Protecting privacy. Promoting transparency.

Order P12-01

SCHINDLER ELEVATOR CORPORATION

Elizabeth Denham, Information and Privacy Commissioner

December 19, 2012

Quicklaw Cite: [2012] B.C.I.P.C.D. No. 25
CanLII Cite: 2012 BCIPC No. 25

Summary: Schindler collects information using a GPS and engine status data system installed in its service vehicles, which are assigned exclusively to its mechanics. Mechanics do not report to work at an office; they travel from their homes to job sites on assigned routes. The GPS component of the system records a vehicle's location and movements, as well as the time and date of its locations. The engine status component records the vehicle engine's start and stop times, as well as things like excessive speeding, braking and acceleration. Among other things, Schindler collects and uses this information for employment management purposes; the information is personal information and employee personal information. Schindler is in the circumstances, including the policies it follows as to how and when it collects and uses this information, authorized to collect and use it.

Statutes Considered: *Personal Information Protection Act*, ss. 1, 5, 11, 13(2)(b), 14 and 16(2)(b).

Authorities Considered: B.C.: Order F07-18, [2007] B.C.I.P.C.D. No. 30; Order P06-05, [2006] B.C.I.P.C.D. No. 39; Order P06-04, [2006] B.C.I.P.C.D. No. 35; Order F08-03, [2008] B.C.I.P.C.D. No. 6; Order P05-01, [2005] B.C.I.P.C.D. No. 18. **Ont.:** Order PO-2811, [2009] O.I.P.C. No. 127. A**lta.:** Order P2009-005, [2010] A.I.P.C.D. No. 4; Order F2005-003, [2005] A.I.P.C.D. No. 23; Order P2006-004, [2006] A.I.P.C.D. No. 38; Order P2006-005, [2007] A.I.P.C.D. No. 46; Order P2006-008, [2007] A.I.P.C.D. No. 16; Investigation Report P2005-IR-009, [2005] A.I.P.C.D. No. 46; Investigation Report P2005-IR-004, [2005] A.I.P.C.D. No. 49.

Cases Considered: *Dagg v. Canada (Minister of Finance)* [1997] 2 S.C.R. 403; *Canada (Information Commissioner) v. Canada (Canadian Transportation Accident Investigation and Safety Board*) 2006 FCA 157; *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police*) 2003 SCC 8, [2003] 1 S.C.R. 66; *Eastmond v. Privacy Commissioner of Canada* 2004 FC 854; *University of Alberta v.*

Alberta (Information and Privacy Commissioner) 2009 ABQB 112; *Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner)* (2001), 154 O.A.C. 97 (ONSC Div. Ct.); *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300, (2002), 166 O.A.C. 88 (Ont. C.A.); *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)* 2011 ABCA 94; *Teamsters, Local 419 v. Securicor Cash Services*, [2004] O.L.A.A. No. 99; *Otis Canada Inc. v. International Union of Elevator Constructors, Local 1,* [2010] B.C.C.A.A.A. No. 121; *Re St. Mary's Hospital (New Westminster) and Hospital Employees Union,* (1997), 64 L.A.C. (4th) 382 (Larson); *Pope & Talbot Ltd. v. Pulp, Paper and Woodworkers of Canada, Local No. 8*, [2003] B.C.C.C.A.A. No. 362; *Canadian Pacific Ltd. v. Brotherhood of Maintenance of Way Employees*, (1997), 59 L.A.C. (4th) 111 (Picher); *Re Finning International and International Association of Machinists and Aerospace Workers*, *Local 99,* (2004), 135 L.A.C. (4th) 335 (Smith); *Spectra Energy v. Canadian Pipeline Employees' Association,* [2011] C.L.A.D. No. 266 (Laing); *R. v. Ward*, 2012 ONCA 660; *H. J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, 2006 SCC 13, [2006] 1 S.C.R. 441; *Gordon v. Canada (Health)*, 2008 FC 258; *Girao v. Zarek Taylor Grossman Hanrahan LLP*, 2011 FC 1070; *Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner*) (2001), 154 O.A.C. 97 (ONSC Div. Ct.); *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300, (2002), 166 O.A.C. 88 (Ont. C.A.); *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2012 ONCA 393; *Rizzo & Rizzo Shoes Ltd.,* [1998] 1 S.C.R. 27; *Re: Sound v. Motion Picture Theatre Associations of Canada*, 2012 SCC 38; *R. v. Wise*, [1992] 1 S.C.R. 527; *Jones v. Tsige*, 2012 ONCA 32; *Wansink v. TELUS Communications Inc.*, 2007 FCA 21, [2007] 4 FCR 368.

TABLE OF CONTENTS

INTRODUCTION

[1] This case involves increasingly common, and important, questions about how technologies that enable businesses to monitor work-related activities to a much greater extent than before affect the privacy of individuals during the considerable portion of their lives spent in the workplace.

[2] Since 2010, Schindler Elevator Corporation ("Schindler") has used a system comprising Global Positioning System ("GPS") and engine monitoring technologies installed in its elevator service vehicles. The technologies are part of a system known as the Fleet Complete system. This suite of technologies is installed in vehicles that Schindler's field mechanics use to visit work sites, where they repair or maintain elevators. The mechanics work from home. They keep their vehicles at home and travel to and from work from there, without reporting to a Schindler office as part of their daily routine.

[3] Schindler's adoption of these technologies prompted a complaint to this Office. The complaint was made by Schindler employees who are members of the International Union of Elevator Constructors, Local 82 ("IUEC"). This Office's mediation efforts were not successful, so a written inquiry was held respecting the complaints.

[4] The complainants say that Schindler's use of this system contravenes the *Personal Information Protection Act* ("PIPA"). Among other remedies, the complainants seek orders under s. 52 prohibiting Schindler from using the technologies to collect and use personal information and requiring Schindler to destroy all personal information it has already collected contrary to PIPA. Schindler denies that the technologies collect personal information at all and says that, even if it is personal information, it is employee personal information the collection, use and disclosure of which are permitted under PIPA.

[5] The question in this case is whether PIPA authorizes Schindler to collect, use and disclose information generated by the Fleet Complete system for, among other things, the purpose of ensuring that its employees keep their work hours, do not use vehicles for personal use, and drive safely and lawfully.

ISSUES

[6] The issues in this case, which were set out in the notice of inquiry that this Office issued to the parties, can be stated as follows:

1. Is the information collected by the technologies Schindler uses 'personal information' within the meaning of s. 1 of PIPA?

2. If it is, is that personal information also 'employee personal information' within the meaning of s. 1 PIPA?

3. Does PIPA authorize Schindler to collect that information (ss. 11 and 13(2)(b)) and to use that information (ss. 14 and 16(2)(b))?

4. Has Schindler complied with its obligations under s. 5 of PIPA?

DISCUSSION

[7] **Description of the System**—As deployed by Schindler, the Fleet Complete system generates GPS-derived vehicle location information and information about the operation of the vehicle. The latter class of information includes engine ignition times, speed and distance travelled. Schindler's evidence is that, although Fleet Complete has other capabilities, its deployment generates the following information:[1]

1. Through GPS technology contained in the system, real-time information about the location and movements of a service vehicle ("GPS data").[2]

2. Through other technology contained in the system, information relating to engine status and thus vehicle operation ("engine status data"):

    a. Distance travelled;

    b. Speed of the vehicle;

    c. Harsh braking;

    d. Sharp acceleration;

    e. Idling (defined as the length of time the vehicle is stationary with its engine running);

    f. Time at which the vehicle's ignition turns on;

    g. Time at which the vehicle's ignition turns off;

    h. Movement without the vehicle's ignition being on.

[8] Schindler says it does not "constantly" monitor data as part of its operations; information is recorded, but viewed and used only in accordance with its policy on use of data.[3] Rather, it has programmed the Fleet Complete system to generate "exception reports". An exception report "summarizes all the occasions that the operation of a Schindler vehicle has deviated from accepted norms", such as speeding, harsh braking or rapid acceleration.[4] These reports are created only where "a rule is broken", not when a vehicle is operated normally in accordance with how Schindler has programmed the Fleet Complete system".

---

[1] Although I will analyze the issues with reference to the information collected by each of the technologies generally described above, for convenience I will sometimes refer to the GPS data and engine data technologies collectively as "technologies".

[2] It is not clear from the material how accurate the GPS positioning information is, *i.e.*, it is not clear whether location is shown within 1 metre, 2 metres or 10 metres, for example. This said, both Schindler and the complainants have made their submissions on the basis that a relatively high degree of accuracy is involved.

[3] The complainants raised an issue about this, alleging inconsistent practice by Schindler on this score, as discussed below.

[4] Initial submission, para. 14.

[9] The 'exception reports' are produced according to these parameters:[5]

1. Speeding in excess of 15 km/h per hour over the posted speed limit;

2. Idling for more than 18 minutes;

3. Harsh braking, defined as deceleration by 12 km/h or more in 2 consecutive seconds;

4. Sharp acceleration, defined as acceleration by 11 km/h or more in 2 consecutive seconds;

5. First ignition off after scheduled start time; and

6. Last ignition off before scheduled stop time.

[10] A clarifying comment is needed here. Schindler says in its reply submission that the complainants' initial submission makes "no attempt to distinguish between GPS information and Engine Status information", even though "the two are clearly different". Schindler also contends that there are "clear analytical differences between GPS information about the location of a vehicle and purely operational Engine Status data."[6] I reject below the notion that there is in these circumstances a salient distinction between the kinds of data for PIPA compliance purposes. I will say here, though, that Schindler's criticism of the complainant's submission is ill-placed, since Schindler's own GPS policy lumps the two kinds of data together as "GPS" data.

[11] The title of the policy, further described below, is "Vehicle Global Positioning System (GPS) Policy". It refers throughout to "GPS data", "vehicle GPS" or "vehicle GPS data", without ever explaining what these terms mean. After referring to "[v]ehicle GPS", for example, it says that "[k]ey performance indicators such as harsh braking, sharp acceleration, and speeding may be monitored through exception reporting", to reduce "instances of unsafe driving". It says "vehicle GPS data" may be used for "investigating…concerns about the conduct of employees reporting to work locations in a timely manner". Yet Schindler's own evidence is that safe-driving and work-hours matters are addressed using the engine status data described above, not only "vehicle GPS data" in the sense of GPS location information.

[12] Again, as will be seen below, nothing turns on Schindler's suggested analytical distinction between the kinds of data, or on how its GPS policy is worded, but its criticism of the complainants is, as I say, ill-placed. This is why, to

[5] Affidavit of Robert Devine, Schindler's Technical and Field Support Director.
[6] Reply submission, para. 7.

avoid further confusion, I use two different terms, where warranted,[7] to distinguish between the system-generated "GPS data" and "engine status data".

[13] **How Schindler Uses the Information**—In January 2010, Schindler told the IUEC that it intended to install and use the Fleet Complete system. It said it would use the information collected in accordance with its 'Vehicle Global Positioning System (GPS) Policy'[8] ("GPS Policy"), which it provided to the IUEC at that time.[9] The system was installed in vehicles in May 2010. In September 2010,[10] Schindler sent a letter to all its employees about hours of work. That letter said that Schindler would use engine status data to help determine if employees were meeting their hours-of-work obligations.[11]

[14] Against this backdrop, I will now outline the evidence in this inquiry as to Schindler's purposes in collecting and using GPS data and engine status data. In the response to Schindler's evidence, which is summarized below, the complainants submit, among other things, that employee self-reporting is effective, that Fleet Complete is not a necessary response to the issues Schindler says it was intended to address, and Schindler had not identified, before implementing Fleet Complete, any demonstrable problems relating to either vehicle use or employee performance.

Operational Efficiency

[15] Schindler uses a program called the Planning Assistant for Superintendent Scheduling ("PASS"), developed in anticipation of Fleet Complete's implementation, to support efficient planning of service routes in conjunction with Fleet Complete.[12] PASS is used to create route assignments based on certain assumptions. Schindler says that GPS data from Fleet Complete allows it to validate or correct these planning assumptions, which helps optimize route efficiencies. Fleet Complete is also used to assign emergency service calls more

[7] For convenience, I sometimes refer to the "technologies" or "Fleet Complete".
[8] A copy of which forms Exhibit 2 to the Verbruggen affidavit.
[9] Before the system was installed, Schindler and the IUEC tried to resolve the IUEC's concerns, but failed to do so. Affidavit of Laurie Verbruggen, Schindler's Privacy Officer, paras. 5-9.
[10] At para. 10 of her affidavit, Verbruggen deposes that this letter was sent in November 2010, but at para. 45 she says it was sent in September 2010. A copy forms Exhibit 1 to her affidavit and it is dated September 2010. This version is not the same as the version submitted by the complainants, through an affidavit sworn by Gordon Heard, the IUEC's business manager at the time the complaints leading to this inquiry were made. The two versions are signed by different Schindler National Operations Managers; the Schindler copy appears to be a letter template, and is not addressed to anyone. The two versions are, nonetheless, essentially the same as regards the hours-of-work purposes they each state for collection of information through the Fleet Complete system.
[11] Verbruggen affidavit, para. 10.
[12] This description of the purposes for Schindler's collection and use of information is based on the Verbruggen affidavit and Schindler's submissions.

efficiently. Schindler says its reputation depends on how quickly it can respond to emergencies where, for example, people are trapped in elevators, and Fleet Complete improves responsiveness and follow-up evaluation.

[16] Before implementing PASS and Fleet Complete, Schindler says, it relied on less-informed methods to plan routes. It also had to rely on employees to self-report on their adherence to route assignments, tasks completed and hours of work. Acknowledging that by far most of its employees are diligent in reporting, Schindler says the demands of work often make it difficult for them to report as the day proceeds, with after-the-fact reporting, sometimes days after, being a source of errors. It also says direct observation of employee performance by supervisors is not as effective, noting that it has a supervisor-to-employee ratio of 1:10 and a mobile workforce.

