Protecting privacy. Promoting transparency.

Order F13-04

UNIVERSITY OF BRITISH COLUMBIA

Elizabeth Denham, Information and Privacy Commissioner

February 1, 2013

Quicklaw Cite: [2013] B.C.I.P.C.D. No. 4
CanLII Cite: 2013 BCIPC No. 4

Summary: The information UBC collects from a GPS system installed in its Campus Security patrol vehicles is 'personal information' of its employees in view of its use for purposes relating to the whereabouts and behaviour of the employees at work. UBC is authorized to collect and use this information in the circumstances. UBC failed, however, to give proper notice of collection of personal information, which it must do now.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, ss. 26, 27 and 32.

Authorities Considered: B.C.: Order P12-01, [2012] B.C.I.P.C.D. No. 25; Order F07-10, [2007] B.C.I.P.C.D. No. 15; Order F07-18, [2007] B.C.I.P.C.D. No. 30; Order F08-03, [2008] B.C.I.P.C.D. No. 6. **Ont.:** Order PO-2763, [2009] O.I.P.C. No. 31.

Cases Considered: *Canada (Information Commissioner) v. Canada (Canadian Transportation Accident Investigation and Safety Board*), 2006 FCA 157, leave to appeal denied, [2006] S.C.C.A. No. 259; *Otis Canada Inc. v. International Union of Elevator Constructors, Local 1*, [2010] B.C.C.A.A.A. No. 121; *Rizzo & Rizzo Shoes Ltd.,* [1998] 1 S.C.R. 27; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403; *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police*, 2003 SCC 8, [2003] 1 S.C.R. 66; *R. v. Wise*, [1992] 1 S.C.R. 527; *U.S. v. Jones*, 132 S.Ct. 945 (2012); *Jones v. Tsige*, 2012 ONCA 32.

INTRODUCTION

[1] Like Order P12-01,[1] this decision considers technology that generates information about the location, movements, speed and ignition status of

[1] [2012] B.C.I.P.C.D. No. 25.

a vehicle. It similarly considers whether this is 'personal information' of individuals who drive the vehicle in the course of their employment duties, and whether their employer is authorized to collect, use and disclose that information.

[2] There are differences, however. This case involves the actions of a public body, the University of British Columbia ("UBC"), under the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), not those of a private sector organization under the *Personal Information Protection Act* ("PIPA"). Underlying this decision is a complaint by the union representing employees of UBC's Campus Security Department, the Canadian Union of Public Employees, Local 116 ("CUPE"). The complaint centres on GPS technology that UBC installed in patrol vehicles used by UBC's Campus Security Department at UBC's main campus on Vancouver's Point Grey. Despite the statutory differences between FIPPA and PIPA, however, I similarly conclude that the information UBC collects through the vehicle GPS system is 'personal information', but that it is authorized to collect and use that information.

ISSUES

[3] The notice of hearing issued by this Office frames the issues as whether UBC "is collecting and using personal information contrary to ss. 26, 27 and 32 of FIPPA." CUPE seeks "a declaration that UBC violated FIPPA", specifically, ss. 26, 27 and 32, by installing and using the GPS system and thus "collecting, monitoring, storing and using" employees' personal information.[2] It also seeks an order requiring that UBC "cease and desist from using GPS tracking devices to collect, monitor and store employees' personal information."[3]

[4] A threshold question is whether UBC is collecting 'personal information'. If it is not, FIPPA does not apply. If it is collecting personal information, it remains to be seen if UBC has the authority under s. 26 to collect the information and, if so, whether it is collected in a manner authorized by ss. 26 and 27. The last issue is whether UBC's use of the information is authorized under s. 32.

[5] This order arises from a complaint to this Office under s. 42 of FIPPA, not a request for review to which a burden of proof set out in s. 57 applies. The notice of hearing advised the parties that, FIPPA being silent on the burden of proof, each party should "provide information and submit arguments to justify its position on the issue." This is consistent with, for example, Order F07-10,[4] where it was noted that a public body is "expected, for all practical purposes, to provide evidence of compliance with Part 3 of FIPPA in the context of an investigation under s. 42". It was also said, and I agree, that this "does not equate with the imposition of a legal burden of proof". I also agree that, where

[2] Initial submission, paras. 47 and 48.
[3] Initial submission, para. 49.
[4] [2007] B.C.I.P.C.D. No. 15, at para. 10.

the legislation is silent, this does not place a formal burden of proof on either party.[5] In the absence of a statutory burden of proof, it is incumbent on both parties to provide evidence to support their positions, bearing in mind that it is ultimately my role to decide if the public body has complied with FIPPA, and bearing in mind that public bodies are usually best placed to offer evidence that they have complied.

[6] I will deal here with a preliminary point. In its initial submission, CUPE raises the concern that UBC's policy on GPS information does not clearly set out which UBC employees are permitted to have access to the information; nor is there "any indication how, if at all, individuals would be restricted from accessing information in order to ensure that only those who require access are permitted access to this Personal Information."[6] CUPE also expresses concern about retention of the information stating, "it is simply unnecessary for information to be stored at all."[7]

[7] UBC objects to these concerns being addressed here. It points out that, as noted above, the notice of hearing frames the issues to be considered as whether UBC "is collecting and using personal information contrary to ss. 26, 27 and 32 of FIPPA." I agree with UBC that CUPE's concern about which UBC employees have access to the GPS system information is, in one respect, a personal information security issue under s. 30.[8] It is also, in my view, a disclosure issue under s. 33.2(c) of FIPPA, *i.e.*, the issue of whether each employee to whom the information is accessible needs that information to do her or his job. As they were not raised earlier, and are not set out in the notice of hearing, I will not address CUPE's concerns in this decision.

DISCUSSION

[8] **Background—**UBC's Point Grey campus is very large, extending over some 400 hectares and comprising over 500 buildings. Campus facilities include bars, restaurants, a hospital, arts venues and a museum. Some 41,000 students attend UBC each year and the Point Grey campus houses approximately 8,000 students, faculty members and staff.[9]

[5] Order F07-10, at para. 11.
[6] Initial submission, para. 34.
[7] Initial submission, para. 35.
[8] As is CUPE's concern about retention of the GPS system information.
[9] This description of the background to the complaint is based on the affidavit sworn by Tony Mahon. He became UBC's Director of Campus Security in 2007; before that he was a member of the RCMP for 34 years.

[9] As part of its security operations, UBC's Campus Security Department provides campus security around the clock and throughout the year.[10] This involves patrolling the campus by car, on foot and on mountain bikes. The patrol vehicles are used, generally, to patrol the roads on campus, and to respond to calls anywhere on campus. At any given time, at least one of the two vehicles is on patrol.

