employees under both BC *PIPA* and Pre-2015 *PIPEDA*. It is generally accepted that GPS tracking devices can collect information about an identifiable individual, and thus can collect personal information. Through GPS tracking, employees are identifiable, even if not identified at all material times. Employers using GPS technology are aware which employees are driving specific vehicles assigned by the employer, or which cell phone belongs to specific employees. Thus, employers can ascribe the collected information to those specific employees.[60]

Under BC *PIPA*, information produced by GPS is not considered "work product information," so it is not excluded from the definition of "personal information." To qualify as work product information, it would have to be actively "prepared or collected." Data collected by GPS is not "prepared or collected" by its employees. The information is collected automatically, absent any conscious actions of individual employees producing the information.[61]

ii. BC *PIPA* Decisions: The Elevator Trilogy

The Elevator Trilogy decisions involved employers using GPS technology to collect personal information from their employees without consent. In *Schindler* and *Re ThyssenKrupp Elevator (Canada) Limited* ("*ThyssenKrupp*"),[62] the GPS system was installed on company vehicles,

---

[59] See *BC PIPA, supra* note 4, s 6; *PIPEDA, supra* note 3, Schedule 1, cl 4.3.

[60] See *ThyssenKrupp, supra* note 55 at para 22; *KONE, supra* note 55 at para 16; *PIPEDA GPS Case, supra* note 25.

[61] See *ThyssenKrupp, supra* note 55 at paras 24-26; *KONE, supra* note 55 at paras 19-20; *Schindler, supra* note 46 at paras 94-97. In *PIPEDA GPS Case,* the Office of the Privacy Commissioner of Canada did not explicitly mention the similar exception under *PIPEDA* s 7(1)(b.2), but one can infer that GPS information does not fit under this exception because no mention of s 7(1)(b.2) was made in the decision.

[62] *Supra* note 55.

collecting information such as vehicle location to a street address, speed, harsh braking, rapid acceleration, whether the ignition was turned on or off, and notifications when vehicles left particular locations. *Re KONE Inc.* was distinct because the GPS information was collected from phones assigned to employees ("*KONE*").[63] In all three cases, the complainant employees argued that their employee personal information could not be collected and used for managing the employment relationship because it was contrary to sections 13 and 16 of BC *PIPA*.

Virtually identical monitoring technology was used in *Schindler* and *ThyssenKrupp*. *ThyssenKrupp* is more recent, and applied the same legal tests used in *Schindler* to determine whether the use and collection of employee personal information was acceptable. Due to their similarity, this paper will focus the analysis on the more recent case, *ThyssenKrupp*, as well as *KONE*, which was slightly different because the GPS data was collected from employees' phones.

ThyssenKrupp involved an elevator servicing company that employed a mobile workforce of mechanics that generally worked independently, travelling straight from their homes to client sites. The mechanics were assigned to customers within their designated geographical areas. ThyssenKrupp employees were not permitted to use their vehicles for non-work-related purposes. The employer claimed the technology was installed to verify employee payroll and attendance, ensure compliance with the company's vehicle usage policies, ensure vehicle maintenance, monitor safe driving, ensure employee safety, and improve operational efficiency. The technology allowed the employer to know the location of every vehicle and how vehicles were being operated. The employer could receive near real-time alerts for GPS location, alerts when a vehicle was operated contrary to established parameters, or when a vehicle left a certain location.

First, the adjudicator confirmed that the employer was collecting "employee personal information." The information was reasonably required for employment purposes, and solely used for the employer's purposes stated above.[64] Second, the adjudicator applied the factors outlined in *Schindler* and determined that the employer's GPS monitoring was reasonably required to manage the employment relationship, and a reasonable person would consider it appropriate in the circumstances for ThyssenKrupp to collect and use this information.[65]

In finding ThyssenKrupp's collection reasonable, an important factor considered by the adjudicator was that the information collected was not particularly sensitive. The GPS systems were not continuously monitored; the location relates to the vehicle, but not necessarily the employees' precise location; and the information relates to employees' assigned employment locations and employment duties such as work hours and operation of company vehicles.[66] The GPS system was also likely to be reasonably effective for the employer's stated purposes because the mechanics were mobile, worked individually, and in-person supervision was not practical.[67] Further, the collection was not covert, and managers did not constantly or continuously review the

[63] *Ibid*.
[64] See *ThyssenKrupp, supra* note 55 at paras 30-33.
[65] *Ibid* at para 67; see also *BC PIPA, supra* note 4, ss 13(2)(b), 16(2)(b).
[66] See *ThyssenKrupp, supra* note 55 at para 50.
[67] *Ibid* at para 51.

