ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER P2008-010

September 30, 2010

ENGEL BRUBAKER

Case File Number P0549

Office URL: www.oipc.ab.ca

Summary: An unnamed police officer brought a complaint that the Organization, a law firm, had created a database which it was using to collect and disseminate information of Edmonton Police Service members who had engaged in misconduct. He complained that this database contravenes of the *Personal Information Protection Act*.

The Adjudicator found that any information in the database that is solely about the manner in which police officers performed their work is not the personal information of officers in the context of its collection, use and disclosure for the purposes of conducting defences against offence proceedings. However, she found that any information about the work of police officers that is intertwined with matters that are personal to them has a dual aspect, and is both non-personal and personal. She also found that information relating to officers' performance of their work that is collected, used or disclosed for initiating actions against officers is their personal information.

The Adjudicator held that she could make no order with respect to personal information that falls outside the Act under section 4(3)(k) (information in a court record).

The Adjudicator confirmed the decision of the Organization to collect, use and disclose, and to enter and retain in its database, any personal information of police officers that is publicly available.

She also confirmed the decision of the Organization to collect, use and disclose, and to enter and retain in its database, any personal information of police officers that is reasonable for the purposes of an investigation or legal proceeding. This includes any information that would be reasonable to collect, use and disclose to assist with an investigation for defending against an offence proceeding and for defending in an offence proceeding, for both existing and possible future offence proceedings in which the officer might be involved. It also includes information that would be reasonable to collect, use and disclose to assist with an investigation for initiating an action against an officer that is reasonably in contemplation and for pursuing such an action that is existing or reasonably in contemplation.

Statutes Cited: AB: *Administrative Procedures and Jurisdiction Act,* R.S.A. 2000, c.A-3; *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 4(1)(a), 4(1)(b); *Health Information* Act, R.S.A. 2000, c. H-5; Personal *Information Protection Act* S.A. 2003, c. P-6.5, ss. 1(f), 1(g), 1(k), 4(1), 4(3)(a), 4(3)k), 4(5)(a), 4(5)(b), 7, 8, 11, 14, 14(d), 14(e), 16, 17, 17(d), 17(e), 19, 20, 20(m), 20(j), 33, 52; *Personal Information Protection Act Regulation*, AR 366/2003, ss. 7(d), 7(e); *Police Act*, R.S.A. 2000, c. P-17, ss. 20(1), 20(1)(c), 45(2), 45(3), 51; **CANADA**: *Canadian Charter of Rights and Freedoms,* s. 7. *Personal Information Protection and Electronic Documents Act*, S.C. 2000.

Orders Cited: AB: 99-025, F2004-026, F2004-030, F2007-021, H2004-005, P2007-002, P2008-008, P2009-009; **ON**: P-721; MO-2025.

Court Cases Cited: *R.v. Zundel*, [1992] 2 S.C.R. 731; *Alberta (Attorney General)* v. *Krushell,* [2003] ABQB 252; *Ferenczy v. MCI Medical Clinics*, [2004] O.J. No. 775; *R.* v. *McNeil*, [2009] S.C.J. No. 3; *State Farm Mutual v. Privacy Commissioner of Canada* [2010] F.C. 736.

I. BACKGROUND

[para 1] On June 8, 2006, the Complainant, an unnamed police officer, brought a complaint (with the support of the Edmonton Police Association) that the Organization, a law firm, had created a database which it was using to collect and disseminate information of members of the Edmonton Police Service (EPS) who had allegedly used force against individuals, in contravention of the *Personal Information Protection Act* (PIPA or the Act).

[para 2] Mediation did not resolve the complaint, and the matter was moved to inquiry. At inquiry, the Criminal Trial Lawyer's Association applied and was granted status to participate as an intervenor.

[para 3] The Complainant's initial submission provided an e-mail in support of the complaint which the Complainant stated was sent on or about February 14, 2006 by an employee of the Organization (a student-at-law) (or by someone on her behalf) to an e-mail address described as "Crownbusters". The e-mail stated that the law firm has started a database to keep track of EPS members that are involved in files "where excessive force/misconduct is present", and indicated a willingness on the part of the law firm to receive and to share such information.

[para 4] As the e-mail in question was in my view sufficient to raise the issue of whether there had been a collection, use and disclosure of personal information by the Organization in contravention of PIPA, I asked the Organization to indicate whether it had a database such as that described in the e-mail, and if so, to give a further description of what the database contained.

[para 5] In a letter dated August 10, 2009, the Organization confirmed that it has maintained an electronic database since approximately 2006. In that database is an electronic file folder which contains the first and last names of EPS members and their regimental numbers. The Organization stated that the database contains subfolders which may contain one or more of the following about the police officers:

1) Electronic copies of Court transcripts or Court decisions;
2) Electronic copies or internet links to decisions of the Law Enforcement Review Board and of Presiding Officers (Designated Officers) appointed by the Chief to conduct hearings pursuant to the Police Act;
3) Newspaper articles and letters to the editor;
4) Letters to the Chief of Police and/or Edmonton Police Commission;
5) Letters from the Chief of Police and/or Edmonton Police Commission;
6) Records obtained from public bodies pursuant to the Freedom of Information and Protection of Privacy Act;
7) The name of a client and the Organization's file number; and
8) Synopses of information provided to the Organization with respect to potential misconduct

[para 6] The Organization also stated that it is in the very early stages of compiling similar information and records with respect to RCMP members, Sheriffs and Correctional Officers (For the purposes of this order, I will refer to all of these individuals as "police officers").