Safety and security

[17] Schindler says it has a duty to take reasonable steps to protect other road users from unsafe driving by its employees; it says Fleet Complete enables a pro-active approach to safety. Before, it could only address unsafe driving habits when it received complaints from other drivers or employees, or when an employee was charged with a road safety offence. Now, exception reports enable it to identify and address unsafe driving practices pro-actively.

[18] So far, Schindler says, it has only used this information to coach employees and to raise awareness about safe driving. It is possible, however, that it may use the data to initiate discipline.

[19] According to Schindler, between June 2010, shortly after Fleet Complete was implemented, and June 2011, it recorded a year-over-year drop in accident costs of over 30%. It believes this drop stems from heightened employee awareness around speeding, harsh braking and harsh acceleration, and that this has improved safety for employees.

[20] As for safety, Schindler cites one example where concerned co-workers could not find an employee and the system allowed it to track down an employee who was unaccounted for. Fleet Complete, Schindler therefore says, allows it to ensure its employees are safe. It also says the system helped with an investigation into a workplace fatality involving a mechanic.

Vehicle maintenance and security

[21] Data about engine use and status, Schindler says, helps it schedule vehicle maintenance more efficiently. The information also allows it to address overuse and underuse of specific vehicles, allowing it to more efficiently level out vehicle wear and tear on a fleet basis.

[22] GPS data have also enabled Schindler to locate two vehicles that had been stolen.[13]

Hours of work

[23] Schindler says it uses GPS data and engine status data alongside other tools to deal with performance and related disciplinary matters. It says it does not discipline an employee for actions discovered solely through GPS data. That data, Schindler says, can assist in determining what actually occurred. Schindler also acknowledges, however, that GPS data will often be the only means by which it can establish whether an employee has been truthful about their activities during the work day.

[24] Because its mechanics have considerable autonomy in their work, Schindler cannot verify their locations and activities at all times. For this reason, when a complaint or other event triggers an inquiry, Schindler may use GPS data as part of its investigation. It says there have been several examples where that information has been vital.

[25] It gives the example of a British Columbia-based mechanic who was terminated, after investigation, for theft of time and personal use of his work vehicle. GPS data revealed personal use of his vehicle in off-work hours; engine status data, it appears, indicated that he had not worked the hours he was required to (with some 36% of claimed work time not actually having been worked).

[26] It offers a similar example from Ontario, where a Schindler supervisor by chance saw an employee driving his work vehicle in a city some distance from his assigned route. Schindler says that GPS data helped establish improper personal use of the vehicle and that the employee had not worked the hours he was supposed to.

[27] Schindler says it uses engine status data to assist in determining whether an employee has worked the hours she or he is required to work. According to Laurie Verbruggen's evidence, Schindler will use engine status data when a weekly 'exception report' suggests, based on the time on which a vehicle engine was first turned on or later turned off, that an employee was not at work for his or her scheduled hours. Her evidence is that the exception reports are triggered, as their name suggests, exceptionally, only when "a rule is broken" and they "do not arise where the vehicle is operated normally", according to the limits mentioned above.[14] Schindler says, again, that engine status data only

[13] Verbruggen affidavit, para. 42.
[14] Verbruggen affidavit, para. 14.

supplement other methods for investigating concerns triggered by these reports. The employee involved is given a full opportunity to respond and explain the circumstances.

[28] **'Personal Information' Under PIPA**—According to the complainants, all of the information that Schindler collects from the system is 'personal information' within the meaning of s. 1 of PIPA. Schindler argues it is not. It also argues, in the alternative, that the information is 'work product information'. If Schindler is correct on either point, PIPA does not apply to collection and use of the information.

[29] Section 1 of PIPA defines 'personal information' as follows:

> "personal information" means information about an identifiable individual and includes employee personal information but does not include
>
> (a) contact information, or
> (b) work product information.

[30] The parties devoted a good deal of time to the meaning of PIPA's definition of 'personal information'. Because of the importance of that question in this case, and in similar cases, I will deal with that question at some length.

The parties' perspectives on 'personal information'

[31] The complainants say the Fleet Complete system collects information about the movements, location and driving habits of identifiable employees. The employees are identifiable using information that Schindler possesses as to vehicle assignments and about each employee's work assignments. The information, therefore, is personal information under PIPA.

[32] The complainants also cite various court and other decisions to support their argument that the information in issue is information about identifiable individuals and is personal information. They say the Supreme Court of Canada has indicated that an "expansive" interpretation of 'personal information' is warranted.[15] According to them, a decision of the Office of the Privacy Commissioner of Canada, PIPEDA Case Summary 2006-351, is determinative of whether this is personal information.

[33] Schindler argues that a purposive interpretive approach is necessary, but this must not be an overly expansive interpretation.[16] It says 'personal information' "should not be defined 'literally', as an 'expansive intake' mechanism

[15] Initial submission, paras. 67ff.
[16] Initial submission, para. 33.

to scoop as much information under the scope of PIPA as possible."[17] According to Schindler, PIPA's definition of personal information, which refers to information "about an identifiable individual", does not encompass the GPS data or engine status data. It acknowledges that the information it collects relates to identifiable individuals,[18] but argues that, because the information is not truly "about" them, it is not personal information. The information is, rather, "about" Schindler's vehicles, and the fact that it "may be linked to an employee is irrelevant", it being no more personal information than "operating statistics of a machine in a factory are personal information of one or more of the operators." [19] Schindler says that 'personal information' is "about" someone only if it is all of these things: "about oneself", "could be considered in a fundamental way to be the individual's own", *and* is information "which the person could reasonably expect to treat as confidential and under his control".[20]

[34] Schindler relies on court decisions under the federal *Privacy Act*, decisions under the *Canadian Charter of Rights and Freedoms*, and an Alberta Court of Appeal decision under that province's *Personal Information Protection Act*. It also relies on a British Columbia labour arbitration decision about engine status information. All of these authorities, Schindler says, support its contention that this case does not involve personal information.

Federal access and privacy decisions

[35] Schindler and the complainants both place considerable emphasis on the Supreme Court of Canada's decision in *Dagg v. Canada (Minister of Finance)*.[21] That case dealt with the definition of 'personal information' under the federal *Privacy Act*. They also address *Canada (Information Commissioner) v. Canada (Canadian Transportation Accident Investigation and Safety Board*).[22] Schindler places particular reliance on that decision (to which I will refer as "*NAV Canada*").

[36] I will first discuss *Dagg*, which arose from an access to information request under the federal *Access to Information Act*. The applicant sought copies of sign-in logs for a federal government office building for a specific month. The logs recorded the names, identification numbers and signatures of employees entering the building on weekends, as well as their location in the building and the times of their arrival and departure. Before disclosing the logs, the government redacted employees' names, identification numbers and signatures.

[17] Initial submission, para. 33.
[18] Reply submission, para. 16.
[19] Initial submission, para. 10.
[20] Initial submission, para. 33.
[21] [1997] 2 S.C.R. 403.
[22] 2006 FCA 157, leave to appeal denied, [2006] S.C.C.A. No. 259 (Q.L.).

[37] The question was whether the redacted information was excluded from the *Privacy Act* definition of 'personal information' by s. 3(j) of that Act, which excluded "information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including…the classification, salary range and responsibilities of the position held by the individual". At its heart, the issue was whether the information was about the position or about the employee.[23]

[38] Writing for the majority, Cory J. reasoned that the information was about the position on the basis that the number of hours spent at the workplace generally relates to the position or functions of the individual, and provides a general indication of the responsibilities associated with the position. Further, there was no subjective aspect or element of evaluation in the log records that would relate the information to the individual.

[39] La Forest J., writing in dissent, emphasized the importance of a broad interpretation of 'personal information' in light of the legislative intention, under the federal access and privacy regime, to make privacy paramount over access. He said the definition of 'personal information' was intended to capture all information about a specific person, subject only to specific exceptions, and noted that information relating to the number of hours worked by a particular employee is considered personal information under Ontario's *Freedom of Information and Protection of Privacy Act*. While he acknowledged that it was not strictly necessary to his analysis, he also found that a reasonable expectation of privacy favoured a conclusion that the information was personal information. He would have held that the information was about the individual and not the position.

[40] It is noteworthy that Cory J. agreed with La Forest J. that employees' names on the sign-in logs were their personal information. Their point of disagreement was whether the exclusionary language of s. 3(j) captured that and other information, with Cory J. finding that it did. Cory J. expressly agreed, however, with La Forest J.'s approach to interpreting the term 'personal information'. The difference between majority and minority, in other words, had to do with other aspects of the statutory scheme.

[41] In *NAV Canada*, the Federal Court of Appeal adopted a narrower definition of the meaning of personal information in the workplace context than was favoured in *Dagg*. *NAV Canada* involved a request under the federal access to information law for access to recorded communications between cockpit occupants and air traffic controllers. The central issue was whether the

[23] At the federal level, the *Access to Information Act* and the *Privacy Act*, although separate statutes, interact to define the scope of the right of access to information under the former.

recordings were 'personal information' under the federal *Privacy Act* and *Access to Information Act*.

[42] The Federal Court of Appeal acknowledged that 'personal information' can be defined very broadly, to encompass information about an identifiable individual, without more,[24] but went on to reject this approach. Instead, it held that personal information must be understood as "equivalent to information falling within the individual's right of privacy".[25] Adopting what it described as a "privacy-based interpretation" of personal information, the Court considered the meaning of privacy, which it described as connoting "concepts of intimacy, identity, dignity and integrity of the individual".[26] The Court, in my view, equated "personal information" with "personal life", distinguishing it from an individual's professional life, including work performance:

> 54**.** The information contained in the records at issue is of a professional and non-personal nature. The information may have the effect of permitting or leading to the identification of a person. It may assist in a determination as to how he or she has performed his or her task in a given situation. But the information does not thereby qualify as personal information. It is not *about* an individual, considering that it does not match the concept of "privacy" and the values that concept is meant to protect. It is *non*-personal information transmitted *by* an individual in job-related circumstances. [original emphasis]

[43] The Court also said the conversations had "no personal content",[27] and thus did not qualify as 'personal' information.

[44] Schindler relies on *NAV Canada* to support its argument that 'personal information' ought not to be interpreted expansively, that the term should be approached using a privacy-based interpretation, one which sees privacy as connoting "concepts of intimacy, identity, dignity and integrity of the individual".[28] There is no doubt that, at a general conceptual level, privacy may be considered to involve interests such as intimacy, identity, dignity and integrity of the individual. It is, however, one thing to posit theoretical perspectives on what 'privacy' means in the abstract and quite another to use such concepts to drive the interpretation of statutory language.

[45] The Supreme Court held, in *Dagg* that the *Privacy Act* definition of 'personal information' is expansive. It was equally clear on this in the later

[24] *NAV Canada*, para. 43.
[25] *NAV Canada*, para. 44.
[26] *NAV Canada*, para. 52.
[27] *NAV Canada*, para. 55.
[28] *NAV Canada*, para. 52.

decision of *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police*).[29] There is, to be sure, some tension between the interpretive approach in *Dagg* and *Royal Canadian Mounted Police* and the approach in *NAV Canada*.[30]

[46] I certainly respectfully disagree with the reliance in *NAV Canada*, in the face of those Supreme Court decisions, on *Charter* decisions to interpret the definition of the term 'personal information' enacted by Parliament. *Charter* values are of assistance in statutory interpretation, but cases decided under the *Charter*—which does not explicitly mention 'personal information' or 'privacy' and has a different goal than, for example, PIPA—should be used with caution in the face of the statutory language and purposes of laws like the *Access to Information Act*, the *Privacy Act* and, perhaps even more so, PIPA.[31]

[47] An added consideration is that these court decisions all involve interpretation of federal public sector access to information and privacy legislation. The goal of such legislation is, on the one hand, to foster government openness and, on the other, protection of individuals' privacy, all in accordance with the legislative language Parliament employed.[32]

[48] These cases do, however, serve to underscore the importance of statutory interpretation in determining the meaning of 'personal information' under PIPA, including in relation to employment. If the intention of the Legislature in defining 'personal information' in PIPA were to create a zone of 'personal privacy', a realm described in *NAV Canada* as concerned with "intimacy, identity, dignity and integrity of the individual", then very little information about an individual in his or her capacity as an employee would be considered personal information. If, however, the intention of the Legislature was to address all information that is capable of identifying an individual, 'personal information' would include a great deal of information indeed.

[49] In my view, the purposes, structure and wording of PIPA point to a broader definition of personal information than that adopted by the Federal Court of Appeal in *NAV Canada*.[33] Nothing in PIPA suggests that 'personal'

---

[29] 2003 SCC 8, [2003] 1 S.C.R. 66.

[30] The Court of Appeal in *NAV Canada* referred to the Supreme Court's decision in both cases.

[31] In a similar vein, I note that Doherty J.A. recently said, in *R. v. Ward*, 2012 ONCA 660, a *Charter* case, that s. 8 of the *Charter* "is not about protecting individual privacy…as between non-state actors."

[32] This was acknowledged by the Supreme Court in, for example, *Dagg* and in *H. J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, 2006 SCC 13, [2006] 1 S.C.R. 441, a case also cited in *NAV Canada*.

[33] It also has to be noted that even though it is an appellate decision, *NAV Canada* has not been influential in at least two later Federal Court trial level decisions. The first of these also dealt with the federal access to information and privacy scheme: *Gordon v. Canada (Health)*, 2008 FC 258. The second, *Girao v. Zarek Taylor Grossman Hanrahan LLP*, 2011 FC 1070, arose under PIPEDA.

information was intended to be confined to a personal zone of privacy or intimacy outside or within the worlds of work and commerce. Rather, the purposes of PIPA are achieved by a definition of personal information that facilitates the mandated balancing of the interest in protecting it with the interest in using it in accordance with the legislatively-prescribed standards. I return to this issue later, but first will discuss other decisions the parties cited.