collected information.[68] Lastly, the adjudicator noted that the monitoring was not offensive to the employees' dignity because it was not continuous, produced only weekly reports and occasional real-time monitoring, and the personal information was less sensitive than other types such as video footage.[69]

Although ThyssenKrupp's collection and use of the GPS information was reasonably required to manage the employment relationship, they were ordered to stop collecting and using the information until they provided proper notice to the employees.[70] BC *PIPA* sections 13(3) and 16(3) require meaningful notice of the collection and use. ThyssenKrupp provided a general policy noting that the employer collected information for purposes authorized by law. This notice was insufficient and lacked specificity in describing what personal information was being collected.[71] Conversely, the employer in *KONE* provided adequate notice by providing a general privacy policy regarding the use of employee personal information, a letter notifying employees of the GPS technology prior to collection, and multiple training and educational sessions about the technology.[72]

In *KONE,* the factual scenario and employer's purposes for using GPS were similar. The major difference was that the collection was limited to GPS location information only, and the information was collected from employees' mobile phones, rather than company vehicles. Collecting GPS information from employees' phones made the collection of personal information slightly more sensitive than in *ThyssenKrupp.* The information was more sensitive because it is reasonable to assume that employees carry their phones on their person, which made the location tracking more precise.[73] These distinctions were also notable because in *KONE,* less personal information was collected. The employer did not collect information related to the vehicle such as employees' driving habits.

Despite the slight differences in manner of collection and the type of information collected, the adjudicator in *KONE* came to a similar result. Applying the factors from *Schindler* and *ThyssenKrupp*, the employer's monitoring was reasonably required to manage the employment relationship.[74]

Numerous important factors can be extracted from these cases when assessing whether an employers' collection and use of GPS information is reasonable for the purposes of managing an employment relationship. First, the adjudicators continuously stressed the non-continuous nature of the *collection*. This made the information collected less sensitive, less invasive, and helped limit collection to information reasonably required for the employers' stated purposes. Second, the information was not constantly or continuously *used* by the employer. Much of the information was only used periodically. Third, the collection and use were limited to purposes related to the

---

[68] *Ibid* at paras 52, 54, 56, 58.
[69] *Ibid* at para 66.
[70] *Ibid* at para 94.
[71] *Ibid* at paras 84, 77.
[72] See *KONE, supra* note 55 at paras 79, 82.
[73] *Ibid* at para 49.
[74] *Ibid* at paras 45, 71.

employees' employment duties during work hours. Only in rare situations did the employers monitor employees outside the scope of their working duties and working hours. Lastly, context was important in these decisions. The workforce was mobile and independent, which made in-person supervision an impractical alternative.

iii. *PIPEDA GPS Case*[75]

The relevant facts in the *PIPEDA GPS Case* were virtually identical to *Schindler* and *ThyssenKrupp*. The complainant employees filed a complaint with the Office of the Privacy Commissioner of Canada regarding their employer's collection of their personal information without their consent. The technology collected location data from vehicles and produced reports regarding vehicle usage. The employer cited workforce productivity, efficiency, employee safety, and the protection and management of company assets as the purposes of the monitoring. Notably, the collection was not constant, and employees were made aware of the collection and use beforehand. Applying the *Eastmond* test, the employer's collection was found to be reasonable under *PIPEDA* section 5(3).

The outcome in the *PIPEDA GPS Case* was unremarkable. In the context of a mobile workforce, it seems reasonable that an employer should be able to monitor their employees in ways that employers can monitor employees working in-person. The case only appears problematic because the lack of clarity surrounding collection of employees' person information under Pre-2015 *PIPEDA* resulted in this case unnecessarily utilizing the Office of the Privacy Commissioner's resources. As per above, the complainant employees claimed that they had not consented to the employer's collection and use of their personal information. Under Post-2015 *PIPEDA*, the employees may not have made that same complaint, because the legislation clearly states that employee personal information can be collected to reasonably manage an employment relationship without employee consent. The effect, in this case, was that the Commissioner's Office was forced to adjudicate a decision that appeared to be a completely reasonable collection and use of employee personal information.