[10] Campus Security employees often work alone, day or night. They wear uniforms and have radio communications, but are unarmed. They sometimes face hostile and violent situations, UBC says. It notes that, of eight reported common assaults on campus in 2010, six were against Campus Security staff. In 2010, staff dealt with 16,370 security-related incidents of one sort or another. These included property crime, such as theft, and personal crime.

[11] The nature of patrol work means that employees are often out of their patrol vehicle, responding to calls or security situations. They use radios to communicate with the operations centre. They are required to check in with the centre regularly so that the operations centre knows they are safe. This said, patrolling employees are sometimes out of radio contact because of the size of the campus.

[12] The technology in dispute was installed in July 2008.[11] The system comprises Global Positioning System ("GPS") and engine monitoring technologies. The particular system is the Nero Global Vehicle Tracking System. The system allows someone in UBC's operations centre to see the current location of a vehicle. The system also allows the speed of a vehicle and when it is turned on and off to be viewed.

[13] The system can be monitored around the clock by all Campus Security communications officers working in the operations dispatch centre. The location of monitored vehicles, their speed and ignition data are displayed on a monitor viewable by the (typically) one communications officer on shift.[12] With the exception of two Campus Security managers, the only employees who have access to the information are members of CUPE, who have read-only access.

[14] The information is used to dispatch the closest vehicle in response to security incidents. It can also be used to locate a vehicle where a Campus Security employee does not respond to radio communications. UBC installed the equipment so it could dispatch patrol vehicles efficiently, locate patrolling

[10] Campus Security works in conjunction with police where necessary.
[11] It was also installed in a Campus Security community relations vehicle, which is used for patrol backup, in November 2009.
[12] When the communications officer is on break, patrol staff will monitor the GPS system and other systems.

employees for their safety, and, for maintenance purposes, to keep track of the distance that vehicles travel.

[15] The system does not display the name or other identifying information of the employee who is driving a vehicle at any given time. It only transmits information about the location and status of the vehicle in which it is installed. The individual monitoring the system cannot tell what the driver is doing at any given time when the vehicle is stationery. When a vehicle is moving, the only information displayed is speed and location.

[16] UBC says it does not monitor vehicles as an employee management tool. It acknowledges, though, that it may use information from the system to investigate an incident involving a patrol vehicle, such as reported speeding or an accident. It will only use the data for this purpose if it learns of a matter through other means. It has only done so once, when an employee reported that he had used a vehicle to pursue another vehicle off campus, which is against the rules. The system confirmed that the vehicle left campus and had been speeding, although UBC did not use this information in the disciplinary proceedings.

[17] CUPE complained to UBC about the system, and then complained to this Office. After the complaint to this Office, UBC issued a policy on use of the GPS system. Mediation was not successful, resulting in the inquiry leading up to this order.

[18] **Is UBC Collecting & Using 'Personal Information'?**—A threshold question is whether UBC is collecting 'personal information' in the first place. If not, FIPPA has nothing to say about what it is doing. UBC argues that the system-generated information is not 'personal information' at all. This is consistent with arguments made in Order P12-01.

[19] Before considering the meaning of 'personal information' in the context of this case, I will note that UBC's position in this proceeding is at odds with its own published GPS policy. The policy is entitled 'GPS—Campus Security Vehicles'.[13] The policy defines 'personal information' as "information about an identifiable individual," and includes detailed guidance to operational staff on use of the GPS system for on-shift location monitoring. Section 5 says that Campus Security management employees were to be given an orientation "on the appropriate use of the GPS technology as it applies to privacy legislation", with training to be given to managers "to ensure that they use it appropriately." Sections 7 through 16 quite clearly show that UBC's Campus Security Department, at least,

[13] A copy of this policy, which is dated January 2010, forms exhibit "C" to the affidavit of Tony Mahon, UBC's Director of Campus Security, who approved the policy. A copy also forms appendix "O" to CUPE's initial submission.

considered that GPS location information is 'personal information'. Sections 10 through 16 read as follows:

> 10. Personal Information collected under the GPS Technology will be stored and accessed in Canada unless UBC obtains consent of the employee to store or access the Personal Information outside of Canada.
>
> 11. UBC will make every reasonable effort to ensure the Personal Information is accurate and complete.
>
> **COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION**
>
> 12. The GPS system will be used primarily for the purpose of Campus Security patrol officer safety. The safety of Campus Patrol staff is critical as staff are out of radio contact from time-to-time in various parts of the campus and due to the nature of their duties, confrontational situations may occur.
>
> 13. UBC will monitor the usage of vehicles through the use of the GPS system to ensure that vehicles are being used in accordance with laws pertaining to speed and to ensure that vehicles are not leaving the duty jurisdiction without permission.
>
> 14. UBC will monitor through the GPS system the kilometers travelled by each vehicle to accurately ensure the vehicles are serviced at regular intervals.
>
> 15. UBC will not use the GPS system as a performance management tool. However, UBC may use Personal Information where staff have been involved in an accident or a near miss or report of unsafe driving, or in other reasonable circumstances to conduct an investigation into breach of law, conduct or UBC policy, including Operational Policy 0-09 UBC Campus Security Vehicle Use.
>
> 16. UBC may disclose Personal Information collected by the GPS system for purposes consistent with its collection, where it has received an order from a court or body with authority to the production or otherwise in compliance with law.

[20] UBC did not comment on the discrepancy between its own operational policy and its position in this inquiry, but in the end nothing turns on this, since, for reasons given below, I find that the information that UBC collects is 'personal information' within the meaning of FIPPA.

What is 'personal information' for the purposes of this case?

[21] FIPPA defines 'personal information' as "recorded information about an identifiable individual other than contact information".[14] As UBC notes, to be 'personal information', information must be about "an identifiable individual". Citing Ontario decisions, UBC says it is "not reasonable to expect that an individual may be identified if the information from the GPS system is disclosed."[15] Ontario's *Freedom of Information and Protection of Privacy Act* ("Ontario's FIPPA") also requires that information must be about "an identifiable individual", and it has been held there that in order for information to be personal information, it must be reasonable to expect that an individual may be identified if the information is disclosed.[16]

[22] The question is not, as UBC's submission suggests, whether it is reasonable to expect that an individual may be identified "if the information from the GPS system is disclosed". In the Ontario orders cited by UBC, the question of identifiability was assessed for purposes different than those involved here. In those cases, the issue was whether an individual could be identified by either an access to information applicant, or others who might receive the information once it had been disclosed, using the disclosed information and other information available to recipients. Here, the issue is whether the GPS system information is, in UBC's hands and not someone else's, information about "an identifiable individual". The question is whether the system information is reasonably capable of identifying a particular employee either alone or when combined with other information that UBC has.[17]

[23] UBC cites no British Columbia decisions on FIPPA's requirement that information be about "an identifiable individual", even though a number of orders have dealt with it.[18] Consistent with those decisions, and authorities from other

---

[14] The term "contact information" covers business contact information. It is not in issue here.