Other decisions about what is 'personal information'

[50] The complainants and Schindler rely on federal decisions and authorities from Ontario and Alberta to support their opposing interpretations.[34]

[51] Within the statutory framework of PIPEDA, the Office of the Privacy Commissioner of Canada ("federal Privacy Commissioner") has determined that information derived from tracking technology on vehicles is personal information. The complainants therefore rely, not surprisingly, on PIPEDA Case Summary 2006-351,[35] which involved use of technology in circumstances somewhat resembling the present case. The system disclosed vehicle start and stop times, speed, location, mileage and off-shift parking location. The employer argued that this was information related to a vehicle, not location information associated with a particular individual. The Assistant Privacy Commissioner found that, because the information collected "can be linked to specific employees driving the vehicles, they are identifiable even if they are not identified at all times to all users of the system."[36] She concluded that the information was personal information covered by PIPEDA. The company's stated purposes for collecting the information were to manage workforce productivity, ensure safety and protect and manage its assets. The Assistant Privacy Commissioner found that the loss of privacy entailed by the company's use of the information was proportional to the benefit gained, and she also held that there was no less privacy-intrusive alternative.

[52] A similar conclusion was reached in PIPEDA Case Summary 2009-011, which concerned mobile data terminals with GPS devices. These had been installed by a municipal transportation company in vehicles used to provide transportation services to mobility-impaired individuals. The primary purpose of the system was to improve dispatch efficiency and route scheduling, to provide clients with more accurate vehicle arrival information, and for emergency location. The Assistant Privacy Commissioner found that the information

---

[34] While interpretive approaches in other jurisdictions can be helpful, care must, of course, be taken to respect differences between the various laws.

[35] http://www.priv.gc.ca/cf-dc/2006/351_20061109_e.asp. The complainants also cites PIPEDA Case Summary 2009-011, http://www.priv.gc.ca/cf-dc/2009/2009_011_0527_e.asp, a similar case in which a similar view was expressed.

[36] Page 2.

collected was personal information, but it was not particularly sensitive and the interests in collecting it were legitimate.[37]

[53] The findings in these two cases support a definition of 'personal information' that is broader than Schindler advances. Other findings of the federal Privacy Commissioner also support a broader definition for PIPEDA purposes. In PIPEDA Case Summary 2003-220,[38] for example, a telemarketer objected to her employer sharing her sales results with other employees. This was held to be 'personal information' within the meaning of PIPEDA. As the summary indicates:

> - Although it is recognized that sales statistics of individual employees are information that the company itself generates, records, and processes for reasonable and legitimate business purposes, it is nonetheless clear that sales records attributed to the complainant in order to indicate her on-the-job performance relative to that of others constitute information about her as an identifiable individual.
> - Since there is nothing in the Act to suggest that personal information and company information must always be mutually exclusive, we find the information at issue to be personal information for purposes of the Act.

[54] Another example is PIPEDA Case Summary 2005-303,[39] where a real estate broker published the names of the top five sales representatives in a city. The complainants were not that broker's employees. The Assistant Privacy Commissioner of Canada found that this involved 'personal information'.

[55] Schindler argues that summaries of findings under PIPEDA are of limited use—particularly Case Summary 2006-351—because they do not fully set out the reasoning applied by the federal Privacy Commissioner. I acknowledge that these are only summaries, but find them useful in illustrating the kinds of information that have, in the result, been found to be 'personal information' under PIPEDA.

[56] Both parties refer to *Eastmond v. Privacy Commissioner of Canada*,[40] a Federal Court decision under PIPEDA. Schindler argues that it is distinguishable because it was about constant overt video surveillance of a workplace, which would have captured every action of an employee. Schindler says this surveillance would inevitably capture information of a truly 'personal' nature—information "that does belong in the 'private sphere'"[41]—as employees

---

[37] It is important to underscore that the Assistant Commissioner there noted that the technology was not being used for employee management—it was only being used to improve delivery of the transit service and for client safety.
[38] http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030915_e.asp.
[39] http://www.privcom.gc.ca/cf-dc/2005/303_20050531_e.asp.
[40] 2004 FC 854.
[41] Initial submission, para. 49.

went about their work day.[42] Here, Schindler says, there is only intermittent collection of "data", data "about the operation of a Schindler-owned asset."[43] Although Schindler's attempt to distinguish between "constant" video surveillance and its practices is not persuasive, *Eastmond* is by no means determinative of whether the information here falls within PIPA's definition of 'personal information'.

[57] In *University of Alberta v. Alberta (Information and Privacy Commissioner)*,[44] the court held that, even if an individual is not specifically named in a record, the context in which information is given, its nature, content and other factors may mean that an individual is identifiable, thus making the information 'personal information'. The case involved a request for access to a statistical summary of teaching effectiveness and the number of published papers of faculty members in a department. This was found to contain personal information because the evidence was that some of the complainant's colleagues had identified him from the summary.

[58] Similarly, in *Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner)*,[45] the Ontario Divisional Court concluded that the proper test is whether it is reasonable to expect that, when information is combined with information from sources otherwise available, an individual can be identified. The Ontario Court of Appeal upheld this decision.[46]

[59] Alberta's *Personal Information Protection Act* ("Alberta's PIPA"), the private sector privacy legislation closest to PIPA, defines personal information as "information about an identifiable individual." This term has been considered in decisions and publications of the Office of the Information and Privacy Commissioner of Alberta. In Investigation Report P2005-IR-009,[47] an individual was using his own vehicle for work purposes with his employer's agreement. The organization had a policy on safe driving. When the employee had an accident, the employer obtained data from the vehicle's event data recorder ("EDR"). The Office had to consider whether the EDR data qualified as 'personal information' under Alberta's PIPA:

> [20] PIPA subsection 1(k) defines "personal information" as information about an identifiable individual. The EDR does not itself identify an individual. It does not collect the name or other personal characteristics of

[42] Initial submission, para. 49.
[43] Initial submission, para. 49.
[44] 2009 ABQB 112.
[45] (2001), 154 O.A.C. 97 (ONSC Div. Ct.), affirmed *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300, (2002), 166 O.A.C. 88 (Ont. C.A.).
[46] This same approach was applied by an adjudicator in the Office of the Information and Privacy Commissioner of Ontario in Order PO-2811, [2009] O.I.P.C. No. 127, which was recently upheld by the Ontario Court of Appeal, in *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2012 ONCA 393.
[47] [2005] A.I.P.C.D. No. 46.

> individuals driving the motor vehicle. It does, however, retain the driving data of whoever was operating the vehicle during the (normally) 5 seconds prior to a "triggering event". A triggering event can be either a "Deployment Event" or a "Non-Deployment Event". A Deployment Event normally involves the deployment of the vehicle's emergency restraint system (the airbags). A Non-Deployment Event is an event severe enough to "wake up" the sensing algorithm in the EDR, but not severe enough to deploy the airbags in the vehicle. The EDR can record the vehicle's speed, engine speed, throttle position, the status of the brake light switch, and the status of the driver's seat belt buckle switch (buckled or unbuckled) at the time of the event. This information is stored in a buffer that is capable of storing five values of each data element. Values are recorded at one-second intervals. The data can then be downloaded into readable format.
>
> [21] When E.P. was involved in the motor vehicle crash (a "Non-Deployment Event"), and called in to Precision to report the crash, he was identified as the driver of the vehicle, and any driving data collected by the EDR would be about him as the driver of that vehicle. Precision did not seek to obtain the EDR data in order to determine who was driving the vehicle; they already knew who was driving. Rather, Precision was seeking to obtain detailed information about the manner in which E.P. was operating the vehicle prior to the crash. I am therefore satisfied that the EDR data is in fact "information about an identifiable individual" as contemplated by PIPA.

[60] In Alberta Order P2009-005,[48] an adjudicator considered what is 'personal information' under Alberta's PIPA. An individual had asked an organization for access to information about payments an insurer had made to the organization and its psychologists. The organization provided information about hourly rates, but did not provide details of what staff and consultants were paid. The organization said this was not "about" him, and thus was not his personal information. This meant he had no right of access to it under Alberta's PIPA. The adjudicator said this:

> [para 34] Here, I find that the information that the Applicant requested about how much the Organization paid the doctors and workers on the team that treated him – as well as the information he requested about how much the Co-operator's paid the Organization – is not his personal information. The evidence is that the Applicant's treatment was covered by the Co-operator's and that he did not pay for any professional services or treatment himself. The information regarding payments and fees existed as a result of the Applicant's treatment exists as a result of the Applicant's treatment, so that it is connected to him in some way, but it is not "about" the Applicant.

[48] [2010] A.I.P.C.D. No. 4.

> [para 35] Finally, the possibility that the amounts of the various payments might indirectly reveal something about the Applicant's treatment, such as how much treatment he received, does not mean that it is his personal information. There should be a more direct connection between the information requested and the applicant requesting it in order to make the information "about" him or her rather than merely "related" to him or her.

[61] As I read this decision, information about payments by the insurer to the organization were not about the applicant because they did not relate directly enough to him. He had received treatment at no cost, so the payment-related information was not relevant to his treatment. His treatment was, under the insurance, the reason for the payments, but the relationship between that funding and the applicant was insufficiently direct. Nowhere did the adjudicator say that information must be "about" someone in the sense argued by Schindler or advanced in *NAV Canada*.[49]

[62] The last Alberta case is one on which Schindler places emphasis. *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*, a split decision of the Alberta Court of Appeal,[50] dealt with a retailer that collected driver's licence and licence plate information from individuals who picked goods up at its stores.

[63] The retailer argued, among other things, that the information it collected was not personal information under Alberta's PIPA. The Court was unanimous in deciding that driver's licence numbers are personal information, but divided on the question of whether vehicle licence plate numbers are personal information. The majority concluded that they are not on the basis that vehicle license plates are "about" the vehicle, not "about" an individual. Slatter J.A. said this for the majority:

---

[49] It should also be noted that, at para. 36, the adjudicator underscored how important circumstances are: "I do not preclude the possibility of a future case where information about fees not actually paid by an individual might be his or her personal information. The answer depends on the nature of the request and the facts and circumstances."

[50] 2011 ABCA 94, leave to appeal to the Supreme Court of Canada denied, 2011 CanLII 75051. At para. 8 of its reply submission, Schindler mentions that leave was denied in *Leon's* and also in *NAV Canada*, adding that this makes "two recent court of appeal decisions which advocated a focused, purposive approach to the definition of 'personal information', and in which the Supreme Court has denied leave." I do not understand denial of leave to appeal to necessarily mean that the Supreme Court of Canada endorses the reasoning, much less the outcome, in a lower court. Section 40(1) of the *Supreme Court Act* provides that leave may be granted where the Supreme Court is of "the opinion that any question involved" in the case is, because of its "public importance" or the "importance of any issue of law or any issue of mixed law and fact…one that ought to be decided by the Supreme Court", or is, "for any other reason, of such a nature or significance as to warrant decision by it".

> [47] The "identifiable individual" term has two components. Firstly, the individual must be "identifiable". Generic and statistical information is thereby excluded, and the personal information (here, the relevant number) must have some precise connection to one individual. Secondly, the information must relate to an individual. Information that relates to objects or property is, on the face of the definition, not included.
>
> [48] Further, to be "personal" in any reasonable sense the information must be directly related to the individual; the definition does not cover indirect or collateral information. Information that relates to an object or property does not become information "about" an individual just because some individual may own or use that property. Since virtually every object or property is connected in some way with an individual, that approach would make all identifiers "personal" identifiers. In the context of the statute, and given the purposes of the statute set out in s. 3, it is not reasonable to expand the meaning of "about an individual" to include references to objects that might indirectly be affiliated or associated with individuals. Some identification numbers on objects may effectively identify individuals. Many, however, are not "about the individual" who owns or uses the object, they are "about the object."
>
> [49] The adjudicator's conclusion that the driver's license number is "personal information" is reasonable, because it (like a social insurance number or a passport number) is uniquely related to an individual. With access to the proper database, the unique driver's license number can be used to identify a particular person: *Gordon v. Canada* [citations omitted]. But a vehicle license is a different thing. It is linked to a vehicle, not a person. The fact that a vehicle is owned by somebody does not make the license plate number information about that individual. It is "about" the vehicle. The same reasoning would apply to vehicle information (serial or VIN) numbers of vehicles. Likewise a street address identifies a property, not a person, even though someone might well live on the property. The license plate number may well be connected to a database that contains other personal information, but that is not determinative. The appellant had no access to that database, and did not insist that the customer provide access to it.

[64] Slatter J.A. also placed some weight on the fact that licence plates are visible to everyone:

> [50] It is also contrary to common sense to hold that a vehicle licence number is in any respect private. All vehicles operated on highways in Alberta must be registered, and must display their licence plates in a visible location: *Traffic Safety Act*, R.S.A. 2000, c. T-6, ss. 52(1)(a) and 53(1)(a). The requirement that a licence plate be displayed is obviously so that anyone who is interested in the operation of that vehicle can record the licence plate. The fact that the licence plate number might be connected back to personal information about the registered owner is obvious, but the

> *Traffic Safety Act* nevertheless requires display of the licence plate. Control of that information is provided by controlling access to the database. It makes no sense to effectively order, as did the adjudicator, that everyone in the world can write down the customer's licence plate number, except the appellant.