The *PIPEDA GPS Case* highlights the importance of legislative clarity. Both BC *PIPA* and Post-2015 *PIPEDA* establish clearer guidelines for when and how employee personal information can be collected. By doing so, employees better understand their rights and obligations and are less likely to utilize adjudicative resources in situations where collection and use appears reasonable. This proposition appears to be supported by the fact that, since Post-2015 *PIPEDA* clarified employee consent requirements by implementing section 7.3, no recorded cases have been brought forward under that provision. This does not indisputably prove that employees are now certain about when monitoring can take place, but it suggests employees may more clearly understand their employers' rights to monitor employees without consent. In turn, employees have not resorted to incorrectly filing complaints under section 7.3 based on their lack of consent, because the legislation clearly states that consent is no longer necessary in certain circumstances.

Under both BC *PIPA* and *PIPEDA*, monitoring employees by using GPS *can* amount to acceptable collection and use of employee personal information. Employers must be cognizant of how much

[75] *Supra* note 25.

data they are collecting, ensure monitoring is not continuous unless absolutely necessary, and limit collection to purposes related to the employees' employment duties. The *PIPEDA GPS Case* also supports the notion that including a provision for the collection of employee personal information without consent for the purposes of managing an employment relationship is beneficial because it creates clearer guidelines for when and how employee personal information can be collected.

C. Video Surveillance

i. Video Surveillance and Personal Information

Video surveillance clearly collects personal information by capturing and recording images of identifiable individuals.[76] Compared to GPS, video surveillance is generally more contentious because it collects more sensitive, privacy-invasive information. Unlike GPS, video allows viewers to clearly identify a person based on their physical characteristics.[77] As a result, adjudicative decisions tend to evaluate video surveillance more strictly. Despite the stricter evaluation, the following cases demonstrate that under both BC *PIPA* and *PIPEDA*, monitoring employees through video surveillance may be allowable in some circumstances.

ii. BC *PIPA*: *Re Teck Coal Limited* ("*Teck Coal*")[78]

In *Teck Coal*, employees filed complaints that video cameras at a mine site were collecting their personal information in violation of sections 13 and 16 of BC *PIPA* because they were not reasonable for the purposes of maintaining or terminating an employment relationship. The cameras were aimed in two locations: the tool crib, where expensive tools were kept, and in the office. The employees believed the cameras were being used to monitor their productivity, contrary to the employers' stated purpose of using the cameras to deter or investigate possible thefts, check on equipment status, and ensure workplace safety. The video recordings were reviewed live to view the status of production and safe work, or after the fact to review safety or production incidents, or for disciplinary purposes.

The adjudicator determined that the information was employee personal information collected solely for the reasonable purposes of preventing and investigating employee theft and monitoring operations.[79] Applying the factors laid out in *Schindler*, the adjudicator determined that the employer's use of video surveillance to monitor their employees was not reasonable.[80] The adjudicator noted that video footage is more sensitive because it allows one to identify personal characteristics of the recorded employees. Despite this, the collection was not inherently sensitive because the recorded area was an open, active work area where employee behaviour was observable by managers.[81] Although the monitoring was not covert, a key factor was that the cameras were continuously recording.[82] The adjudicator noted that continuous recording may be

---

[76] See *Teck Coal, supra* note 58 at para 29; see also *Eastmond, supra* note 24 at paras 175-176.
[77] See *Teck Coal, supra* note 58 at para 50; see also *ThyssenKrupp, supra* note 55 at para 66.
[78] *Supra* note 58.
[79] *Ibid* at para 33.
[80] *Ibid* at paras 40, 59.
[81] *Ibid* at paras 50-51.
[82] *Ibid* at paras 49, 7.

allowable where it is reasonable for managing or terminating an employment relationship, but that was not the case in *Teck Coal.*[83]

In *Teck Coal*, the main concerns raised were the effectiveness of the monitoring, and the constant surveillance. Firstly, there was no evidence of specific incidents where video surveillance was used for detecting or responding to safety or production issues. The adjudicator noted only a single incident where the footage was used to discipline an employee for "standing around" on camera.[84] Second, the constant surveillance amounted to an affront to the employees' dignity. In *Puretex,* cameras in a work area were objectionable because the employees experienced a sense of constant surveillance.[85] Similarly in *Teck Coal*, the continuously running cameras likely resulted in a similar sense of constant surveillance which amounted to an affront to the dignity of employees.[86]