[15] Initial submission, para. 32.

[16] UBC cites, at para. 28 of its initial submission, Ontario Order PO-2715, upheld on judicial review: (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.). This same approach was applied in Order PO-2811, 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.

[17] I note, in passing, that the Supreme Court of Canada will consider the Ontario test for identifiability in the context of disclosure of records in response to access requests, having granted leave to appeal on December 20, 2012: *Ministry of Community Safety and Correctional Services v. Information and Privacy Commissioner*, 2012 CanLII 81996 (SCC). The case arises from Ontario Order PO-2811, where an adjudicator found that the first three characters of registered sex offenders' postal codes did not constitute 'personal information' that had to be redacted from records. The Divisional Court and Court of Appeal upheld this finding and the Ministry obtained leave to appeal.

[18] These decisions were identified recently in Investigation Report F12-04, [2012] B.C.I.P.C.D. No. 23, *e.g.*, Order 04-06, [2004] B.C.I.P.C.D. No. 6.

jurisdictions, I recently said this about the issue in Order P12-01, a decision issued after the submissions in this case:[19]

> 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.

[24] In Order P12-01, the employer assigned a service vehicle to each elevator mechanic who had exclusive use of it. This is not the case here. However, the evidence establishes that Campus Security employees generally patrol alone. It is reasonable to infer from the evidence that, at any given time during a shift, only one employee is assigned to drive a vehicle. It is also reasonable to infer that UBC is able, using other shift assignment information, to ascertain the identity of the employee who is driving a patrol vehicle at a given time. This inference is supported by UBC's GPS policy, mentioned above. I am satisfied that the information in issue relates to "an identifiable individual".

[25] However, noting that the definition of 'personal information' refers to information that is "about" an individual, UBC says this information is not "about" individuals. It relies on the Federal Court of Appeal's decision in *Canada (Information Commissioner) v. Canada (Canadian Transportation Accident Investigation and Safety Board*),[20] and *Otis Canada Inc. v. International Union of Elevator Constructors, Local 1*,[21] a British Columbia labour arbitration decision. For its part, CUPE cites PIPEDA Case Summary 2006-351 in support of its argument "that the information being collected through the use of the GPS devices is 'personal information' as defined in Schedule 1 of FIPPA".[22]

[26] I do not propose to discuss either *NAV Canada* or *Otis* in any detail, as I recently dealt with them at some length in Order P12-01. For the reasons given below and in Order P12-01, neither of these decisions is persuasive in determining what 'personal information' means in FIPPA.

[27] FIPPA's definition of 'personal information' is to be interpreted applying well-established interpretive rules:

> 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

[19] At para. 82.
[20] 2006 FCA 157, leave to appeal denied, [2006] S.C.C.A. No. 259 (Q.L.).
[21] [2010] B.C.C.A.A.A. No. 121.
[22] Initial submission, para. 22.

> sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.[23]

[28] As regards FIPPA's "object", s. 2(1) says the "purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy". One way in which this overall goal is achieved is by, as s. 2(1)(d) says, "preventing the unauthorized collection, use or disclosure of personal information by public bodies".

[29] In Order P12-01, I concluded that PIPA's definition of 'personal information' was broader than the organization argued:

> 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.

[30] Order P12-01 dealt with 'personal information' under PIPA, which nowhere refers to "privacy" or "personal privacy". The fact that FIPPA's s. 2(1) refers to "personal privacy" does not, however, necessarily drive a different interpretation of what is 'personal information' under FIPPA as contrasted to under PIPA. FIPPA refers to "personal privacy" in the sense of the privacy of individuals, which is distinct, of course, from protections that might otherwise be afforded by statute or other law to information of or about government or other entities. FIPPA's substantive provisions, certainly, reflect internationally-accepted 'fair information practices'. These are generally expressed in personal information legislation as rules that place reasonable limitations on the power of public institutions to compel individuals to give up their personal information without consent. This aspect of FIPPA's legislative aims is articulated clearly in ss. 2(1)(c) and (d). In the final analysis, nothing in FIPPA's statement of purpose alone suggests that 'personal information' in FIPPA and in PIPA have different meanings.

[31] In fact, where two statutes deal with similar subject-matter, there is much to be said for interpreting the same or similar terms in the same way, assuming

---

[23] *Rizzo & Rizzo Shoes Ltd.,* [1998] 1 S.C.R. 27, para. 21. Most recently, see Order P12-01, and also see Reference re Broadcasting Regulatory Policy CRTC 2010-167 and Broadcasting Order CRTC 2010-168, 2012 SCC 68. Further, s. 8 of the *Interpretation Act* says that a statute must 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."

the overall statutory context and legislative purpose allow it. In Order P12-01, I said that exclusion of 'work product information' and 'contact information' from PIPA's definition of 'personal information' indicates that the definition's introductory language—"about an identifiable individual'—is broader than the organization argued. The PIPA concept of 'work product information' and its exclusion from 'personal information' do not mandate a different meaning for the otherwise similar language in FIPPA's definition of 'personal information'. Bearing in mind the stated statutory purposes of FIPPA and its language, I conclude that it is appropriate to take a similar approach to interpreting 'personal information' as I took in Order P12-01 for the similar PIPA definition.

[32] In saying this, I have kept in mind, as I did in Order P12-01, the fact that, in *NAV Canada*, the Court interpreted the comparable federal definition more narrowly, applying a concept of 'privacy' that it derived from passages in *Charter of Rights* decisions dealing with search and seizure, relying on a law journal article from the 1890s, and citing statements in a 1972 federal government report on computers and privacy. The Court took this approach having cited the purpose statement in s. 2 of the federal *Privacy Act*, which refers to protecting the "privacy of individuals with respect to personal information about themselves held by a government institution". To the extent the Court took this statement as a mandate for a narrower interpretive approach, relying on these disparate sources, I respectfully disagree with that analysis.[24]

[33] The difficulties raised by the *NAV Canada* approach, where the Court referred to conversations between pilots and air traffic controllers as "information of a professional and non-personal nature", can readily be seen.[25] The Court acknowledged that recorded cockpit communications could lead to identification of specific individuals. It also acknowledged that the information might "assist in a determination as to how he or she has performed his or her task in a given situation". But it insisted that this information "does not thereby qualify as personal information" because it did not "match the concept of 'privacy' and the values that concept is meant to protect".[26] The Court admitted that the information "may well in certain circumstances be used as a basis for an evaluation of their authors' performances".[27] Yet it insisted that "the possibility of

[24] As I noted in Order P12-01, tension exists between the narrower interpretation of 'personal information' in *NAV Canada* and that expressed by the Supreme Court of Canada in decisions such as *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, and *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police*, 2003 SCC 8, [2003] 1 S.C.R. 66.
[25] Para. 54.
[26] Para. 54.
[27] Para. 55.

such eventual use" cannot transform the communications into personal information, since they had "no personal content".[28] With respect, I have difficulty accepting this approach. I also note that in *Dagg*, which was cited in *NAV Canada*, La Forest J. distinguished between information about a government employee's position and "information relating primarily to individuals [government employees] themselves or to the manner in which they choose to perform the tasks assigned to them is 'personal information'."[29] This observation is difficult to square with the *NAV Canada* approach.