[65] In dissent, Conrad J.A. vigorously rejected the view that the purpose of Alberta's PIPA is to only protect a 'zone of privacy' or a 'reasonable expectation of privacy' and that these concepts should inform the definition of 'personal information':

> [120] Much was made at the appeal hearing about licence plate numbers and the fact that they are publicly displayed. It was argued that because anyone can copy down a licence plate number, these numbers cannot amount to personal information about an individual as there is no expectation of privacy concerning them. But, as discussed above, this legislation is not designed to protect an expectation of privacy. Nor is it designed to protect against the collection, use and disclosure of personal information by one's neighbour. It is aimed at organizations. PIPA is the Legislature's acknowledgment that the use of modern technology in commerce has made vast quantities of personal information publicly available, and while it is impossible to regulate the flow of information about individuals completely, it is possible to control its collection, use and disclosure by organizations. Every datum centralized in one locale increases the ease of targeting an individual for mass marketing or identity theft.

[66] Schindler relies on the majority reasons in *Leon's Furniture*, saying this:

> Together, *NAV Canada* and *Leon's Furniture* demonstrate that on a purposive interpretation, the definition of "personal information" in PIPA should extend only to that information which is truly "about" an individual. It is not enough that the information merely be connected in some way to an individual, or that an observer can discern something about the individual by examining the information.[51]

[67] I do not necessarily agree that *Leon's Furniture* goes as far as Schindler implies. But to the extent that the majority judgement in *Leon's Furniture* might in fact suggest that 'personal information' is limited to a class of information that is 'private' in some sense, I respectfully disagree as regards PIPA.

[68] The parties in this case also referred to court decisions interpreting s. 8 of the *Charter*, which protects Canadians against unreasonable search and seizure by the state. In many cases, the Supreme Court of Canada has held that s. 8

[51] Initial submission, para. 26.

protects a "reasonable expectation of privacy", and in some cases a "zone of privacy" has been mentioned. The meaning of what is "privacy" for the purposes of constitutional scrutiny of state action does not greatly advance understanding of what the Legislature intended 'personal information' to mean under PIPA.[52]

[69] Arbitrators have considered whether information relating to employees is 'personal information' within the meaning of information and privacy laws, often in circumstances where the employer has conducted surveillance in the workplace and used it to terminate or discipline an employee. While these cases focus primarily on whether surveillance is a reasonable exercise of management rights under the collective agreement, there is no doubt that the product of surveillance, certainly, is considered to be personal information.[53]

[70] One notable exception involving monitoring technologies is *Otis Canada Inc. v. International Union of Elevator Constructors, Local 1*.[54] Schindler relied on this decision in implementing its use of Fleet Complete, and relies on it here. That case arose from a union policy grievance regarding an employer's adoption of telematics devices in employer-owned vehicles. The technology appears to be similar to that in issue here. It was installed in the vehicles and provided information such as start and stop times; idling and speeding reports; mileage; driving times and stop times; gas consumption; and speed.

[71] The arbitrator found that the PIPA test for what is personal information has two elements. First, the information must relate to an *identifiable* individual, and second, it must be *about* that individual. On the evidence, he concluded that the first element was satisfied because the information received by the employer from the devices identified individual employees. He then turned to the question of whether the information is "about" the individual. Although he accepted, citing *NAV Canada*, that the scope of "privacy legislation is 'undeniably expansive'", he read the statutory definition in s. 2 of PIPA in an extremely narrow manner:

> …I do not read this definition to mean that "personal information" includes any and all information about an individual. This is demonstrated, first of all, by the two exceptions to the definitions of personal information, "contact information" and "work product information".

[72] If the arbitrator intended by this to suggest that the exclusion of 'contact information' and 'work product information' from 'personal information' narrows the scope of 'personal information', I respectfully disagree. I do not interpret the express exclusion of two specific categories of information from language

[52] Conrad J.A. made a similar point in *Leon's Furniture*, at para. 111.
[53] See, for example, *Teamsters, Local 419 v. Securicor Cash Services*, [2004] O.L.A.A. No. 99.
[54] [2010] B.C.C.A.A.A. No. 121.

expressed in general terms as signifying an intention that the general language itself is to be given limited scope.[55] There would, in my view, be no need to exclude "contact information" and "work product information" from "personal information" unless the opening language of the definition is otherwise broad enough to encompass the specifically excluded classes.

[73] This is the first order under PIPA where the meaning of 'personal information' is so squarely in dispute. The interpretive approach to PIPA, however, is clear, and I do not, with all due respect, think the arbitrator in *Otis* took the proper approach. PIPA's provisions are to be interpreted in light of its purpose and scheme:

> Today there is only one principle or approach, namely the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.[56]

[74] As to the "object" of PIPA, and the Legislature's intention, s. 2 says this:

> The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need for organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[75] Neither s. 2 nor PIPA's other provisions refer expressly to 'privacy' or a 'reasonable expectation of privacy'. Nor does PIPA articulate a distinction between spheres of 'public' and 'private' life. Rather, it recognizes that organizations have a "need" to collect, use and disclose personal information and protects their interests in doing so. At the same time, PIPA recognizes the "right" of individuals to protect their personal information.[57] PIPA's statutory objective, then, is to balance the competing values of protecting personal information and permitting its use by organizations for purposes that are appropriate in the circumstances.

---

[55] See, for example, R. Sullivan, *Sullivan on the Construction of Statutes*, 5th ed. (LexisNexis: Toronto, 2008), at p. 231 and following.

[56] *Rizzo & Rizzo Shoes Ltd.,* [1998] 1 S.C.R. 27, para. 21. The Supreme Court of Canada has repeatedly affirmed this interpretive approach since Rizzo. For the most recent examples, see Reference re Broadcasting Regulatory Policy CRTC 2010-167 and Broadcasting Order CRTC 2010-168, 2012 SCC 68, and *Re: Sound v. Motion Picture Theatre Associations of Canada*, 2012 SCC 38. Also, s. 8 of the *Interpretation Act* provides that a statute is to be interpreted "as being remedial, and must be given such fair, large and liberal construction and interpretation as best ensures the attainment of its objects."

[57] The same view regarding PIPA's interpretation, and the balancing of interests that it seeks, was expressed in Order P05-01, [2005] B.C.I.P.C.D. No. 18, at paras. 42 and following.

[76] Properly interpreted, the definition of personal information covers information that is "about" the individual in a wider sense than the zone of intimacy, privacy or dignity ascribed to it in *NAV Canada* and *Otis*. In *Otis*, like the Court in *NAV Canada*, the arbitrator turned—unhelpfully, in my view, as I earlier suggested—to cases under the *Charter of Rights and Freedoms*. I have already explained why *Charter* decisions are neither directly applicable to interpretation of PIPA nor persuasive given the contextual differences. I have also explained why *NAV Canada* is not persuasive.

[77] Nor do I think the arbitrator's reliance on the distinction drawn in Ontario decisions between personal information and information in business capacities is well placed. Among other things, Ontario's *Freedom of Information and Protection of Privacy Act* contains no employment-related provisions and the Ontario Information and Privacy Commissioner has interpreted the statute as implicitly addressing these issues.[58]

[78] In deciding whether the telematics information was 'personal information' under PIPA, the arbitrator also considered the purposes for which the information was collected. He found these to be reducing the employer's fleet costs and monitoring the use of company vehicles by employees (but unrelated to location). He held that the information collected through the devices was not personal information:

> 89. In fact, the nature of the form that contains the Telematics data (reproduced above) is that the only information that is "personal" is the name of the employee/driver/mechanic. All the other information on the form relates to vehicle operation. I note that one of the exceptions to "personal information" in PIPA is "contact information" and this includes the name of the individual. I do not conclude that the Telematics data is "contact information" but I reason by way of analogy that the name of an employee is not necessarily protected from disclosure as "personal information". Similarly, I am unable to find that the inclusion of an employee's name in the data reveals "intimate details" of that employee's life (*Plant, supra*). To paraphrase *Nav Canada, supra,* the information at issue is of a professional and non-personal nature (paragraph 54, emphasis in original).
>
> 90. It is true that the data contains information about the stop times of a vehicle and this may also be information about the activities of the driver/employee. However, I agree with the analysis in *Nav Canada, supra,* that this type of information does not engage the right to privacy of individual employees. It is also true that the Telematics data may lead to

[58] I will note here as well that this Office has rejected the Ontario test in decisions under the *Freedom of Information and Protection of Privacy Act*. See, for example, Order F08-03, [2008] B.C.I.P.C.D. No. 6.

> decisions by the Employer to discipline employees. There are two responses to this concern. First of all, the data does not provide a complete or reliable picture of the activities of an individual and other information would be required to sustain just cause for discipline (actual cases of discipline will have to be judged on their individual circumstances).
>
> 91**.** Second, to paraphrase *Nav Canada,* the possible use of the data to evaluate the performance of employees does not transform the information into personal information under PIPA.[59] The information may have the effect of permitting or leading to the identification of a person and it may assist in a determination as to how he or she has performed his or her task in a given situation. "But the information does not thereby qualify as personal information. It is not about an individual, considering that it does not match the concept of "privacy" and the values that concept is meant to protect. It is non-personal information transmitted by an individual in job-related circumstances" (*Nav Canada, supra,* paragraph 54, emphasis in original). I note in *Nav Canada* that the information related to recorded communications of employees and there was no real dispute that the information was *about* the employees. Therefore, it was more directly applicable to issues of discipline than the information in this case which primarily relates to the operation of company vehicles.
>
> 92. In summary, I am not persuaded that the collection and use of an employee's name, by itself, is collection and use of information that is "fundamental" to the "dignity and integrity" of the employee (*Dyment, supra*). Put another way, in the circumstances of this case, the collection of information about the operation of a company vehicle, that also includes the name of the driver of the vehicle, does not transform that data into "personal information" under PIPA. I conclude that the data from the Telematics devices can be considered in the same way as the information obtained from the tachograph in *Dominion Dairies, supra.* The Employer in this arbitration is entitled to know what its employees are doing when they are working and when they are using company vehicles. This information assists management by providing reliable and objective information to improve the efficiency of the vehicle fleet. The same information is not "about" an individual employee and it may be used as part of Employer investigations of disciplinable offences without violating the privacy of employees. As stated in *Nav Canada, supra,* information that is transmitted by an individual in job-related circumstances is not information about that individual.

[79] In this passage, the arbitrator acknowledged that the information might enable an employee to be identified and that "it may assist in a determination as to how he or she has performed his or her task in a given situation." This qualitative aspect to the information was not enough, however—it was not 'about' an employee because it did not "reveal 'intimate details'" of an employee's

[59] As will be seen below, I strongly disagree with this assertion—if correct, it could eviscerate PIPA's employment privacy framework.

life. Similarly, the arbitrator acknowledged that the information "may lead to decisions by the Employer to discipline employees."[60]

[80] This reasoning is not, with deference, persuasive.[61] Again, the meaning of the term 'personal information' must be viewed in light of the purpose of PIPA, its structure and context. In the context of cases such as this, decisions from elsewhere show that information relating to management of an individual employee's relationship with her or his employer is likely to be personal information.[62] Limiting 'personal information' to a personal zone of privacy or intimacy is not consistent with the structure or purposes of PIPA.

[81] In summary, I do not consider *Otis* to be persuasive and decline to apply its reasoning in interpreting the term 'personal information' under PIPA.

[82] The question, then, is whether the test for personal information requires both that the information must be about an identifiable individual *and* that it be "about" that individual. Cases in all jurisdictions, including under British Columbia's *Freedom of Information and Protection of Privacy Act*, agree that, to be personal information, the information must be capable of distinguishing (identifying) a particular individual. I accept that, in order to be personal information, the information must be reasonably capable of identifying a particular individual either alone or when combined with information from other available sources. The information need not identify the individual to everyone who receives it; it is sufficient in a case such as this if the information reasonably permits identification of the individual to those seeking to collect, use or disclose it.

[83] What does an additional requirement that the information be "about" a particular individual add to this? The meaning of "about" as articulated in *NAV Canada* and *Otis* is, again, not appropriate under PIPA. They view the term "about" as restricting personal information to information which relates to the individual in a personal, as opposed to employment, business or professional capacity. Where information can be used for multiple and perhaps equally important purposes, it is neither necessary nor helpful to read into PIPA's definition of personal information a requirement that information must be "about" an identifiable individual in some 'personal' or 'private' way. The reality is that the same information can be and often is used for multiple purposes. The mileage information collected by Fleet Complete, for example, can be (and is) used for

[60] The arbitrator attempted to respond to this by saying that more information would be needed to sustain just cause for discipline. It is not at all clear how this is a principled basis on which to conclude that the information in dispute is not, in itself, 'personal information'. Its sufficiency for discipline purposes is a separate issue.

[61] Further, the arbitrator emphasized that the devices used in *Otis* are not GPS-enabled and do not track employees' locations (see, for example, paras. 86-88), a fact that materially distinguishes *Otis* from aspects of this case, even if the *Otis* analysis were otherwise persuasive.

[62] An exception is *NAV Canada*, which, for reasons given above, I find is not persuasive.

purposes related to asset management (such as scheduling vehicle maintenance) and can also be used for purposes related to employee discipline (such as determining whether an employee is using the vehicle assigned to her or him for personal travel).[63]

[84] Further evidence of legislative intention is found in the special regime PIPA creates for 'employee personal information'. Under PIPA, the default position is that an organization must obtain consent to the collection, use and disclosure of an individual's personal information. There are exceptions to this, perhaps most notably in the employment context. Employers are permitted to collect, use and disclose 'employee personal information' without consent as long as the collection, use or disclosure is, roughly summarized, reasonable for employment relationship purposes. If the Legislature had intended a narrower, or more qualified, definition of personal information—for example, one that only encompasses an individual's 'personal' or 'private' life—provisions addressing collection, use and disclosure of 'employee personal information' would not be necessary because that information would not be governed by PIPA at all. It would restrict PIPA's scope in a way not supported by its purpose or structure to find that information that an organization such as Schindler collects, uses or discloses for a purpose related to an individual, including to make decisions affecting that individual—such as employment discipline decisions—is not personal information because it is not 'private' information of or about that individual.