It was not reasonable for the employer to monitor employees through video surveillance in both the work and office areas. The cameras were not shown to be effective for the employer's stated operational purposes, and despite the fact that the employer used little of the information that it collected, the sense of constant surveillance made the recording unreasonable.[87] The adjudicator also found that the employer provided inadequate notice of the monitoring. A sign posted at the mine entrance advised of the cameras, but there were no signs in buildings where the cameras at issue were located. Further, a sign advising of the presence of video cameras did not amount to meaningful notice about the type of personal information used and collected, and purposes for collection.[88]

iii. *PIPEDA*: *Eastmond*

In *Eastmond*, a CP Rail employee filed complaints with the Office of the Privacy Commissioner of Canada regarding video cameras installed in a CP Rail maintenance yard. The applicant did not consent to the monitoring. The employer's purposes for installing the cameras were to deter theft and vandalism. The court held that the video surveillance was reasonable under section 5(3) based on the four-step test adopted from the adjudicator's decision. First, the court agreed that the employer's purposes for surveillance were legitimate because of past incidents of theft and vandalism.[89] Unlike the decision in *Teck Coal*, the court held that the cameras appeared to be effective because there were no incidents since the cameras were installed.[90] The key factor was that the Court believed the loss of employee privacy was proportional to the benefits. This finding was based on the fact that the recordings were not reviewed unless an incident occurred. If there was no incident, the recordings would be destroyed every 96 hours, without being viewed. This meant the collection was neither continuous, nor surreptitious.[91] Despite the employee's concerns,

---

[83] *Ibid* at para 44.
[84] *Ibid* at para 54.
[85] See *Eastmond, supra* note 24 at para 142 citing *Re Puretex Knitting Co Ltd and Canadian Textile and Chemical Union* (1979), 23 LAC (2d) 14.
[86] See *Teck Coal, supra* note 58, at para 58.
[87] *Ibid* at para 60.
[88] *Ibid* at paras 81, 87-88.
[89] See *Eastmond, supra* note 24 at paras 177-178.
[90] *Ibid* at para 179.
[91] *Ibid* at paras 180-181.

the Court held that the collection was limited to deterring theft and vandalism, and not measuring employee performance.[92] Ultimately, "a reasonable person would consider CP's purposes for collecting by recording the images of CP employees and others on video camera appropriate in the circumstances."[93]

The case becomes problematic because the employee did not consent to the collection, contrary to the consent requirement in clause 4.3 of *PIPEDA* Schedule 1. The Court ultimately decided that the employer's collection fit under the consent exemption in *PIPEDA* section 7(1)(b):

> (b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.

The Court applied 7(1)(b) because the cameras were not actively monitored, meaning collection only occurred when CP Rail officials reviewed the recording to investigate an incident. If an incident occurred involving theft, asking for the individual's permission to collect the information would compromise the availability of the information for the purpose of an investigation.[94]

At first glance, utilizing this exception does not appear problematic. Deterring theft and vandalism seems to be a reasonable purpose for video surveillance. Further, by limiting collection to specific incidents where theft or vandalism may have occurred, the employer placed reasonable limits on collection that avoided the sense of continuous monitoring present in *Teck Coal*. Similar to the *PIPEDA GPS Case*, the issue again is that the employees' reasonable expectations about when consent is required are overridden. Absent the exception from consent for collecting employees' personal information to manage the employment relationship, guidelines for when employees must consent to requirement lack clarity. In *Eastmond*, the employee would have expected CP Rail to require their consent if any monitoring occurred, unless the collection fit under the section 7 exceptions. If employers can frequently rely on the section 7 exceptions for routine monitoring, it tends to make the consent requirement redundant. Organizations and employees would be better served by following the Post-2015 *PIPEDA* and BC *PIPA* models for collection of employees' personal information without consent. This way, employees understand that consent to monitoring is not the default with respect to managing or terminating an employment relationship, and do not rely on mistaken expectations regarding consent. This issue will be expanded on in Part IV, below.

IV. ANALYSIS: REASONABLE EXPECTATIONS OF CONSENT

A. Reasonableness of Monitoring Employees Without Consent

As the nature of physical workplaces evolve and technology advances, monitoring can provide value to employers while protecting employees' rights to privacy. Allowing some forms of employee monitoring without consent is reasonable because it aligns with the purposes of BC *PIPA* and *PIPEDA* by appropriately balancing employers' and employees' interests. Neither

[92] *Ibid* at para 176.
[93] *Ibid* at para 174.
[94] *Ibid* at para 188.

individuals, nor organizations, have absolute rights with respect to the collection and use of personal information. Employee privacy is critical, but as technology advances and the nature of how people work changes, organizations must adapt to those changes to stay competitive. Allowing *reasonable* employee monitoring without consent strikes the appropriate balance in the employment relationship by allowing appropriate forms of monitoring, but also protecting employees from overly invasive monitoring.