[34] UBC also relies on orders under Ontario's FIPPA holding that, to be 'personal information' under Ontario's FIPPA, the information must "be about the individual in a personal capacity", with information that is "associated with an individual in a professional, official or business capacity" falling outside this.[30] It should first be underscored that the Ontario orders carefully acknowledge that such information is *generally* not personal information; even these types of information may be 'personal information' if it reveals something of a personal nature about the individual.[31]

[35] As regards the FIPPA definition, if the Legislature wished to exclude professional, official or business information from the scope of 'personal information', it could have done so explicitly. It chose instead to exclude only 'contact information', defined as "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual".[32] The Legislature went no further, however, suggesting that

[28] Para. 55.

[29] The majority was in agreement on this point. This was pointed out in Order F08-03, [2008] B.C.I.P.C.D. No. 6, at para. 85.

[30] Initial submission, paras. 26 and 27, citing several decisions of the Office of the Information and Privacy Commissioner of Ontario. UBC also says decisions by the Office of the Privacy Commissioner of Canada also "provide useful guidance" on the meaning of 'personal information', yet fails to cite any federal decisions on the point.

[31] See, for example, Order PO-2763, [2009] O.I.P.C. No. 31. I note here, as an aside, that UBC says, at para. 22 of its initial submission, that this Office "has not provided any detailed discussion on the interpretation and scope of 'personal information' in FIPPA or PIPA" to date, adding that other Canadian jurisdictions "do provide useful guidance". This overlooks the many orders and other publications from this Office, going back to the earliest days of FIPPA, that have addressed what is and is not 'personal information' under FIPPA. There is a considerable body of decisions and guidance from this Office on what 'personal information' means under both FIPPA and PIPA. As one example only, Order F08-03, considered *NAV Canada* and the line of Ontario decisions on which UBC relies here. As paras. 80-87 of Order F08-03 indicate, that decision is not supportive of UBC's position in this inquiry. Nor is Order F07-18, [2007] B.C.I.P.C.D. No. 30, which I discuss below.

[32] These kinds of information are quite clearly within the kinds of information that the Ontario cases exclude from 'personal information'.

FIPPA's otherwise general language—"recorded information about an identifiable individual"—is not further circumscribed. I also note that the Legislature has explicitly excluded from PIPA's personal information definition 'work product information', which would fall within professional, official or business information. The Legislature has not similarly excluded 'work product information' from FIPPA's 'personal information' definition. Last, I note that ss. 22(1) and (4) of FIPPA address some of the policy concerns likely underlying the Ontario approach to *generally* excluding professional, official or business information from 'personal information'. At the end of the day, I decline to read into FIPPA's definition the kind of "professional, official or business capacity" carve-out that UBC advances.

[36] Nor do I find persuasive UBC's reliance[33] on comments made in *Dagg* by La Forest J., to the effect that the government institution's employees would have had a reasonable expectation that information in workplace sign-in logs would not be disclosed to the public. UBC cites this to support its contention that whether an individual has a reasonable expectation of privacy is relevant to the analysis of whether information is 'personal information'. UBC says it is "well established that there is no reasonable expectation of privacy for actions taking place in public".[34]

[37] In essence, UBC says that, because Campus Security employees are in public when they are driving patrol vehicles, location information and other vehicle-related information cannot be their 'personal information'.[35] UBC says

[33] Initial submission, para 30. As regards La Forest J.'s comments in *Dagg*, La Forest J. explicitly stated, at para. 71, that his observations were "not strictly necessary" for his analysis, so they are not part of the actual judgement itself. Nor are they of any real assistance in the context of this case, which involves interpretation of a 'personal information' definition that is quite different from the federal *Privacy Act* definition.

[34] Initial submission, para. 30.

[35] Contrary to what UBC asserts in such general terms, it is not "well established" that there is no reasonable expectation of privacy for actions taking place in public. The two Supreme Court of British Columbia decisions on which UBC cites in saying this involved interpretation of British Columbia's *Privacy Act*. Section 1(1) of that Act provides that it is a civil wrong for "a person, wilfully and without a claim of right, to violate the privacy of another", but, significantly, s. 1(2) provides that "the nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others". Section 1(3) stipulates that, in determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties." Nothing in FIPPA comes close to this kind of balancing language, which speaks to many contextual elements in deciding whether privacy has been breached. These two *Privacy Act* cases are, therefore, not helpful in FIPPA's interpretation. Further, Canadian and United States courts have held, in the constitutional setting, that use by law enforcement of GPS devices to track movements of individuals in their vehicles *does* engage privacy interests. In *R. v. Wise*, [1992] 1 S.C.R. 527, a majority of the Supreme Court of Canada held that "there remains an expectation of privacy in automobile travel", even though "it is markedly decreased relative to the expectation of privacy in one's home or office" (p. 534). A more recent example is *U.S. v. Jones*,

that "[a]nyone walking around on UBC's campus can witness security staff doing their job and witness their location in a public space as they do their job" and this is the same information "captured by the GPS system"[36] Because anyone can view where its Campus Security employees are at a given time, that information is public and therefore there can be no reasonable expectation of privacy.[37] It is not "information that goes to the core concepts of personal privacy, such as intimacy, identity, dignity and integrity of the individual", revealing nothing "of a personal nature about the individual."[38] UBC's suggestion that there is *no* privacy interest where information that is collected, and used, relates to an individual's whereabouts in public spaces is not particularly strong in general terms.

[38] More directly, as regards FIPPA's interpretation, it is not of assistance in determining what is meant by 'personal information'. Information that would be personal information if it were not public does not, under FIPPA, cease to be personal information because it becomes public. Knowledge by others does not transform the nature of the information itself.

[39] UBC says, again, that there has been no "detailed discussion" by this Office about what is 'personal information'. It cites decisions from Ontario's Information and Privacy Commissioner on the meaning of "identifiable individual" and "about" an individual. It cites British Columbia court decisions under the *Privacy Act*. It relies on *NAV Canada* and *Otis*. It mentions no other Canadian privacy commissioner decisions. Yet, as I have already explained, many of this Office's decisions do address what 'personal information' means for FIPPA's purposes. Some of those decisions actually are at odds with UBC's position in this inquiry, one of them being Order F07-18, which involved UBC itself taking a position similar to that it takes here.