[85] I conclude that '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. Consistent with PIPA's statutory purposes, this recognizes that information may be used for different purposes at different times.

[86] This duality of purpose, and thus nature, of information, to which I alluded earlier, has been recognized in cases involving employment relationships. For example, under Alberta's *Freedom of Information and Protection of Privacy Act* it has been held that the purpose for which information is sought helps to determine what the information is "about". In Order F2005-003,[64] an employer installed keystroke logging software on an employee's computer to determine how much work he did. Commissioner Frank Work noted that not all information entered into a computer has a personal aspect, but in that case it did, because it was collected for a purpose that made it information about the employee and his personal information:

---

[63] Schindler's submissions acknowledge this. Its policies on use of this kind of information explicitly acknowledge that it may be used for employment-related purposes, including discipline, though Schindler also maintains that this is not personal information.

[64] [2005] A.I.P.C.D. No. 23.

> [para 8] In this case I am of the view that if most or even all of the information that was collected was the Applicant's work-related activity, all of it had a personal component in this case, because it was to be used to determine how much work he did, or his style or manner of doing it, or his own choices as to how to prioritize it. Thus in my view the collected information included personal information of the Applicant. The Applicant also gave evidence that his personal banking information was also collected by the software program.

[87] A further example, also a public sector access and privacy law decision, is Order F07-18.[65] That British Columbia case also concerned an employer that had installed computer spyware on an employee's computer. The employer argued that information disclosing which websites were "visited by a particular computer" was not the employee's personal information. The adjudicator found that the purpose for collecting information was an important factor in determining whether the information was "about an identifiable individual", noting that "[t]he whole purpose of the collection was to demonstrate what the complainants were doing. It was not to simply gather information about how the computer itself was being used, without regard to who was using it".[66]

[88] While these decisions were made under public sector statutes both Order F07-18 and Alberta Order P2009-005[67] usefully illustrate how the character of information can differ depending on the circumstances.

[89] I will now apply these observations about what may qualify as 'personal information' to the evidence before me.

[90] **Is This Work Product Information?**—Schindler argues in the alternative that the GPS data and engine status data information constitute 'work product information', with the result that PIPA does not apply.[68] PIPA defines 'work product information' as follows:

> "work product information" means information prepared or collected by an individual or group of individuals as part of the individual's or group's responsibilities or activities related to the individual's or group's employment or business but does not include personal information about an individual who did not prepare or collect the personal information.

[65] [2007] B.C.I.P.C.D. No. 30.
[66] Para. 49.
[67] [2007] A.I.P.C.D. No 46.
[68] Schindler did not argue that this case involves 'contact information'. No such argument could in any case be made based on the evidence at hand.

[91] Schindler says the information in issue is 'work product information' because it is "generated" by employees in the course of their work. It relies on decisions under Alberta's PIPA.[69] According to Schindler, the

> …data are generated by employees in the course of their work and in relation to the employment tasks at hand, and then entered into and used in various business applications for various business purposes.[70]

[92] The information is, Schindler argues, not about the employee, "but rather records of the tasks performed and the fact of their performance."[71]

[93] The complainants say that, in order for information to be work product information, there must be an element of creativity in the information's preparation, and that is not the case here.[72]

[94] As I understand Schindler's argument, 'work product information' is any information that is "generated by employees in the course of their work".[73] As the complainants point out, PIPA does not refer to information "generated by" employees, the term Schindler uses.[74] It speaks of information "prepared or collected…as a part of the individual's…responsibilities or activities related to" their employment or business. The information in question may be 'generated', the complainants say, but it is generated by machines installed and operated by Schindler.

[95] Schindler relies on Alberta decisions such as Order P2006-005. Alberta's PIPA does not explicitly contemplate 'work product information', but various Alberta decisions interpret 'personal information' to accommodate a similar concept. The same can be said of decisions of the federal Privacy Commissioner. Decisions from these jurisdictions are not particularly helpful in interpreting and applying PIPA's express definition of 'work product information'.

[96] Schindler relies on Order P06-05,[75] a decision of former Commissioner Loukidelis, to support the notion that the information in issue here was "generated" by its employees. That case dealt with emails and other materials created by individuals who, using the organization's email resources, were working together to set up a competing business. Schindler's reliance on Order P06-05 is also misplaced. That case involved emails containing content that had been created—"prepared"—by individuals. In my view, information that comes

---

[69] Order P2006-004, [2006] A.I.P.C.D. No. 38 and Order P2006-005, [2006] A.I.P.C.D. No. 46.
[70] Initial submission, para. 58.
[71] Initial submission, para. 63. Schindler also acknowledges, at para. 62, that one of its "business purposes" may be to investigate misconduct of individual employees, including relating to misuse of a company vehicle.
[72] Complainant's reply submission, para. 21.
[73] Initial submission, para. 58.
[74] Complainant's reply submission, paras. 19-24.
[75] [2006] B.C.I.P.C.D. No. 39.

into existence through a machine's automatic recording of data, without directed, conscious input by an individual as part of the process by which the information comes into existence, is not information "prepared or collected by" that individual. In this case, the information is machine-generated in a manner that is incidental to the conscious, directed, actions of individuals.

[97] The responsibilities or activities of Schindler's mechanics are to service and repair elevators, travelling to and from their homes and job sites to do that. The system that Schindler has installed reflects how, where and when its employees are driving those vehicles (along with other data). This is not, in any real sense, information that the mechanics themselves prepare or collect. Schindler has programmed the Fleet Complete system to achieve its purposes and it automatically generates and records information associated with vehicle speed, braking, acceleration, whereabouts, start and stop times and maintenance. I do not see how this is 'work product information' respecting individual drivers any more than mileage information automatically recorded in factory-installed odometers and transcribed by other Schindler employees each day would be.

[98] **Is Schindler Collecting and Using Personal Information?**—The first issue here is whether the information in question is about an "identifiable individual". The evidence persuades me that the information Schindler collects is capable of identifying individual employees, certainly when combined with other information in its possession. The complainants' evidence is that, at any given time, a vehicle is assigned exclusively to an employee, and Schindler maintains records of the identity of the individual who operated a given vehicle at a given time.[76] The employee to whom a vehicle has been assigned is identifiable by name and employee number.[77] Schindler does not dispute this seriously—it acknowledges that it can "connect the dots" in order to identify the employee driving a particular vehicle equipped with the Fleet Complete system.[78]

[99] However, Schindler says, as noted above, that the information is not "about" its employees, but "about" Schindler's vehicles.

Engine status data as personal information

[100] Earlier I described the kinds of information generated by Fleet Complete and the purposes and conditions for its use by Schindler. In one sense, the information collected by Fleet Complete pertains to, or is "about", Schindler's assets. For example, the system records data relating to engine use and status, and that information is used to avoid excessive vehicle wear and tear and to schedule maintenance.

[76] Affidavit of Al Campbell, para. 2, and Affidavit of Shawn MacWilliams, para. 2.
[77] Campbell Affidavit, para. 2.
[78] Reply submission, para. 16.

[101] Yet the engine status data also are found in what Schindler calls "exception reports", which, as noted above, record excessive speed, acceleration or braking according to criteria Schindler has devised. Its own evidence is that the exception reports "provide advance indicators of unsafe driving patterns", enabling it to take "a more proactive approach to its obligation to maintain the safety of its employees and the public", by addressing "unsafe driving behaviours…before a particular behaviour becomes severe enough that it leads to an accident, a charge, or a public complaint.[79] Schindler concedes that, as its policies make plain, these reports are used to educate employees to drive safely, and that the information may be used to discipline employees who continue to drive unsafely.

[102] It also acknowledges that the engine status data reveal, by recording engine start and stop times, when an employee starts her or his work day. The engine status data is about the vehicle in one sense, but Schindler also uses the information to ensure that its employees are working their assigned hours. It uses GPS data to determine whether employees have strayed from their assigned routes because they are using their vehicle for personal use. Schindler's evidence, for example, discloses that it has dismissed two employees for what it calls "time theft", with the Fleet Complete data being "vital to the investigative process".[80]

[103] There is an air of unreality in Schindler's argument in the face of its own evidence and its stated purposes for collecting and using this information to manage people. It says that the engine status data are about things, not people, and thus are not personal information. Indeed, in its initial submission, Schindler appears to acknowledge that information can have a dual nature and that this is the case regarding its own practices:

> 41. Engine Status Information is information about the operation of a company asset. Nothing distinguishes it from information about a fixed piece of machinery in a factory. A machine may collect certain data about its operating parameters, for example the time it is turned on, the time it is turned off, the amount of time it spends in active production versus in a suspended or paused state. *This data may indirectly reveal information about the actions of the machine operator during the same period*. [added emphasis]
>
> 42. Perhaps the operating data from the same machine reveals that the operator had consistently been using it in a manner outside its specifications or in an unsafe manner, for example, by running it too quickly or not powering down for inspections as required. Upon reviewing the information the company would investigate further and may take action to ensure that the machine was operated in a safe manner in the future.

[79] Verbruggen Affidavit, para. 36.
[80] Verbruggen Affidavit, paras 25-33.

> 43. It would be incongruous for the operator to complain that the employer's review of those operating statistics somehow constitutes an invasion of his privacy. An employer in the ordinary course must be permitted to use information about its assets in order to manage its operations. To characterize all operational information about an employer asset as personal information of the employee operator would radically hamper the employer's ability to manage its operations. [original emphasis]

[104] Schindler has programmed the Fleet Complete system so it can receive, and use, exception reports, which alert it to a certain kind of behaviour, *i.e.*, any driving by an identified employee that is unsafe, unlawful or contrary to Schindler's standards for that kind of conduct. In one sense, one of these reports can be said to disclose that, for example, a vehicle was, at a certain time and location, travelling erratically at speeds of up to 80 kph, with sharp braking and speeding up, in a zone where the speed limit is 40 kph. One the one hand, this report would say something about the vehicle as a thing. But at the same time, it would say something about the employee driving it. It would disclose to Schindler how the vehicle's driver was driving on that occasion; a compilation of exception reports would, further, disclose, over time, information about how an employee drives more generally.

[105] This dual nature of the information is acknowledged in the above passage from Schindler's submissions, which recognizes that "information about the operation of a company asset" may also reveal information about the operator: "information about the actions of the machine operator during the same period". Schindler collects this information precisely because it wants to know when its employees are driving outside the standards that Schindler lays down. It wants to know so that it can coach the driver to modify the behaviour or so that it can discipline, perhaps even dismiss, the driver.

[106] The same observation applies to engine status data showing engine start and stop times. Nothing in Schindler's materials suggests that the time at which a vehicle's engine starts or stops is of interest to it for any reason other than ensuring that employees are starting and stopping work when they should.[81] It is interested in knowing this in part, I infer, to increase efficiency, as well as to manage employee performance. One might as well say that, when a time-clock is punched at the factory door, the record of the time it was punched is about the clock, not the employee who punched it. The fact that the clock in this example has a dedicated time-keeping purpose makes no difference—the engine status data 'exception reports' Schindler receives also have a dedicated purpose. To characterize this information as being about the vehicle, saying nothing about the behaviour of the person starting it or turning it off at any given time, is

[81] True, these times will inherently be part of the data-set disclosing engine use, and thus wear and tear, for maintenance and repair purposes, but the start and stop time data clearly are captured and reported separately, for the purposes of ensuring employees are working when they should be.

unhelpful in the context of Schindler's avowed purposes for collecting and using that information, which include employee management.[82]

[107] Nor is Schindler on firm ground when it says that engine status data is not 'personal information', since review of "operating statistics" might reveal something about the actions of a specific employee, but would not involve "an invasion of his privacy".[83] This conflates the threshold question of whether information is 'personal information' with the later analysis of whether PIPA's employment-related provisions permit an organization to collect, use or disclose employee personal information.

Location information as personal information

[108] Similarly, GPS data disclosing a vehicle's location is in one sense about the vehicle, whether stationary or not. It may, for example be used by Schindler to locate a missing or stolen vehicle, and for that purpose it is information about Schindler's assets and their preservation.[84] For this purpose, the information is about the vehicle.

[109] However, the GPS location data also disclose the whereabouts of an individual at any given time,[85] and may be used by Schindler for employment-management purposes. A formalistic analysis, seeking to definitively and conclusively distinguish information about a vehicle's location from information about a driver's location is not helpful without regard to the context of purpose and use, which may vary, as Schindler's own policies and actions illustrate.

[110] The evidence here makes it clear that Schindler uses location information for employee performance management, not just to determine where its assets are. It is interested in more than the location of its property; it is interested, at least in part, in what the information says about what its employees are doing. Schindler's policies explicitly acknowledge, for example, that location information may be used in determining, in relation to its policies on personal vehicle use and regarding 'time theft', where a given employee has travelled at given times. In these circumstances, to view location information as relating only to the vehicle's movements, disclosing nothing about the individual who has exclusive

---

[82] The engine status data also record idling, *i.e.*, the amount of time that a vehicle is stationary with its engine running. If Schindler uses this information for the purpose of investigating whether an employee has been idle—perhaps taking too long a break—then it could be seen as information about the employee and thus personal information.

[83] Initial submission, para. 43.

[84] As another example, if GPS location information were used to schedule vehicle maintenance by disclosing the distance travelled by a vehicle, this information would for that purpose be information about the vehicle.

[85] The fact that the individual is at work is not relevant at this stage of the analysis—that comes later.

use of it and whose actions are necessary for it to move from place to place, also has an air of unreality about it.[86]

[111] Schindler acknowledges that, while location information will "directly reveal only the location of Schindler's own vehicle", it also "may indirectly reveal the geographic location of the employee to whom the vehicle is assigned."[87] The fact is, Schindler has used location information precisely because it may help establish wrongdoing. Grounds to suspect wrongdoing are the occasion for the use; they do not somehow magically transform the nature of the information itself.