In both BC *PIPA* and Post-2015 *PIPEDA*, statutory limits adequately protect employees from offensive forms of monitoring. First, notice requirements protect employees from covert surveillance. This protects the reasonable expectations of employees who must be made aware of the collection and purposes of that collection. The requirement for meaningful notice is effective because it requires employers to inform employees about the type of personal information used and collected, as well as the purposes for the use and collection.[95]

Second, both BC *PIPA* and Post-2015 *PIPEDA* limit surreptitious monitoring. These protections are achieved by ensuring collection is reasonable and limited to information necessary for appropriate purposes. The limitation on collection ensures that employers establish clear purposes for collection, and limit their collection to achieving those reasonable purposes. For example, although employee management can be an appropriate purpose, solely or constantly using technology to assess employee performance may be deemed continuous monitoring and overly invasive.[96] Specific to video surveillance under BC *PIPA*, the Acting Information and Privacy Commissioner noted that monitoring employees through video surveillance should be a last resort after exploring less privacy-invasive alternatives.[97] Video surveillance should not replace adequate employee management.[98] This point is especially important when considering how technology impacts employment relationships. If technology allows employees to work outside the direct supervision of their employers, it seems reasonable that employers should be able to engage in some form of monitoring that resembles supervision that would occur in-person. The reasonableness of employer purposes change as society, and employment relationships, shift.

Third, the legislation and decisions made pursuant to the legislation adequately protect information according to its sensitivity, and degree of privacy-invasiveness. The opposite results in *Eastmond* and *Teck Coal*, which both concerned video surveillance, demonstrate that where more sensitive information is in question, collection and use must be more limited to appropriate purposes. *Investigation Report F15-01*[99] demonstrates that highly invasive monitoring must be necessary for

---

[95] See for example *ThyssenKrupp, supra* note 55 at para 76; see also *Teck Coal, supra* note 58 at para 81.

[96] See for example *PIPEDA GPS Case, supra* note 25; see also *Over-collected and Overexposed: Video Surveillance and Privacy Compliance in a Medical Clinic*, Audit & Compliance Report P16-01, 2016 BCIPC 56 at 4, [2016] BCIPCD No 56 (QL) [*Report P16-01*].

[97] *Ibid, Report P16-01*.

[98] *Ibid.*

[99] *Use of Employee Monitoring Software by the District of Saanich,* Investigation Report F15-01, 2015 BCIPC No 15, [2015] BCIPCD No 15 (QL) (this case was decided under the British Columbia *Freedom of Information and Protection of Privacy Act* (*FIPPA*), RSBC 1996, c 165, which governs public sector organizations in BC. Despite this, there are similarities between collection of personal information under *FIPPA* and *BC PIPA*, and the question of whether the information is "necessary" under *FIPPA* s 26(c) involves a similar analysis as determining whether collection is necessary for achieving appropriate purposes under *BC PIPA*).

achieving the employer's stated purposes ("*District of Saanich"*). In that case, the District of Saanich installed software that captured keystroke logging, automated screenshots of employee activities every thirty seconds, and continuous tracking of computer program activity on employee workstations. Although it was important that the employer combat threats to their information technology systems, the District's collection was deemed overly invasive, exceeding what was necessary to achieve the purpose of protecting their information technology systems.[100] *District of Saanich* was decided under BC public sector privacy legislation, and no comparable cases have been published under BC *PIPA*. Despite this, based on the rulings on GPS and video surveillance, it seems unlikely that such invasive means of monitoring would be acceptable except for limited and appropriate purposes.

Lastly, legislative requirements for adequate protection of personal information collected ensure that personal information will be protected.[101] In addition, the requirement for appropriate organizational policies helps employees establish reasonable expectations for methods and purposes of collection.[102]

Both BC *PIPA* and Post-2015 *PIPEDA* appear to limit employee monitoring to reasonable situations and, as a result, adequately protect employee privacy interests. The legislative safeguards against unreasonable monitoring suggest that collecting employee personal information without consent reasonably achieves the purposes of private sector privacy legislation.

B. Reasonable Expectations of Employees

Under BC *PIPA* and Pre-2015 *PIPEDA*, employees *may* be monitored by their employers, subject to the reasonableness of the collection. The legislation makes it clear that, despite the overriding importance of consent, there may be situations where employers can monitor their employees without consent. As discussed in the previous section, this exception reasonably balances employers' rights to operate effective businesses with individual privacy rights. The *PIPEDA GPS Case* and *Eastmond* demonstrate that when this exception to consent does not exist, employers and adjudicative decision-makers look to other avenues under the legislation to collect employee personal information regardless. If employee monitoring will happen regardless, the legislation should set clear guidelines for when monitoring for the purposes of managing an employment relationship can occur without consent.