---

132 S.Ct. 945 (2012), where, for example, Alito J. (writing for himself and three other justices) said, at p. 964, that "the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy" in individuals' movements in public spaces.

[36] It is, to say the least, highly debatable to equate casual human observation of an individual's location in a public space with the information generated by a GPS system that tracks movement continuously, transmits it in real time for monitoring, and records it possibly for posterity. I will note here that UBC's reliance, at para. 49 of its initial submission, on Order No. 331-1999, [1999] B.C.I.P.C.D. No. 44, is misplaced. In that order, it was held that an access to information applicant should be given a copy of a letter he had already received, with the name of a police officer about whom he had complained being included in the disclosed copy. In other words, the applicant already knew the officer's name and further disclosure to him through his access request was permitted under s. 22. This is quite a different situation from the present. There is a material difference between human observation of another's location in public, as UBC posits, and disclosure of a record of personal information to someone who already has it.

[37] Initial submission, para. 49.

[38] Initial submission, para. 33.

[40] For the above reasons, it is not appropriate to interpret what is 'personal information' under FIPPA by applying a reasonable expectation of privacy test. Nor, for the reasons just given and as discussed in Order P12-01, am I persuaded that what can be called the *NAV Canada* approach is appropriate under FIPPA.[39]

[41] The next issue is whether, in fact, UBC is collecting 'personal information'.

Is UBC collecting 'personal information'?

[42] Information about the location of a Campus Security employee during her or his shift, and information about where the employee has been or is driving in real time, is personal information. Similarly, information from the GPS system about the vehicle's speed can be personal information because it is information about how the employee is driving (fast, slow, contrary to UBC policy or the law, and so on) and that is why UBC reserves the right, in certain cases, to collect and use it to investigate and possibly sanction employees for their actions.

[43] UBC concedes that information collected by the system "may allow UBC, after linking the operator to the vehicle, to determine how the operator performed their task in a given situation."[40] It also acknowledges that, on at least one occasion, it had recourse to system information to confirm whether a patrol vehicle had left campus and had been speeding. UBC says it did not use this information in the related disciplinary process, but the fact remains, it had recourse to the information to determine what its employee had done, measured against UBC's rules on employee use of vehicles.

[44] This purpose for collecting the GPS system information is confirmed by UBC's own GPS policy. It confirms that UBC's purposes in collecting information from the GPS system include assessing, as against UBC's standards, how its employees perform their work duties. Section 12 of the policy says the information "will be used primarily for the purpose of Campus Security patrol officer safety." Section 13 says, however, that UBC will also use the system to "monitor the usage of vehicles…to ensure that vehicles are being used in accordance with laws pertaining to speed and to ensure that vehicles are not leaving the duty jurisdiction without permission." Although section 15 says UBC "will not use the GPS system as a performance management tool", it also says

[39] As was the case in Order P12-01, the parties were given an opportunity to make submissions about *Jones v. Tsige*, 2012 ONCA 32, a decision of the Ontario Court of Appeal that recognizes the existence in Ontario of a common law cause of action for 'intrusion upon seclusion'. In the end, that case, while of general interest, does not assist in deciding the issues at hand under FIPPA.

[40] Para. 35, initial submission.

that it "may use Personal Information where staff have been involved in an accident or a near miss or report of unsafe driving, or in other reasonable circumstances to conduct an investigation into breach of law, conduct or UBC policy, including Operational Policy 0-09 UBC Campus Security Vehicle Use."

[45] Consistent with the above discussion, and what I said in Order P12-01, I find that, when UBC collects and uses system information disclosing the whereabouts of a patrol vehicle, it is collecting personal information of the driver assigned to that vehicle for the shift in question. The information discloses the location and movements of the employee, even allowing for the fact that, at times, the location may be general[41] because the employee may be out of the vehicle and nearby. The fact remains even in such a case that the system will give UBC a reasonably good idea of where its employee is on campus. UBC's GPS policy and its submissions in this inquiry confirm that it uses the GPS system for this purpose.

[46] I am also satisfied that system information disclosing vehicle speed is information about how the assigned employee is driving, whether she or he is driving faster than UBC's policy or rules allow, or faster than the law allows. This is a feature of the system that, as noted above, UBC makes use of for exactly these purposes. It wants to know whether its Campus Security employees are speeding or driving unsafely—that is a reason for its use of the system. This is, as with location information, confirmed by UBC's GPS policy and its submissions in this inquiry.

[47] It should be noted here in passing that, while there is no sufficient basis to conclude that UBC is collecting system information to ensure hours of work are kept, if it were to do so, the information would in my view be 'personal information'. In that event, the guidance below would have to be kept in mind.

[48] **Is UBC Authorized to Collect the Personal Information?**—The next question is whether UBC is authorized under FIPPA to collect and use the personal information collected through its use of the GPS system.

[49] As regards collection, UBC relies on s. 26(c) of FIPPA, which authorizes a public body to collect personal information if the information "relates directly to and is necessary for a program or activity of the public body". It does not rely on other grounds set out in s. 26. Respecting the first element of this provision,

[41] As in Order P12-01, there is no evidence before me as to the accuracy of the location information, whether it is to the metre or something else. I am prepared to infer, as the parties clearly appear to do, that the location is communicated with a fair degree of on-the-ground accuracy and precision.

UBC says the personal information "relates directly to" its program of campus security, including the elements of security staff safety and dispatch efficiency.[42] On the second ground, UBC says the information is "necessary for" that program. It relies on Order F07-10, which laid out certain criteria for determining whether personal information is "necessary" for a program or activity.

[50] CUPE's perspective on the appropriate test for collection and use of personal information differs materially from UBC's. It cites decisions of the Office of the Privacy Commissioner of Canada under the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), notably the four-part test applied in PIPEDA Case Summary 2006-351.[43] PIPEDA applies to certain private sector activity, not the federal government. In Order P12-01, I recently declined to adopt this test in cases arising under PIPA. Nor do I consider that four-part test to be appropriate in cases arising under FIPPA. Rather, the approach in Order F07-10 is, as I will now discuss, the appropriate approach.

[51] As was noted in Order F07-10, in FIPPA's context we are dealing with public bodies that often have the legal authority to compel individuals to give up their personal information without consent. FIPPA's accountability goals respecting personal information practices are expressed in s. 2(1), including the legislative aim of "preventing the unauthorized collection, use or disclosure of personal information by public bodies". I therefore agree that, as was said in Order F07-10, the collection of personal information by public bodies is to

> …be reviewed in a searching manner and it is appropriate to hold them to a fairly rigorous standard of necessity while respecting the language of FIPPA. It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future. Nor is it enough that it would be merely convenient to have the information.[44]

[52] This does not mean, however, that personal information will be considered to be "necessary"

> ...only where it would be impossible to operate a program or carry on an activity without the personal information. There may be cases where personal information is "necessary" even where it is not indispensable in this sense. The assessment of whether personal information is "necessary" will be conducted in a searching and rigorous way. In assessing whether personal information is "necessary", one considers the sensitivity of the

[42] Initial submission, para. 51.
[43] That test involves answering these questions: 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?
[44] Para. 48.