[112] I conclude that Schindler is collecting personal information in the form of GPS location information. At the very least, when Schindler, in accordance with its policy, accesses and uses GPS information as part of an investigation into an employee's performance, it is using personal information.

[113] To summarize, I have found that the information in issue is 'personal information' of Schindler's employees, not 'work product information' or 'contact information'. The next issue is whether it is 'employee personal information'.

[114] **Is Schindler Collecting and Using 'Employee Personal Information'?**—PIPA creates special rules for employee personal information. Schindler, in another alternative argument, says the information is 'employee personal information' that it is authorized to collect and use.

[115] PIPA defines 'employee personal information' as follows:

> 'employee personal information' means personal information about an individual that is collected, used or disclosed *solely for the purposes reasonably required* to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about that individual's employment. [emphasis added]

---

[86] I note, in this respect, that the Supreme Court of Canada has taken a similar view of state claims that location-tracking devices placed on a vehicle only track the vehicle and not its driver. *R. v. Wise*, [1992] 1 S.C.R. 527, dealt with a radio-transmitter tracking device placed on a vehicle. The police had not obtained a warrant to do this, and the appellant argued that the tracking of his movements was an unreasonable search and seizure under s. 8 of the *Charter*. The majority ultimately held that the location evidence could be admitted. Cory J. noted, for the majority, that the police were interested in monitoring the vehicle's movements only because it would reveal, at least roughly, the movements of the driver. A similar purposive analysis underlies the Ontario Court of Appeal's reasoning in *R. v. Ward*, cited above. *Wise* and *Ward* are *Charter* cases involving state action, but a similar purposive approach is appropriate in determining whether monitoring of a vehicle's location is 'personal information' in the context of Schindler's collection and use of location information to help determine whether an employee has violated his or her employment obligations.

[87] Initial submission, para. 34. The emphasis is Schindler's.

[116] This contains two important elements. First, the collection, use or disclosure of information must be for "purposes reasonably required" to establish, manage or terminate an employment relationship. Second, the collection, use or disclosure must be "solely" for those purposes.

[117] Both of these questions were addressed to some extent by former Commissioner Loukidelis in Order P06-04.[88] That case concerned a film production company that collected residency information from employees in order to obtain tax credits. He found that the information was personal information and that it was "reasonably required" to establish, manage or terminate the employment relationship.

[118] He said the nature of each employment relationship is relevant, noting PIPA's stated purpose of recognizing, not just individual interests, but also the "need of organizations to collect, use or disclose personal information for purposes a reasonable person would consider appropriate in the circumstances". In this light, former Commissioner Loukidelis considered that organizations, in collecting, using or disclosing personal information, are not limited to purposes imposed by statute or another legal obligation or duty. He acknowledged that an organization's business decision to obtain tax credits was reasonably required in order for the organization to achieve its business purpose.[89] Noting that employers will not have "free rein to assert" that a purpose is "reasonably" required, he concluded as follows:

> [47] The circumstances of each case, which must be assessed objectively, will govern. Any number of considerations may be relevant in assessing whether an employer's purposes in collecting, disclosing and using personal information are "purposes reasonably required". These may include the nature of the employment relationship itself (as in this case) or factors such as statutory requirements or benefits that may be available to the employer.[90]

[119] In contending that this is 'employee personal information', Schindler says its employees' work obligations include caring for the vehicles assigned to them and obeying traffic and other laws and policies.[91] Assignment of work among employees, and the development of particular routes and tasks, is also "intimately connected to the employment relationship", and the information it collects assists in all these respects.[92] The complainants, by contrast, argue that Schindler is improperly using the information for employee performance management.

---

[88] [2006] B.C.I.P.C.D. No. 35.
[89] See Order P06-04, paras. 37 and following.
[90] He also noted, at para. 46, that s. 4(1) of PIPA requires organizations, in meeting their PIPA responsibilities, to "consider what a reasonable person would consider appropriate in the circumstances."
[91] Initial submission, para. 69.
[92] Initial submission, para. 70.

[120] Schindler's purposes are, as the complainants acknowledge, to manage employee performance—to manage productivity, manage hours of work, and ensure they drive safely and lawfully

[121] These are legitimate, reasonable, business purposes. A business is entitled to ensure, subject to applicable laws and agreements, that its employees meet productivity standards. It is also a reasonable purpose for a business to collect personal information to ensure that its employees are actually working the hours for which they are paid. It is, at least reasonable for a business to be able to ensure that its employees are, in the course of their employment, driving company vehicles lawfully and with reasonable care.[93] I therefore find that the information is collected for purposes reasonably required to manage an employment relationship.

[122] The second condition is that the collection, use or disclosure must be "solely" for reasonably required purposes. The evidence establishes, again, that Schindler uses Fleet Complete data for various purposes and the character of the information may vary according to the purpose. For example, when Schindler uses engine status data for vehicle maintenance or fleet preservation, that does not involve a use of personal information. If Schindler uses the same data for employee discipline purposes, however, it is using personal information. The same information can, again, have more than one aspect, or character, depending on context and purpose. What matters in assessing the "solely" criterion, is whether, as between the organization and the employee, the organization's sole purpose in collecting, using or disclosing information in its character as 'employee personal information' is to manage an employment relationship. This is why, in Order P06-04, former Commissioner Loukidelis noted that "solely" would mean an organization could not collect home address information as employee personal information if it also intended to use the same information to market products to its own employees without consent.[94]

[123] **Employee Personal Information**—The fact that the information Fleet Complete generates is 'employee personal information' does not end the matter. Schindler can collect, use and disclose that information only if PIPA's rules on collection, use and disclosure of employee personal information also allow it.[95] Those rules are found in ss. 13, 16 and 18, which apply, respectively, to collection, use and disclosure of employee personal information. They share common elements, which can fairly be summarized, for the purposes of this

[93] The separate issue of whether the collection, use or disclosure of employee personal information is authorized under, respectively, ss. 13, 16 and 19 of PIPA, viewed in light of s. 4(1). I return to these questions below.
[94] Order P06-04, para. 48.
[95] The same point was made in Order P06-04, at para. 56.

case, by saying that an organization can only collect, use or disclose employee personal information without consent if:

1. The collection, use or disclosure is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual; and

2. The organization notifies the individual that it will be collecting, using or disclosing employee personal information about the individual, and the purposes for collecting, using or disclosing it, without the consent of the individual.

[124] The central issue, of course, is whether a collection, use or disclosure of employee personal information is "reasonable for the purposes of establishing, managing or terminating an employment relationship between" an organization and an employee.

Considerations in employee personal information cases

[125] The complainants say that the Federal Court in *Eastmond* "endorsed" the following:

> a) The Employer must demonstrate that there is a substantial problem which constitutes cause to initiate GPS tracking for the fulfillment of the alleged purpose.
>
> b) The Employer must demonstrate that GPS tracking is effective in the fulfillment of the alleged purpose.
>
> c) The Employer must demonstrate that GPS tracking is necessary for the fulfillment of the alleged purpose.
>
> d) The Employer must demonstrate that it has exhausted all available alternatives and must demonstrate that there is nothing else that can reasonably be done to fulfill the alleged purpose in a less intrusive way.[96]

[126] This statement of the test, taken from the complainants' initial submission, notes how the court in *Eastmond* actually stated the factors. Here is what Lemieux J. said:

> [127] I am prepared to take into account and be guided by those factors, which I repeat are:
>
> - Is camera surveillance and recording necessary to meet a specific CP [employer] need?

[96] Initial submission, para. 82.

- Is camera surveillance and recording likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?[97]

[127] While it is true that the first factor is found in some labour arbitration decisions relating to video surveillance in the workplace, *Eastmond* does not require an organization to show that there is a "substantial problem which constitutes cause", as the complainants contend. It speaks to demonstrating that the measure is necessary.

[128] As for the second factor, the complainants say Schindler must demonstrate that GPS tracking "is" effective in fulfilling the purpose, whereas *Eastmond* actually states the question as whether the surveillance is "likely to be" effective. The complainants further argue that Schindler must, according to *Eastmond*, also show that the tracking is "necessary" to fulfill the stated purpose.

[129] To my mind, the complainants' version of the fourth factor would require an organization to exhaust all available alternatives and show that nothing else could reasonably be done to achieve the purpose less intrusively. Reduced to its essence, this aligns well with the fourth factor actually set out in *Eastmond*, and is consistent with the reference in *Eastmond* to a proportionality analysis. For reasons given below, I do not think the Legislature intended PIPA to require an organization to adopt the least-privacy-intrusive alternative regardless of cost or reasonableness.

[130] The *Eastmond* test has figured in many decisions of the Office of the Privacy Commissioner of Canada under PIPEDA, including in cases similar to this one. In PIPEDA Case Summary 2006-351, for example, the Assistant Commissioner stated the test as follows:

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?

[131] Both the complainants and Schindler refer to labour arbitration decisions relating to workplace video surveillance in arguing whether the collection and use of personal information in question are reasonable in this case. The complainants

[97] These factors had been applied by the Privacy Commissioner of Canada in the decision under appeal in *Eastmond*. See PIPEDA Case Summary 2003-114, http://www.priv.gc.ca/cf-dc/2003/cf-dc_030123_e.asp.

offer this quote from *Re St. Mary's Hospital (New Westminster) and Hospital Employees Union*,[98] dealing with video surveillance of "production work":

> Examples of the most serious kinds of infringements against the right to privacy include surveillance of production work…or to monitor employees for disciplinary purposes or to conduct surveillance of the social or sensitive areas of the workplace such as locker-rooms, washrooms and lunch-rooms.[99]

[132] It also relies on this quote from *Pope & Talbot Ltd. v. Pulp, Paper and Woodworkers of Canada, Local No. 8*, a British Columbia labour arbitration decision:[100]

> Constant camera surveillance of an employee's productivity, whether that is the primary purpose or just incidental, would obviously be preoccupying and may understandably be regarded in some circumstances as a diminution of one's sense of personal dignity or privacy.[101]

[133] The complainants quote this passage from *Canadian Pacific Ltd. v. Brotherhood of Maintenance of Way Employees*:[102]

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

[134] In their reply submission, the complainants say *Re Finning International and International Association of Machinists and Aerospace Workers*, *Local 99*[103] and *Spectra Energy v. Canadian Pipeline Employees' Association*[104] support the following statement:

> It is well settled that the legal burden of establishing that the collection of the personal information in issue is reasonable for the purposes stated for its collection rests upon the organization and must be based upon clear and compelling evidence providing a factual basis for the intrusion into the privacy rights of employees.[105]

---

[98] (1997), 64 L.A.C. (4th) 382 (Larson).
[99] *St. Mary's*, pp. 398-399.
[100] [2003] B.C.C.C.A.A. No. 362. I note here in passing that, at para. 14, Arbitrator Munroe rejected the employer's assertion that the video surveillance was only of its equipment, not the employees.
[101] *Pope & Talbot*, para. 32.
[102] (1997), 59 L.A.C. (4th) 111 (Picher).
[103] (2004), 135 L.A.C. (4th) 335 (Smith).
[104] [2011] C.L.A.D. No. 266 (Laing).
[105] Reply submission, para. 65.

[135] Schindler says the cases on which the complainants rely are inapplicable. It says *St. Mary's* dealt with covert, not overt, video surveillance, and adds this:

> Arbitrators have distinguished between the reasonableness standards required to justify overt video recording of the workplace, and the much more restrictive standards required to justify covert recording of employees. Neither is applicable to the current case, but the principles developed in the covert recording case law are particularly unhelpful. That case law recognizes that covert surveillance *is* severely and inherently privacy-intrusive. By its nature it is intended to catch a person in some act, unaware that they are being observed.[106] [original emphasis]

[136] Schindler argues that the overt video surveillance cases are distinguishable. It says that overt surveillance "captures every action of the employee", resulting in the capture of employee actions that fall within the "'private sphere' – information that is of a truly personal nature about themselves". Schindler says video surveillance is "the equivalent of an informational dragnet", but the Fleet Complete system is not.[107] It only provides information "about the operation of a Schindler-owned asset", capturing no information about any action by the employee not directly connected to the operation of that asset." Accordingly, any comparison to a video system that records "every movement of an employee" is inapt.[108]

[137] Although Schindler says the video surveillance cases are distinguishable, it nonetheless relies on the balancing approach taken in *Pope & Talbot*, which dealt with video surveillance in the workplace:

> [31] But just as an employee's privacy interests require protection against the overzealous exercise of management rights, so also must an arbitrator acknowledge the employer's legitimate business and property interests. What is required, then, is a contextual and reasonable balancing of interests. There is no absolute rule affording precedence to one legitimate interest over the other. It is a question of whether the particular camera surveillance, in the purported exercise of a management right, is reasonable in the circumstances.

[138] What test does PIPA call for? The factors applied in *Eastmond*, and in decisions of the federal Privacy Commissioner, have not been adopted by this

---

[106] Initial submission, para. 47.
[107] Initial submission, para. 49.
[108] Initial submission, para. 50. This is, of course, consistent with Schindler's contention that the information Fleet Complete collects is not personal information in the first place, a contention that I have rejected. I will also note here, in passing, that Schindler's submission implicitly suggests that, by its nature, video surveillance of the workplace is in every case constant, all-seeing, pervasive. This is, of course, not necessarily so, as the arbitration case law shows. This said, I have found some of the arbitration cases of some assistance, as discussed below.