Eastmond was not an isolated incident of employers governed by Pre-2015 *PIPEDA* resorting to section 7 exceptions to collect employee personal information. In *Wansink v. Telus Communications*[103] ("*Wansink*"), an employer collected recordings of employee voice notes and argued that the collection fell under the section 7(1)(a) exception to consent. This exception applies where the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way. The Federal Court of Appeal held that this was clearly not a situation where the section 7(1)(a) exception applied. *Wansink* was another example where the Court found the

[100] *Ibid* at 26.
[101] See *BC PIPA, supra* note 4, s 34; *PIPEDA, supra* note 3, Schedule 1, cl 4.7.
[102] See for example *BC PIPA, supra* note 4, s 5.
[103] *Supra* note 41.

collection of personal information to be reasonable, yet the employer was forced to find a workaround to the lack of consent.

Where employers and adjudicators are forced to circumvent consent requirements to reasonably monitor their employees, the value of consent is diluted. The *PIPEDA GPS Case*, *Eastmond*, and *Wansink* all overlook the apparent "cornerstone" of *PIPEDA*: consent.[104] The impression that employees must provide consent for all but a limited number of situations where personal information is collected is diminished because employers simply looked to other sections of Pre-2015 *PIPEDA* to circumvent consent requirements. If this is the result, there does not appear to be any rational reason for failing to include a provision allowing for employee monitoring without consent for the purposes of managing the employment relationship. Maintaining the current exceptions to consent for the collection and use of employee personal information under BC *PIPA* and Post-2015 *PIPEDA* create a legislative scheme that sets clearly established guidelines for when exceptions to consent are allowable. This will not eliminate complaints related to employee monitoring, but it will reduce confusion about whether an employer must obtain employee consent. In turn, this will reduce the number of employee complaints regarding consent by establishing clearer expectations for when employers must obtain employee consent or not.

V. LOOKING FORWARD: EMPLOYEE MONITORING IN A REMOTE WORKING AGE

A. Employee Perceptions of Monitoring

The rapid shift to remote work after the COVID-19 pandemic may encourage employers to find new avenues to monitor employees in order to assess performance and maintain adequate security measures. Employers may believe that more extensive remote monitoring technology can improve their ability to assess employee performance. Despite the potential benefits, increased monitoring may raise privacy concerns and questions about the ethics of such monitoring. Although both BC *PIPA* and *PIPEDA* allow employers to engage in some degree of monitoring, employers must assess whether the benefits outweigh any potential negative impacts.

Cases such as *Teck Coal* suggest that overly invasive monitoring can amount to an affront to employees' dignity. This clearly suggests that monitoring impacts how employees feel about their work and their employers. A 2021 study of employers in the United States found that 70% of the organizations surveyed have put systems in place to monitor remote employee productivity. In turn, organizations that implemented monitoring technology or plan to do so reported considerably higher levels of employee turnover.[105] This finding suggests that although employee monitoring may become more prominent as remote work expands, employees may seek out work that involves lesser degrees of monitoring.

A 2021 study assessing the impacts of workplace surveillance on remote workers outlined numerous factors that shape how employees react to surveillance. One prominent factor was the clarity of the monitoring purposes. When workers do not see a clear work-related purpose for

---

[104] *Ibid*.

[105] VMware, "The Virtual Floorplan: New Rules for a New Era of Work" (2021), online (pdf): *VMware* <www.vmware.com> [https://perma.cc/34WE-5LHV] at 12.

monitoring technologies, they are likely to perceive the surveillance measures negatively.[106] Building on this point, a study on Canadian public servant attitudes towards workplace surveillance technologies found a "very strong correlation between one's sense of intrusiveness of a technology and their views of its reasonableness for use in a public sector work environment."[107] Notably, the study found that technologies viewed as "very unreasonable" tended to capture physical characteristics by recording audio, video, and location. Conversely, respondents tended to view computer surveillance methods such as keylogging, internet usage recording, and email analysis as less intrusive. The authors argued this is likely due to the clearer relationship that these methods have with performance monitoring.[108]