> personal information, the particular purpose for the collection and the amount of personal information collected, assessed in light of the purpose for collection. In addition, FIPPA's privacy protection objective is also relevant in assessing necessity, noting that this statutory objective is consistent with the internationally recognized principle of limited collection.

[53] The approach taken in Order F07-18 by Adjudicator Catherine Boies Parker is also of assistance.[45] In that case, UBC had installed software on an employee's computer and used it to surreptitiously monitor his access to the internet for personal purposes during work hours. The software collected information identifying the websites the employee visited, when he visited them and the length of time he was on each website. It also captured screenshots of web pages. This information was used in terminating the individual's employment. As I noted above, UBC argued that information about the websites visited was not personal information, and argued in the alternative that, if it was personal information, s. 26(c) of FIPPA authorized its collection.

[54] The Adjudicator cited with approval the approach taken in Order F07-10, including the principle that, "in considering whether information is necessary, one should consider the sensitivity of the personal information, the particular purpose for the collection and the amount of personal information collected, assessed in light of the purpose for collection."[46] As regards application of these principles, she said this:

> [71] Applying the principles set out above to this case, I find that the test is not whether it is impossible to manage the employment relationship without the collection of the disputed information. As a result, I agree with UBC that information may be considered necessary even if there are alternative means of managing the employment relationship. However, I do not agree that the existence of alternatives is not relevant to the assessment of whether the collection of information is necessary.
>
> [72] The cases relied on by UBC do not exclude consideration of alternatives in the assessment of reasonableness; they simply find that an employer is not required to exhaust all other alternatives, regardless of the reasonableness of those alternatives. Similarly, in the context of FIPPA, I find that the employer is not required to exhaust all possible other means of managing the relationship, without regard to whether those alternative

[45] After it did not succeed in that case, UBC filed an application for judicial review in the Supreme Court of British Columbia. As of this date, however, UBC has not sought to set the matter down for a hearing on the merits, some five years after seeking relief. In any case, I consider Order F07-18 to be soundly reasoned.

[46] Order F07-18, para. 70.

> means are reasonable or likely to succeed. However, if there are reasonable and viable alternatives to the surreptitious collection of personal information, that is a matter to be considered in determining whether the collection was necessary for the purposes of s. 26(c).[47]

[55] Accepting that UBC's collection of the personal information was motivated by concerns about the employee's productivity, and by evidence that he was "'surfing the net on company time'",[48] she also agreed with UBC that "reasonableness is a factor in considering whether the collection of information is necessary under s. 26(c)."[49]

[56] With these considerations in mind, the first question to be decided is whether UBC is collecting personal information that is "directly related to" a program or activity. UBC says it collects the GPS information for employee safety purposes, patrol dispatch efficiency and maintenance purposes. I find that collection and use of personal information for employee safety purposes, patrol dispatch efficiency and maintenance purposes is directly related to a UBC program or activity. Collection of personal information by UBC's Campus Security department for these purposes falls well within the mandate and operations of that department. Consistent with Order F07-18, I also find that collection of personal information for potential use in investigating employee conduct or accidents involving UBC vehicles is directly related to a UBC activity or program, *i.e.*, its management of employment relationships.

[57] The second question is whether the personal information being collected is "necessary for" a UBC program or activity.

[58] As regards employee safety, CUPE says UBC has "not even attempted to show" that its collection of GPS information is "justified" for safety or dispatch purposes, "other than by making bald assertions."[50] It says "there is no information or evidence as to how any outstanding issues, if they did or do exist, are corrected by the use of the GPS monitoring devices."[51] In advancing its case, CUPE does not refer to Order F07-10 or Order F07-18. It cites s. 26 by

---

[47] Footnotes omitted.
[48] Para. 73.
[49] Para. 90. The Adjudicator went on to find against UBC on the evidence. She held that it was not reasonable for UBC to surreptitiously collect the information when it had taken no other steps to address the concerns. She held there was no real evidence that alternative means of addressing the problem would have been ineffective. She therefore found that, given the evidence before her, collection of the information relating to the employee's internet use was not necessary to the management of the employment relationship and so the collection was not authorized under s. 26(c).
[50] Initial submission, para. 38.
[51] Initial submission, para. 43.

number, but its arguments rely on principles outlined in PIPEDA Case Summary 2006-351. That decision dealt with use of GPS by an employer regulated under PIPEDA, the language, structure and purposes of which are by no means the same as FIPPA's. I declined to apply PIPEDA Case Summary 2006-351 in Order P12-01—it is even less helpful here given the language and purpose of s. 26(c).[52]

[59] Turning to the evidence, UBC refers to its "legislative obligation to ensure the safety of workers who work alone", saying that, without the system, UBC is only able to track the location of an employee who does not respond to a check-in call by conducting an in-person search of a very large campus. The GPS information enables it to more quickly locate an injured employee, UBC says.[53] The affidavit of Tony Mahon, UBC's Director of Campus Security, speaks to the employee safety aspects of the GPS system's use. He notes, among other things, that, due to the size of the campus, Campus Security employees sometimes are out of radio contact with the operations centre. He also notes that "patrol vehicles are generally occupied by one security staff member."[54] This aspect of the radio communications situation makes the periodic safety check-in calls, I infer, sometimes less than reliable.

[60] Information disclosing the location of a Campus Security patrol officer at a given moment is not particularly sensitive viewed in light of the officer safety goal of collection. I accept that the GPS information provides a more reliable means than radio communication does of knowing where employees are to be found on a large campus with many buildings and other structures. I also accept that the information enables Campus Security operations staff to more quickly and reliably locate patrol officers who do not respond to radio check-in calls than would be the case through in-person searches of the campus.

[61] As regards dispatch efficiency, Tony Mahon deposed that, owing to the real-time location monitoring afforded by the GPS system, a shift supervisor can "quickly dispatch the closest vehicle to the call in question", referring to the example of rapid response to a break-and-enter-in-progress call.[55] He also deposed to the fact that, at any given time, the more than 400 hectare campus is patrolled by only two vehicles.[56]

---

[52] I noted earlier UBC's failure to refer to relevant decisions of this Office—the same observation applies to CUPE's reliance on a PIPEDA case, without adverting to relevant FIPPA decisions of this Office.
[53] Initial submission, para. 45.
[54] Mahon affidavit, para. 9.
[55] Mahon affidavit, para. 21.
[56] Mahon affidavit, para. 9.