Office to date and I do not propose to do so. There are some similarities between PIPEDA and PIPA, but they differ materially in how they approach workplace privacy issues. PIPEDA contains no definition of 'employee personal information' and no other provisions that deal expressly with employment privacy. PIPEDA is simply not tailored to handle employment relationships in the way PIPA is.[109] Given the differences in the statutory language and structure, and the legislative intention evident in PIPA, I conclude that the approach taken under PIPEDA should not be applied under PIPA.[110]

[139] As regards PIPA's language, the overriding criterion is reasonableness. Sections 13, 16 and 19 speak to whether the collection, use or disclosure of employee personal information is "reasonable for the purposes of establishing, managing or terminating an employment relationship". That standard is to be viewed in light of s. 4(1), which requires organizations, in meeting their PIPA responsibilities, to "consider what a reasonable person would consider appropriate in the circumstances."

[140] There is also the balancing of rights and needs mandated by s. 2, which "recognizes both the right of individuals to protect their personal information and the need for organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." This legislative statement contemplates a balancing of interests, and s. 4(1) requires organizations to consider, in meeting their PIPA obligations, what a "reasonable person would consider appropriate in the circumstances". It is not desirable to try to offer a definitive list of considerations for determining what is reasonable, since the circumstances will vary from case to case. However, some of the considerations that may arise in cases such as this can be identified here.

[141] My finding earlier that Schindler is collecting and using 'employee personal information' involved a finding that Schindler is doing so for "purposes reasonably required" to establish, manage or terminate an employment relationship. It does not follow, it should be underscored here, that a finding of reasonable purpose for that reason alone means that the nature or amount of information being collected, or the particular manner of the collection, use or disclosure, are reasonable within the meaning of ss. 13, 16 or 19. Those sections refer to what is "reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the

---

[109] This point was made in an Alberta investigation report, *R.J. Hoffman Holdings Ltd.*, Investigation Report P2005-IR-004, [2005] A.I.P.C.D. No. 49, which dealt with overt video surveillance in the workplace. Having noted the difference between PIPEDA and Alberta's PIPA regarding employment privacy, the "actual language" of Alberta's PIPA was said to govern (para. 34).

[110] The Alberta Information and Privacy Commissioner has also declined to apply the PIPEDA test. See Order P2006-008, [2007] A.I.P.C.D. No. 16, where the *R. J. Hoffman* test was used in a case involving surveillance of a recreational facility change room used by patrons.

individual." This requires a further determination, of whether the collection, use or disclosure of employee personal information itself, not the purpose for it, is "reasonable". Sections 13, 16 and 19 are not redundant—they clearly contemplate further scrutiny, by applying to the collection, use or disclosure an objective standard of what is reasonable, viewed in light of what a reasonable person would consider appropriate in the circumstances. The assessment of reasonableness will occur in the context of the established purposes for the employer's collection, use or disclosure and thus should have some regard to that context. But the assessment may also address a number of other possible considerations.

[142] One of these is whether the personal information is of a sensitive nature. An example of sensitive information is information revealing the health history or medical conditions of an employee who is on medical leave or disability. Another example might be marital status information that reveals sexual orientation. Examples of information that will not, generally speaking, be considered as sensitive include an employee's name, home address, telephone number or age.[111]

[143] Another factor may be how much employee personal information is being collected or used. An employer should not collect, or use, more employee personal information than is reasonably required for the employer's purpose. This is not to say that PIPA limits an organization to collecting or using only information that is indispensable to the organization's purposes. I see no indication in PIPA that an organization will be held to such a strict standard of necessity. Organizations should, rather, tailor their collection, use or disclosure of employee personal information, collecting, using or disclosing only that which is reasonably required to achieve their purposes.

[144] Of course, this involves some assessment of whether the collection, use or disclosure in question is likely to be effective in fulfilling the organization's objectives. If there is no reasonable likelihood of effectiveness, it is hard to see how a particular collection, use or disclosure of employee personal information can be reasonable, even if the purposes for collection are "reasonably required". An organization does not have to establish effectiveness to a standard of certainty, but there should be a reasonable likelihood of effectiveness.

[145] A related consideration is whether there are alternatives. If alternatives exist, an organization should be prepared to show that it has given them reasonable consideration. I am not suggesting that an organization absolutely must adopt an available measure simply because it is a less privacy-intrusive, or the least privacy-intrusive, without regard to cost to the organization or the

[111] A factor in other cases may be whether the organization is required by law, or government policy or rules, to collect, use or disclose the personal information in question. For example, employers are required to collect employee's social insurance numbers for income tax purposes. See Order P06-04, referred to above.

effectiveness of the collection, use or disclosure in achieving the organization's stated goal.[112] PIPA does not focus solely on privacy and privacy does not always trump the interests of an organization, as s. 2 makes clear.[113] Rather, the assessment of alternatives should consider the balance between the organization's interests and, as s. 2 says, the "right of individuals to protect their personal information".

[146] In cases involving employee monitoring or surveillance, another consideration may be whether the personal information has been collected covertly. As labour arbitrators across Canada have repeatedly recognized, covert monitoring has the potential to capture considerable amounts of personal information, especially where it is pervasive and continuous. While PIPA will permit surreptitious surveillance or monitoring in appropriate circumstances, it may be more appropriate for the reasonableness assessment to be more searching where more sensitive personal information may be collected (for example, through covert monitoring of email use or computer use).[114]

[147] Before considering the circumstances of this case, I will underscore a key point about technological change and PIPA. The range of circumstances that may be relevant in a given case will undoubtedly change as technological innovation drives changes in employment relationships and ways of working. As the Ontario Court of Appeal observed earlier this year:[115]

> It is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form. Technological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the *Charter*, has been recognized as a right that is integral to our social and political order.

[148] The same can be said about evolution of the law under PIPA. As technology-enabled work practices evolve, employers may implement practices with novel implications for personal information protection in the employment setting. As the line between one's work and one's personal life grows fainter through ubiquitous computing and connectivity, new considerations will arise. Technological change will raise new challenges for determining what is

---

[112] The costs to an organization may be increased direct costs of pursuing alternatives, or they may consist of implications for the efficiency of the organization's business operations, including productivity.

[113] In this regard, I agree with similar observations by the majority in *Leon's Furniture*, at para. 57.

[114] This case in some respects involves monitoring, but it is overt monitoring: employees are aware that Schindler is monitoring, for example their work start and stop times.

[115] *Jones v. Tsige*, 2012 ONCA 32, at para. 68. Following a request by the complainants, the parties were given an opportunity to make submissions about *Jones*. That case recognizes the existence in Ontario of a common law cause of action for 'intrusion upon seclusion'. Although the passage I have quoted is illuminating in a general sense, *Jones* is not apposite in the context of PIPA.

reasonable for the purposes of PIPA's employment-related provisions.[116] A notable strength of PIPA is that it is not technologically prescriptive, thus allowing the balancing of interests it contemplates to evolve over time. PIPA's appeal to what is reasonable accommodates changes in technology, evolution in business practices, and shifts in societal standards, without inevitably diminishing personal information protections to the vanishing point.[117]

Is Schindler authorized to collect employee personal information?

[149] Schindler says it is authorized to collect and use employee personal information for the purposes of "operational efficiencies", "safety" and "preservation of Schindler property".[118]

[150] It is reasonable for Schindler to use the Fleet Complete system data to schedule vehicle maintenance, to reduce vehicle wear and tear by balancing vehicle over-use and under-use, and to ensure that its service routes are efficient and that emergency calls are efficiently responded to. I accept on the evidence that the technology offers improvements over earlier methods of doing these things, including in light of the challenges with employee self-reporting and direct supervisor monitoring of a mobile workforce for route efficiency purposes in a situation where there is a roughly 1:10 supervisor-to-employee ratio.

[151] Of course, Schindler readily acknowledges that it is collecting and using engine status data and GPS data for employment-management purposes, *i.e.*, to ensure safe driving, proper hours of work, and compliance with rules around use of company vehicles. The remaining question, then, is whether the collection and use of this information is, as required by ss. 13, 16 and 19, "reasonable" for those purposes.

[152] I outlined above some of the factors that may be relevant in assessing reasonableness. Consideration of a number of factors leads me to the conclusion that Schindler's collection, use and disclosure of employee personal information is reasonable.

Sensitivity and amount of information

[153] The first factor is sensitivity. The GPS data reveal an individual employee's location at a given time—they can show where the employee went during the work day. Combined with readily-available GPS mapping and street-level imagery services such as Google Street View, this information can

---

[116] Similar observations were endorsed by the Federal Court of Appeal in *Wansink v. TELUS Communications Inc.*, 2007 FCA 21, [2007] 4 FCR 368, a case involving PIPEDA.

[117] As for the present state of affairs, the outcome in this case is of course circumstance-specific and no larger message is intended about use of monitoring technologies in the employment setting.

[118] Initial submission, para. 86.

give a fairly detailed picture of where an employee was at any given time. It is relevant, however, that this information arises, overwhelmingly, in the context of work-day activities, where there are assigned service routes, job sites and tasks.[119] These factors tend, in the present case, to diminish the sensitivity of the location information. It is also important, in my assessment of this case, that GPS location information is not collected and used routinely and is not continuously monitored.

[154] The information is recorded and stored, but is only accessed as one part of the material that may be used in an investigation regarding an employee's compliance with her or his employment duties. As indicated earlier, Schindler's evidence is that location information is used for employment-related purposes—*i.e.*, for an investigation into an employee's conduct—only if other circumstances prompt it to investigate.

[155] The engine status information likewise is not, in these circumstances, sensitive information. Like most individuals, Schindler's employees have established hours of work, and information about when they appear to have started or stopped work is not readily described as sensitive as between them and their employer. Nor is the exception report information, which reveals driving behaviour falling outside employer-set parameters, particularly sensitive information, certainly as between employee and employer. This collection and use of information is tailored to the purposes for the collection.

[156] The complainants rely on Al Campbell's evidence that a Schindler manager told an employee, in May 2011, that "Schindler was changing the way that it monitored the GPS", to generate reports about vehicle start and stop times, with employees being questioned and possibly disciplined.[120] Schindler already had, some seven months earlier, through the September letter, signalled this (as did the GPS Policy, issued in January 2010). Schindler's evidence is that engine status data may be used to help determine hours of work if an exception report is triggered and indicates a possible concern. Schindler's policy of using that information as only one piece of information in making inquiries is, again, relevant. I also have in mind that this is not, as I have already said, particularly sensitive information as between employee and employer. Accordingly, even if an exception report were triggered by an apparent late or early engine ignition time, I would find that to be reasonable in the circumstances.

---

[119] I conclude that Schindler's employees are expected to follow these routes, subject to emergency callouts or other route variations (such as coverage for colleagues who are absent). Those same routes are in part GPS-based, I find, and are communicated to employees, who are expected to follow them.

[120] Campbell affidavit, para. 8.

Likelihood of effectiveness

[157] The next consideration is whether the collection and use of employee personal information is likely to be effective. Schindler's evidence is that, before it acquired the technologies, its efforts to ensure that its employees drove safely depended on complaints from members of the public, chance observations by Schindler supervisors, or its knowledge of traffic-related charges or offences.[121] The engine status data now permit Schindler to take a "more proactive approach", since the weekly exception reports "provide advance indicators of unsafe driving patterns." When it learns of unsafe driving, Schindler first coaches the employee involved, though it acknowledges that a case could become serious enough to warrant discipline.[122] According to its evidence, in the one-year period following June 2010, shortly after Fleet Complete was installed, Schindler noted a year-over-year "drop in accident costs of over 30%", which it believes is attributable to the system-related "heightened awareness around speeding and harsh braking/accelerating."[123] I am persuaded that Schindler has shown that the engine status data are reasonably likely to be effective in ensuring that its employees drive safely, lawfully and in accordance with its policies.

[158] I make the same finding respecting Schindler's collection and use of engine status data—specifically, engine start and stop times—to help establish whether hours of work are being kept as required. Schindler's employees are paid by the hour. Like other employers, Schindler has an interest in ensuring that its employees actually work the hours they are supposed to and for which they are paid. It is beyond controversy that most employers keep some track, through various means, of whether their employees are working the hours for which they are paid.

[159] In an office or factory setting, this may be done by direct observation, or it may be done using other means, such as time clocks, access swipe cards or sign-in sheets. As the evidence shows, Schindler's elevator mechanics are a mobile workforce and do not report to any Schindler office or dispatch facility before or after work. The mechanics "work largely alone and all mechanics work without constant supervision",[124] with a roughly 1:10 supervisor-to-employee ratio. It is, Schindler says, "impossible for Schindler to verify the whereabouts and activities of its mechanics at all times."[125] I am persuaded that the start and stop time data, and GPS data as to location during times when an employee is supposed to be working on a jobsite, are reasonably likely to be effective in

[121] Verbruggen affidavit, para. 35.
[122] Verbruggen affidavit, paras. 36 and 37. At the time this affidavit was sworn, Schindler had not yet initiated disciplinary actions for unsafe driving.
[123] Verbruggen affidavit, para. 41.
[124] Verbruggen affidavit, para. 30.
[125] Verbruggen affidavit, para. 30.

verifying hours of work, noting again that these data are not continuously, routinely, monitored.[126]

Are there alternatives?

[160] The complainants' evidence on this point demonstrates, they say, that no problem has been shown with the old self-reporting and work assignment methods. Schindler has shown that, before it installed the Fleet Complete technologies, it relied on employee self-reporting and this was not as effective, according to Schindler's evidence, as the Fleet Complete system. Despite employees' best efforts, Schindler submitted, self-reporting was after-the-fact and often inaccurate and incomplete. Given the high numbers of employees for each field supervisor, direct observation was not, I accept, as effective an approach. Schindler has not only considered, but used, the only apparent alternative, which is self-reporting in writing, by cell phone and direct observation.

Collection is not covert

[161] There is no suggestion that Schindler is collecting and using employee personal information covertly, *i.e.*, without the knowledge of its employees. The existence of the Fleet Complete, what it does and how Schindler uses it is known to the complainants through the GPS Policy and September letter, as well as meetings between Schindler and the IUEC before Fleet Complete went live.