A second prominent factor that shaped how employees react to surveillance was the perceived degree of surveillance. Workers perceiving greater levels of surveillance while working tend to possess more negative attitudes toward the surveillance.[109] Surveillance measures perceived to be excessive were shown to lead to higher employee turnover and absenteeism, weakened morale, decreased trust in management, and poorer relations between employees and employers.[110]

Lastly, a 2019 study on millennials conducted by Deloitte suggested that millennials are placing more value on their data and protecting their privacy.[111] About 33% of respondents said they stopped or decreased a business relationship because of the amount of personal data that the company requested to collect. Further, 25% of respondents stopped or decreased a business relationship because of a company's inability to protect their private data, or because of how a company tracks or customizes their online behaviours.[112] This study was not limited to privacy concerns related to employment, but suggests that millennials are increasingly concerned about collection of their personal information.

B. Implications for Employers

The studies noted above suggest that employees may harbour scepticism about remote monitoring technology, which is not necessarily surprising. Although monitoring may become a more prominent feature for employers, employers must account for potential concerns among their workforces. The rules governing the collection and use of employee personal information under both BC *PIPA* and *PIPEDA* provide strong guidelines for employers to address employee concerns.

---

[106] N Abdelaal et al, "Workplace Surveillance and Remote Work: Exploring the Impacts and Implications Amidst Covid-19 in Canada" (2021), online (pdf): *Cyber Secure Policy Exchange* <www.cybersecurepolicy.ca/workplace-surveillance> [https://perma.cc/B3RU-M23C] at 33.

[107] Etienne Charbonneau & Carey Doberstein, "An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector" (2020) 80:5 Public Administration Rev at 785.

[108] *Ibid* at 785-786.

[109] N Abdelaal et al, *supra* note 106 at 32.

[110] *Ibid*.

[111] Deloitte, "The Deloitte Global Millennial Survey 2019: Societal discord and technological transformation create a 'generation disrupted'" (2019), online (pdf): *Deloitte* <www2.deloitte.com> [https://perma.cc/T9N7-DEMH] at 19.

[112] *Ibid*.

First, BC *PIPA* and *PIPEDA* requirements for meaningful notice of any collection and use of employees' personal information can help address employee scepticism. Advising employees of any collection, as well as the purposes of collection, can help set appropriate guidelines. This informs employees about the scope of collection, and educates employees about the reasonable purposes for collection. Developing clear policies and practices will help employees understand how the monitoring may be reasonably connected to a work-related purpose.

Second, legislative requirements that collection of personal information must be reasonable and limited to legitimate purposes should help reassure employees that the degree of surveillance will not be overly invasive. The *District of Saanich* case demonstrates that constant monitoring of employee devices will not be acceptable where the benefits are disproportionate to the degree of collection. This also suggests that employers should reasonably limit the scope of monitoring where possible. Not only is overbroad monitoring perceived negatively by employees, but it is generally not allowed under BC *PIPA* and *PIPEDA*. Employers can better preserve relationships with their employees by exploring less privacy invasive monitoring options first, before defaulting to more invasive methods of collection.

When employers are considering the impacts of potential monitoring technology on their employees, they should engage in a similar balancing act as private sector privacy legislation puts at the forefront. Monitoring technology must appropriately balance individual privacy rights with organizational abilities to effectively run their businesses. Technology that is overly invasive may strain employment relationships, but they may also be contrary to privacy legislation.

VI. CONCLUSION

Monitoring employees is becoming more commonplace amongst private sector employers. This raises questions about the efficacy of Canadian private sector privacy laws. Specifically, employees may believe that Pre-2015 *PIPEDA* better protected employee privacy rights because it did not allow for collection of employee personal information without consent. In practice, the Office of the Privacy Commissioner of Canada and courts appeared to tolerate the same scope of employee monitoring as under BC *PIPA*. In the absence of provisions allowing for reasonable collection of employee personal information for the purposes of managing the employment relationship, decision-makers resorted to alternatives such as general exceptions to consent or implied consent to allow reasonable employee monitoring. Rather than confirming employees' reasonable expectations that Pre-2015 *PIPEDA* required consent for collection of employee personal information, these decisions introduced uncertainty surrounding whether, and in what situations, employee monitoring required consent.