[62] As regards dispatch efficiency, I take this evidence to mean that GPS improves responsiveness because it shows the geographic location of the two patrol vehicles in real time. Without the system, the dispatcher would have to call each vehicle not already engaged on a call, obtain descriptions of their locations, manually find the locations on a map, decide which vehicle is closer to the call scene, and then dispatch the closest vehicle. As with officer safety, I find that the location information involved is not sensitive in context, and I further accept that it improves the efficiency of patrol dispatch. In reaching this latter finding, I have kept in mind that patrol dispatch efficiency touches on the safety of students and other campus users and on property loss and damage.

[63] UBC's vehicle maintenance aims could be served without the system, CUPE says—"there are simple and effective methods" to ensure proper vehicle maintenance.[57] No real detail is given as to use of the system for vehicle maintenance purposes. Tony Mahon simply says that Campus Security "also uses the information provided by the GPS system to monitor the kilometres travelled by the vehicles for maintenance purposes."[58] In collecting GPS system information disclosing the distance a vehicle has travelled in a certain period, UBC is collecting information that reveals the vehicle's status. As was the case regarding similar uses of information in Order P12-01, UBC is not collecting this information to use it in relation to an individual. Its collection and use of this information to ensure proper vehicle maintenance is not objectionable.

[64] This leaves collection and use of GPS information in relation to the manner in which UBC's employees drive their patrol vehicles. The thrust of CUPE's complaint is that UBC "clearly intends to monitor employees for reasons unrelated to" employee safety, dispatch efficiency or vehicle maintenance, and that use of the information for monitoring how employees drive "or in other reasonable circumstances" (quoting UBC's policy) is not permitted by FIPPA.[59] CUPE says this policy language "firmly establishes that the information may be used routinely for purposes that are not demonstrably justified or consistent with the stated purposes for introducing the system."[60] This, CUPE says, "clearly invites overuse and abuse of the collected Personal Information."[61]

[65] UBC denies that any inferences about other uses can be drawn. It also says that Tony Mahon's evidence shows the contrary, demonstrating that "UBC supervisors do not monitor the vehicles through the GPS system as an employee

[57] Initial submission para. 37.
[58] Mahon affidavit, para. 22.
[59] Initial submission, paras. 32, 33 and 38.
[60] Initial submission, para. 33.
[61] Initial submission, para. 45.

management tool."[62] The evidence, UBC says, shows that the system has only been used once "in relation to an employee management issue", and then only "to verify that an event self-reported by the employee in question had in fact occurred." This after-the-fact use to confirm the incident is different, UBC says, from using the system to "detect the incident in the first place."[63] UBC goes so far as to assert that the evidence "establishes that the GPS System is used for safety and dispatch purposes, and not as an employee management tool."[64]

[66] It is understandable that CUPE thinks that UBC uses GPS information to routinely monitor its Campus Security employees for employment management purposes. UBC's GPS policy explicitly states that, while the system will be "used primarily for the purpose of Campus Security patrol officer safety, … . UBC will monitor the usage of vehicles…to ensure that vehicles are being used in accordance with laws pertaining to speed and to ensure that vehicles are not leaving the duty jurisdiction without permission."[65] The policy also says that, while the system will not be used "as a performance management tool", UBC may use "Personal Information" from the system where "staff have been involved in an accident or near miss or report of unsafe driving."[66]

[67] This language is less than clear. On the one hand, the policy says UBC "will monitor use of vehicles" to ensure compliance with speeding laws. On the other hand, the policy says the system will not be used "as a performance management tool", with GPS information being used only where an accident or other circumstances trigger its use. The stated purposes overlap in a material degree as regards safe vehicle use, but it is not clear whether this is achieved by routine monitoring or after-the-fact recourse to information only when triggered by other factors. There is, to be sure, a difference between routine monitoring of employee actions through GPS and cause-based, after-the-fact, resort to GPS information, yet UBC's policy fails to clearly distinguish between the two.

[68] The evidence before me, on the other hand, is clearer. Tony Mahon deposed as follows:

> UBC supervisors do not monitor the vehicles through the GPS system as an employee management tool. However, to the extent that UBC must investigate an incident that involves a patrol vehicle, such as a report of

[62] Reply submission, para. 9.
[63] Reply submission, para. 10.
[64] Reply submission, para. 19.
[65] GPS policy, sections 12, 13 and 15. Tony Mahon deposed that UBC supervisors do not monitor vehicles as an employee management tool, but he also acknowledged that UBC has used GPS information in relation to an employee's performance, and in a disciplinary context at that, for precisely the kinds of purposes contemplated by its own policy.
[66] GPS policy, section 15.

> speeding or a vehicle accident involving a Campus Security vehicle, UBC may conduct an investigation after the fact by reviewing the information provided by the GPS devices in the vehicles. That is to say, while UBC does not use the GPS system to actively monitor employee performance or conduct, UBC may, from time to time, use the system in response to employee issues involving the use of the vehicles that it has learned of through other means.[67]

[69] The only time UBC has used the information "in relation to an employee management issue" was, Mahon deposed, in response to the self-reported incident mentioned earlier. UBC had recourse to the GPS information to verify what happened, but did not use the information in the disciplinary process itself. CUPE has expressed concerns around UBC's possible future use of the information for routine monitoring of employees, but the only evidence before me is that UBC does not do this and, in fact, has only once had recourse to the information and then only after the fact.

[70] In Order P12-01, I considered whether PIPA authorized an organization to collect GPS-generated location information to determine if an employee had complied with his or her hours of work obligations and the employer's rules around personal use of company vehicles. As I have already found here, I concluded that the location information was not particularly sensitive, and went on to give weight to the "rules under which information is accessed and used" by the employer. However, to be clear, consistent with what I said in Order P12-01, if a public body were to engage in continuous, real-time monitoring of employees' whereabouts, during or outside work hours, for employment management purposes, I would look particularly carefully at the situation.

[71] Where clear and specific grounds exist that make the GPS information necessary for the purpose of investigating employee vehicle use, that information would, in my view, be "necessary" for the purposes of FIPPA. Examples include an accident involving a Campus Security vehicle, a complaint of speeding or other inappropriate or unlawful driving, or a report of a Campus Security vehicle being off-campus. There may also, as UBC's policy contemplates, be other circumstances that would make use of the GPS information "necessary", and it would not be appropriate for me to close off that possibility here. Suffice it to say that any such other circumstances would also have to be clear and specific to authorize collection by UBC.

[72] CUPE also raises concerns about other issues and I will now deal with those.

---

[67] Mahon affidavit, para. 38.