Offence to employees' dignity

[162] The complainants' say use of Fleet Complete is offensive to their dignity. In his affidavit, Shawn MacWilliams, a Schindler elevator mechanic and an IUEC shop steward, MacWilliams deposed that, since the "GPS tracking devices were installed, several fellow employees have been questioned on their start and stop times." He also offered what he described as "recent examples" of how Schindler is using Fleet Complete as "an employee performance management and discipline tool." He referred to a situation where an employee had been docked an hour's pay based on vehicle start and stop time data, two where employees had received verbal warnings about start and stop times, and one where an employee was questioned about his movements and where he was working at a specific time three weeks previously.[127]

[163] MacWilliams also deposed that the use of the GPS and engine status data has "had a serious negative effect on employee morale", adding that it is "offensive to my dignity and to the dignity of my co-workers to be monitored electronically." He also expressed the opinion that use of the technology has had

[126] In this regard, I note Schindler's evidence that the data can vindicate and absolve an employee.

[127] MacWilliams affidavit, para. 9. Two personal examples were also set out in an affidavit sworn by Al Campbell, a Schindler elevator mechanic.

a "demoralizing effect on the workforce". He added that it "is very frustrating and worrisome to work in an environment that you know that you can be questioned by management about your locations and movements and use of your company vehicle at any time", based on the data.[128]

[164] There is nothing remarkable in the management of a company questioning its employees about their compliance with company rules as to hours of work, performance of assigned work tasks (including following assigned service routes), and use of company property according to the rules. If the complainants are suggesting that use of data materially affects an employer's right to pose such questions, I do not agree.

[165] In any event, I am not persuaded that any offence to the dignity of employees tips the scales against Schindler.[129] I say this given the nature of the data being collected and the rules under which information is accessed and used by Schindler. I am particularly influenced by the fact that the GPS-derived location information is not continuously monitored. If an organization were to engage in continuous, real-time monitoring of employees' whereabouts, during or outside work hours, for employment management purposes, I would want to look very carefully at the situation.

[166] Having considered these factors and the circumstances of this case overall, I am persuaded that Schindler's collection and use of employee personal information for the purposes, and in the manner, described above is reasonable and is authorized under PIPA.

[167] **Has Schindler Met Its Other Obligations?**—The last issue to be considered is the complainants' contention that Schindler is not meeting its obligations under s. 5 of PIPA, also citing what they say are Schindler's s. 10 obligations.

[168] The complainants' submissions appear to follow two approaches. On the one hand, they allege that Schindler is "not following its stated restrictions on its use of the GPS Tracker for employee performance management purposes", using it instead "for the routine continuous monitoring of employees" and for disciplinary purposes, "without applying any reasonable restrictions."[130] As I understand it, they argue that, because (they say) Schindler is continually monitoring location information and using it for discipline, its GPS Policy fails to disclose the purposes for Schindler's collection of personal information, as required by s. 19(1)(a).

---

[128] MacWilliams affidavit, para. 10. Similar concerns were expressed in the Campbell affidavit.
[129] Whether Schindler's practices are conducive to a harmonious and optimally-productive labour relations environment is not a question for me to decide.
[130] Initial submission, para. 74.

[169] The complainants also argue, however, that, given the "highly intrusive nature" of GPS technologies, "Schindler's compliance with ss. 5 and 10(1)(a) of the Act requires a specific GPS policy, akin to that described at paras. 22-24 of OPCC Decision #2006-351."[131] The complainants suggest that, in order to comply, Schindler would have to adopt a "policy that restrictively delineates the 'limited, exceptional, and defined circumstances' in which Schindler will allow itself to use GPS data for employee performance management purposes."[132] Schindler's existing policy fails to delineate such circumstances, they say, instead applying an "overly broad" standard of "reasonable concern" as the basis for its use of GPS information.[133]

[170] The complainants cite these aspects of ss. 5 and 10:

> **Policies and practices**
>
> 5 An organization must
>
> (a) develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under this Act,
>
> …
>
> (c) make information available on request about
>
> (i) the policies and practices referred to in paragraph (a), and
>
> …
>
> **Required notification for collection of personal information**
>
> 10**(**1) On or before collecting personal information about an individual from the individual, an organization must disclose to the individual verbally or in writing
>
> (a) the purposes for the collection of the information, and ….

Sections 5 and 10 and personal information practices

[171] If the complainants are suggesting that s. 5, alone or in combination with s. 10, imposes substantive obligations or limitations respecting what employee personal information an organization may collect, use or disclose, I do not agree. Section 5(a) stipulates that an organization must have "policies and practices" necessary for it to "meet all the obligations" of the organization under PIPA. Consistent with this, an organization must, under s. 5(c), "make information available on request about…the policies and practices" it develops under s. 5(a).

[131] Initial submission, para. 76.
[132] Initial submission, para. 76.
[133] Initial submission, para. 77.

[172] These provisions speak to policies and practices for fulfilling, or meeting, substantive obligations or limitations otherwise arising under PIPA, including those addressing collection, use and disclosure of 'employee personal information'. Sections 5 and 10 do not add to this and require Schindler to develop a policy "that restrictively delineates the 'limited, exceptional, and defined circumstances' in which it will allow itself to use GPS data for employee performance management purposes." Whether Schindler is permitted to use GPS data and engine status data is to be considered under PIPA's substantive provisions relating to employee personal information, which I have already done, not ss. 5 and 10.

Notice of purposes

[173] The complainants appear to treat s. 10(1)(a) as the relevant notice provision. That section applies where an organization is collecting "personal information about an individual from the individual". Schindler is not collecting personal information "from" its employees. The applicable notice requirements are those expressly set out in ss. 13, 16 and 19, which are specific to non-consensual collection, use or disclosure of employee personal information. Section 10 applies to personal information where it is collected directly from the individual it is about, in consensual collection situations.[134]

[174] This argument regarding ss. 5 and 10 does not affect the substance of the complainants' central argument about notice. Under ss. 13, 16 and 19, an organization must notify an individual that it will be collecting, using or disclosing employee personal information about the individual, "and the purposes" for it, before the organization do so without the individual's consent. The question is whether Schindler has met these notice requirements and whether it has, as the complainants argue, failed to align its practices with the notice given to its employees.

[175] Schindler's compliance is to be assessed against both the GPS Policy and the September letter. The complainants' evidence acknowledges that the September letter contains statements as to Schindler's purposes for collecting, using and disclosing personal information. The GPS Policy does so as well. Neither should be read in isolation. Whether the notice Schindler gave its employees complies with PIPA must be measured against what both the GPS Policy and the September letter say together.[135] Both were, the evidence establishes, communicated to Schindler's employees,[136] and, in my view,

[134] As an exception, s. 10(3) provides that, if consent is deemed under ss. 8(1) or (2), notice need not be given before collection.

[135] I note that the GPS Policy refers to use of data for "investigating internal matters, including concerns about the conduct of employees reporting to work locations in a timely manner", and so on. The September letter, which focussed on hours-of-work obligations, expands on this.

[136] The evidence of both parties is that the September letter was sent to employees and the GPS Policy was provided to the IUEC, the employees' representative.

together they fulfill Schindler's obligation to give notice of "the purposes" for collection, use and disclosure of employee personal information.

[176] The GPS Policy begins with the general statement that Schindler will "utilize vehicle GPS" for operational efficiencies, for safety and for preservation of fleet property. It goes on to say that data from a vehicle's "GPS system will not be routinely or continuously monitored for the purpose of managing employee performance such that disciplinary action could result." It also gives "[s]ome examples of appropriate use of vehicle GPS data", including "investigating and responding to a complaint raised by a member of the public", "investigating internal matters, including concerns about the conduct of employees reporting to work locations in a timely manner, adhering to appropriate break/lunch schedules, improper use of vehicles off-duty, etc.", and "providing feedback to employees about their driving habits in order to enhance safety and fuel efficiency."[137]

[177] The GPS Policy specifies that Schindler "may use vehicle GPS technology as a tool to review and enhance employee performance when circumstances warrant", including where

> … Schindler has a reasonable concern that an employee's conduct is inconsistent with requirements established under Schindler's policies, Code of Conduct, and general obligations and expectations of employees of the Company. An employee whose behaviour is inconsistent with reasonable standards of conduct will be subject to appropriate disciplinary action, up to and including discharge.[138]

[178] Another portion of the GPS Policy says "GPS data" may be used to assist with locating "employees and resources quickly in the case of an emergency or when communication has been lost", adding:

> Key performance indicators such as harsh braking, sharp acceleration, and speeding may be monitored through exception reporting to identify and correct problems thereby reducing instances of unsafe driving.

[179] Last, the GPS Policy provides that "GPS data may be used to assist with locating vehicles quickly in the case of theft", and to "assist with the proactive scheduling of maintenance, reducing repair costs, preserving resale values and prolonging the life span of Schindler vehicles."[139]

[137] Page 2, GPS Policy.
[138] Page 2, GPS Policy.
[139] Page 2, GPS Policy.

[180] The September letter also told employees the following:[140]

> Another part of meeting our commitments to the customer and operating efficiently is ensuring each of us report [*sic*] to work on our scheduled workdays prepared to perform our assigned duties. We wish to take this opportunity to remind you of the expectations regarding your hours of work. As an employee working in our <<Department 11>> department, you are expected to be at your first job site at <<Start Time>>. As you are aware, in order to ensure adequate coverage throughout the business day you are to take a mandatory <<Lunch Break Duration minutes>> minute lunch break. You are required to be at your last job site until <<End Time>>. ;;;
>
> Please be advised that in light of the recent arbitral award between Otis and the IUEC regarding the use of telematics devices, we will be using our Fleet Complete System to assist us in determining whether the hours of work requirements as set out above are being complied with.
>
> Any deviation from the above hours of work requires approval from your Supervisor in advance. If you find yourself in a work situation where the absence of a co-worker prevents you from continuing to perform your work tasks, you are required to contact your Supervisor for further direction.
>
> Failure to abide by these hours of work can result in discipline up to and including discharge. Please be advised that in recent months we have been obligated to terminate the employment of three mechanics for violations of our attendance policy. If you require a refresher on the provisions of this policy please refer to your employee handbook or contact your Supervisor directly.

[181] In my view, an employee reading the GPS Policy would know that her or his employer was collecting and using information relating to the employee's actions on the job. The employee also would know that the personal information was being collected and used for performance management, including, possibly, disciplinary purposes. The employee would know that the scope of uses would include unsafe driving, reporting to work in a timely manner, location during work hours and possible improper vehicle use during off-duty hours. As regards work-hours monitoring, that use of data was further reinforced by the September letter, which elaborates on the GPS Policy's reference to this purpose.

[182] Al Campbell's evidence for the complainants referred to a Schindler supervisor telling him, in October 2010, that he had used the technology to catch Campbell and another employee "speeding every morning" at a certain location.[141] This is not evidence that Schindler's policy was other than as notified to employees through the GPS Policy or September letter. It may or may not

[140] As indicated earlier, and as reflected in the above quote, the version of the letter appended to the Verbruggen affidavit appears to be a draft form-letter version of what was sent to employees. I am quoting here from the version appended to the Verbruggen affidavit.
[141] Campbell affidavit, para. 7.

disclose that a particular supervisor, assuming his claim was accurate, did something contrary to Schindler's policy. But it does not disclose a *purpose* for collection or use of information that differs from what Schindler had notified its employees of.

[183] In his affidavit, Gordon Heard deposed that a Schindler manager had, in response to IUEC concerns about the technology, emailed the IUEC on January 28, 2010 "with written answers to Local 82's questions".[142] A copy of that email has not been provided to me and Heard did not elaborate on what the email said. He deposed, however, that in its

> …dealings with Schindler, including their written correspondence, Local 82 was assured that data from the GPS devices would not be routinely or continuously monitored for the purpose of managing employee performance such that disciplinary action could result. Indeed this is reflected in writing in Schindler's GPS Policy.[143]

[184] Heard also acknowledged that Schindler had, in September 2010, "issued a warning letter to its employees in B.C. concerning the use of the new GPS tracking devices in its vehicles", adding that this "letter contradicts Schindler's earlier assurances" that the technology would not be "routinely or continuously monitored for the purpose of managing employee performance", with possible disciplinary action.[144] As with the May 2011 statement, the September letter, taken together with the GPS Policy, speaks to the purpose for collection. The email to which Heard referred, and the dealings he mentioned, relate to frequency of collection, not purpose of collection and use.

[185] This evidence is not sufficient to persuade me that Schindler is collecting or using employee personal information for purposes beyond those set out in the GPS Policy and September letter.

Schindler should revise and consolidate its GPS policy

[186] As an aside and not part of my findings, Schindler should revise its GPS Policy to account for the outcome of this inquiry, by capturing my findings and setting out comprehensively the purposes for which employee personal information may be collected, used or disclosed through the Fleet Complete system. The revised policy would also offer a desirable single source of notice to existing (and new) employees of Schindler's purposes. The September letter elaborated on the GPS Policy in one respect, but it is desirable at this stage for there to be a single, comprehensive, policy statement.

---

[142] Heard affidavit, para. 5.
[143] Heard affidavit, para. 2.
[144] Heard affidavit, para. 6.

[187] The desirability of a revised policy is underscored by Schindler's own reply submission. As I noted earlier, Schindler's own GPS Policy does not clearly distinguish between the two kinds of data. This lack of clarity does not extend to adequacy of Schindler's notice of purposes, but its own failure to clearly distinguish between the technologies leaves me with little sympathy for its contention about the complainants' confusion as between GPS data and engine status data.

CONCLUSION

[188] For the reasons given above, under s. 52(3)(a) of PIPA, I confirm that Schindler has performed its duties under PIPA respecting its collection, use and disclosure of GPS data and engine status data, including duties under ss. 5 and 10.

December 19, 2012

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner for British Columbia