Conversely, Post-2015 *PIPEDA* and BC *PIPA* have created greater certainty regarding consent requirements for employee monitoring. The statutes make it clear that in certain employment situations, employers do not require employee consent, so long as the collection and use are reasonable for managing the employment relationship. In turn, employees have clear expectations about whether, and in what situations, employee monitoring can occur without consent. Both BC *PIPA* and Post-2015 *PIPEDA* include limits on employee monitoring that adequately protect employees in the absence of the ability to withhold their consent. In Bill C-11, the apparent

decision to retain employers' abilities to collect and use employee information without consent for the purposes of managing an employment relationship suggests that Parliament recognizes that this provision strikes a more appropriate balance than under Pre-2015 *PIPEDA*.[113] Although employee monitoring should be allowed in some situations, employers must balance the urge to use technology to monitor employee performance with the changing values of a largely millennial workforce that may harbour scepticism about monitoring and data privacy. While BC *PIPA* and Post-2015 *PIPEDA* have not dealt specifically with some of the more invasive means of digital surveillance, the issue will likely arise in the future, and the legislation appears properly equipped to balance individual and organizational rights.

[113] Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts,* 2nd Sess, 43rd Parl, cl 24 (first reading 17 November 2020).

Bibliography

Legislation

Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 2nd Sess, 43rd Parl, cl 24 (first reading 17 November 2020).

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165.

Personal Information Protection Act, SBC 2003, c 63.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Organizations in the Province of Alberta Exemption Order, SOR/2004-219.

Organizations in the Province of British Columbia Exemption Order, SOR/2004-220.

Organizations in the Province of Quebec Exemption Order, SOR/2003-374.

Jurisprudence

British Columbia Hydro and Power Authority v British Columbia (Information and Privacy Commissioner), 2019 BCSC 2128.

Eastmond v Canadian Pacific Railway, 2004 FC 852.

Employer accused of wrongful disclosure, PIPEDA Case Summary #2003-198, 2003 CanLII 44917 (PCC).

Gordon v Canada (Minister of Health), 2008 FC 258.

Individual denied access to personal information, PIPEDA Case Summary #2003-149, 2003 CanLII 42240 (PCC).

Over-collected and Overexposed: Video Surveillance and Privacy Compliance in a Medical Clinic, Audit & Compliance Report P16-01, 2016 BCIPC 56, [2016] BCIPCD No 56 (QL).

R v Cole, 2012 SCC 53.

R v Spencer, 2014 SCC 43.

Re KONE Inc, Order P13-01, 2013 BCIPC 23 (CanLII), [2013] BCIPCD No 23 (QL).

Re Puretex Knitting Co Ltd and Canadian Textile and Chemical Union (1979), 23 LAC (2d) 14.

Re Schindler Elevator Corporation, Order P12-01, 2012 BCIPC 25 (CanLII), [2012] BCIPCD No 25 (QL).

Re Teck Coal Limited, Order P20-04, 2020 BCIPC 24 (CanLII), [2020] BCIPCD No 24.

Re ThyssenKrupp Elevator (Canada) Limited, Order P13-02, 2013 BCIPC 24 (CanLII), [2013] BCIPCD No 24.

Re Twentieth Century Fox Film Corporation, Order P06-04, 2006 CanLII 37938, [2006] BCIPCD No 35 (QL).

Telecommunications company asked to adopt consistent retention practices, PIPEDA Case Summary #2002-73, 2002 CanLII 42331 (PCC).

Use of Employee Monitoring Software by the District of Saanich, Investigation Report F15-01, 2015 BCIPC No 15, [2015] BCIPCD No 15 (QL).

Use of personal information collected by Global Positioning System considered, PIPEDA Case Summary #2006-351, 2006 CanLII 42313 (PCC).

Wansink v Telus Communications Inc, 2007 FCA 21.

Secondary Materials

Abdelaal, N et al, "Workplace Surveillance and Remote Work: Exploring the Impacts and Implications Amidst Covid-19 in Canada" (2021), online (pdf): Cyber Secure Policy Exchange <www.cybersecurepolicy.ca/workplace-surveillance> [https://perma.cc/B3RU-M23C].

Charbonneau, Etienne & Doberstein, Carey, "An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector" (2020) 80:5 Public Administration Rev.

Deloitte, "The Deloitte Global Millennial Survey 2019: Societal discord and technological transformation create a 'generation disrupted'" (2019), online (pdf): Deloitte <www2.deloitte.com> [https://perma.cc/T9N7-DEMH].

Power, Michael, *The Law of Privacy*, 2nd ed (Toronto: LexisNexis Canada, 2017).

VMware, "The Virtual Floorplan: New Rules for a New Era of Work" (2021), online (pdf): VMware <www.vmware.com> [https://perma.cc/34WE-5LHV].

von Tigerstrom, Barbara, *Information and Privacy Law in Canada* (Toronto: Irwin Law Inc., 2020).