[73] **Indirect Collection and Notice of Collection**—CUPE says UBC has run afoul of the requirement in s. 27(1) that, with certain exceptions, personal information is to be collected "directly from the individual the information is about". UBC counters by saying that, in Order F07-18, the Adjudicator held that information gathered through monitoring of a UBC employee's computer was collected directly from that individual:

> [104] Information is collected directly from an individual when the disclosure to the public body occurs as a result of the individual's own activities. Information is collected indirectly when it is obtained from some source other than the individual concerned. Here, the GESS software and the Log Report were the means by which the information was recorded—they were not, however, the source of that information. The source was the complainant's own activities, which led to the recording of the information which was printed in the various reports. As a result, I find that the information was collected directly from the complainant, and that, for the reasons explained above, notice was required.

[74] I agree with this observation and find that the personal information UBC collects using the GPS system is collected directly from the employees within the meaning of s. 27(1).

[75] Even if this were not the case, I have already found that UBC is collecting personal information for employment management purposes and note that s. 27(1)(f) authorizes a public body to collect personal information indirectly if:

> (f) the information is about an employee, other than a service provider, and the collection of the information is necessary for the purposes of managing or terminating an employment relationship between a public body and the employee, …

[76] CUPE also contends that UBC has not given notice of collection in the manner required under s. 27(2). It says that UBC "did not formally advise" employees or CUPE that is was collecting personal information "until approximately one full year after implementation of the GPS devices."[68] UBC also failed, CUPE says, to give notice of the purpose for collecting the personal information, the legal authority for doing so or the contact information for a UBC official who could answer questions or concerns.[69]

[77] As regards the timing of the notice of collection, it is my view that FIPPA requires notice of collection to be given before the personal information is collected, not after. This interpretation is supported by the purposes of the provision, interpreted in the context of Part 3 and FIPPA as a whole, and the

[68] Initial submission, para. 23.
[69] Initial submission, para. 24.

language of ss. 27(3)(b)(i) and (ii) and (4). Adjudicator Boies Parker interpreted s. 27(2) in the same way in Order F07-18 and I agree with her.

[78] UBC says it did give notice before collection. It cites the following evidence from Tony Mahon's affidavit:

> 25. During the two month period prior to installing the GPS units in the vehicles, UBC Campus Security employees were advised on several occasions during daily morning staff meetings that UBC Campus Security was going to have the units installed. During these meetings it was explained to staff that the purpose for installing the GPS devices was for lone worker safety and for effective dispatch.
>
> 26. I also advised the staff's union during a local working conditions meeting sometime in late June or early July 2008 that the devices were being installed in the near future for safety and dispatch purposes, but there was no discussion on this topic at the meeting.
>
> …
>
> 36. In January 2010, UBC issued a GPS Campus Security Vehicle policy, and provided a copy to the Complainant [CUPE] on or about February 11, 2010.

[79] In UBC's view, the verbal notice given to staff and CUPE, and the issuance of the policy, "satisfy UBC's obligation to notify under s. 27(2)."[70]

[80] CUPE's reply submission tendered evidence from Glen MacNeil, a CUPE shop steward and Campus Security patrol officer, which contradicted UBC's evidence on notice. This triggered an objection from UBC that, by providing this evidence in its reply and not its initial submission, CUPE was 'splitting' its case. After several communications back and forth from counsel to UBC, counsel to CUPE and my Office, it was decided that CUPE's evidence would be considered on this point. In the end, however, I need not consider that evidence and therefore have not done so. This is because, as I will now explain, UBC's own evidence establishes that the verbal notice Tony Mahon says he gave did not comply with s. 27(2).

[81] Section 27(2) says that an individual from whom personal information is collected must be advised of the purpose for collecting it, the legal authority for collecting it, and contact particulars for a public body representative who can answer the individual's questions about the collection.

[70] Initial submission, para. 67.

[82] Here, Tony Mahon's evidence is that he verbally advised employees and CUPE representatives that the GPS system was being installed for "lone worker safety and for effective dispatch" or, as he later put it, "safety and dispatch purposes". There is no other evidence to suggest that, before UBC began to collect personal information using the system, UBC mentioned the other purpose for which personal information was to be collected, *i.e.*, for monitoring how employees drive. Any notice that UBC gave in the manner attested to by Tony Mahon was, therefore, inadequate on this ground alone.[71] It was not until approximately 18 months after UBC started collecting personal information that it issued a written statement—its GPS policy of January 2010—that speaks to the purposes for collection of personal information through the system.

[83] Nor does Mahon's evidence show that UBC ever provided (through him or otherwise) the other information that s. 27(2) requires—legal authority for collecting the information and contact particulars for someone who could answer affected employees' questions about the collection. Even UBC's GPS policy, which came after UBC had, I am satisfied, started collecting personal information, does not adequately address the legal authority and contact person requirements. The policy has positive aspects, but it fails to address these two explicit FIPPA requirements.

[84] For these reasons, I find that UBC has not complied with its s. 27(2) obligation to give notice of collection.

[85] **Excessive Access to the Personal Information**—CUPE also raises concern about "which employees would be permitted to have access to the information gathered by the GPS tracking system."[72] In its reply submission, UBC counters by saying that the question "about storage and access" to information are properly addressed under s. 30, but the notice of hearing makes it clear that any such issues are outside the scope of this proceeding. The notice refers only to whether UBC is "collecting and using personal information contrary to ss. 26, 27 and 32 of FIPPA". UBC further argues, however, that Tony Mahon's affidavit addresses what UBC says is this s. 30 issue. In the circumstances, where the issue is not contained in the notice of hearing, I will not address this issue.

[86] I will note in passing, however, that Tony Mahon's affidavit contains evidence specifically speaking to the encrypted transmission, secure and encrypted storage in Canada of personal information collected through the system. It also speaks to Campus Security limiting operational access to the

[71] In making this finding, I leave aside the question of whether Mahon ever told employees that 'personal information' would be collected at all. His evidence speaks, arguably, to his describing a system and its uses, without explicitly notifying employee that 'personal information' *per se* would be collected.
[72] Initial submission, para. 34.

personal information to those dispatch and supervisory employees who have a need for that information to perform their duties.

CONCLUSION

[87] For the above reasons, I make the following orders under s. 58 of FIPPA:

1. Under s. 58(3)(a), I confirm that UBC has performed its duties under ss. 26 and 32 of FIPPA respecting the collection and use of personal information as described above; and

2. Having found that UBC has failed to give notice as required by s. 27(2) of FIPPA, under ss. 58(3)(e) and (4), I require UBC to stop collecting, using or disclosing personal information as described above until such time as:

    a. UBC has delivered to me evidence to my reasonable satisfaction establishing UBC's compliance with s. 27(2) of FIPPA; and

    b. I have thereafter confirmed in writing to UBC and to CUPE my reasonable satisfaction as to UBC's compliance with s. 27(2).

February 1, 2013

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

OIPC File No.: F10-41772