[para 7] The Organization stated that the information and records described above are compiled for the purpose of assisting their clients to "make full answer and defence to criminal charges and for other litigation or law enforcement purposes".

[para 8] The Organization also stated that only its members have access to the database. However, a lawyer within the firm may decide to disclose the information to lawyers outside of the Organization who request the information.

[para 9] The Organization provided initial and rebuttal submissions, as well as additional submissions, a rebuttal of the Complainant's additional submissions, and the additional evidence I had requested. The Complainant provided initial submissions, a comment on the Intervenor's request to participate, additional submissions, a rebuttal of the Organization's additional submissions, and comments on the Organization's additional evidence. The Intervernor also provided a submission.

II. ISSUES

[para 10] The inquiry notice for case file P0549 identified one issue and four sub-issues. Several additional issues were raised by the parties, which I will also consider, as follow:

Issue A: Has the Organization collected, used, or disclosed information about police officers, as described?

Issue B: If the answer is yes, was this information the personal information of these officers? (Personal information is defined in section 1(k) of the Act.)

Issue C: Are the records excluded from the application of PIPA by section 4(3)(k)?

Issue D: Are the records excluded from the application of PIPA by section 4(5)(a) or 4(5)(b)?

Issue E: Was the information collected, used or disclosed in contravention of, or in compliance with, section 7 of the Act? (Section 7 prohibits collection, use or disclosure unless either the Complainant consents in accordance with section 8, or the Organization has authority under sections 14, 17 and 20 to collect use and disclose without consent.)

1. Did the persons whose information is contained in the in the database consent to its collection, use or disclosure?
2. If the Organization is collecting, using or disclosing personal information as defined in PIPA, does it have the authority to do so without consent, as permitted by section 14(e), 17(e) and 20(j) (the information is publicly available)
3. If the Organization is collecting, using or disclosing personal information as defined in PIPA, does it have the authority to do so without consent, as permitted by section 14(d), 17(d) and 20(m) (the collection, use and disclosure is reasonable for the purposes of an investigation or legal proceeding)

Issue F: Was the personal information collected, used or disclosed in accordance with sections 11, 16 and 19 of the Act? (These sections require that collection, use and disclosure be only for purposes that are reasonable, and that it be reasonable for the purpose.)

I will also consider the questions, raised by the Complainant in his submission, of accuracy and security of the information in the database.

III. DISCUSSION OF ISSUES

Issue A: Has the Organization collected, used, or disclosed information about police officers, as described?

[para 11] The information provided by the Organization, set out above, makes it clear that the Organization is collecting, using and disclosing the information relating to EPS members that is contained in the database.

[para 12] I note that while the complaint speaks in terms of the "collection, use and disclosure" of the information of police officers, it focuses on the database. It is not clear, therefore, whether the complaint is meant to embrace the collection, use and disclosure of information relating to police officers for the purposes stated at para 7 above, whether the information is entered into the database or not, or whether the Complainant accepts that such information may be collected, used and disclosed in a contemporaneous time frame by the persons who need it for the stated purposes, but the objection is to entry and retention of this information *in the database*.

[para 13] Entry in a database signifies not only that the information has been collected and may be used and disclosed; it also suggests that there is an intention to retain it, beyond the period in which it is initially and immediately useful, for some future use. As well, the Organization has told me it selectively shares the information with other lawyers; again this signifies not only disclosure, but disclosure for a purpose other than any immediate use of the information by the Organization. Finally, entry in a database is significant in terms of whether it is accessible to persons other than the persons who collected, used or disclosed it initially, which depends upon who has access to the database.

[para 14] To ensure that I have dealt with all of the Complainant's concerns, in this order I will discuss both the collection, use and disclosure of information relating to police officers for the described purposes regardless where the information is stored by the Organization, and I will also consider the significance of entering the same information in the database. To the extent the database is used as a temporary repository of information while the Organization is using it for the immediate purpose, I will not regard the location of such storage as significant (except insofar as it impacts who may access it). However, I will consider the significance of the entry and retention of information in the database insofar as it is intended to create an information resource for future, as yet undetermined, uses, and for other lawyers and their clients, as well as for the Organization.

[para 15] As will be seen below, these last observations are most significant to the potential justification that the information is used and disclosed because it is reasonable for the purpose of a legal proceeding.

Issue B: If the answer is yes, was this information the personal information of these officers? (Personal information is defined in section 1(k) of the Act.)

[para 16] Section 1(k) reads:

> *1 In this Act,*
> *...*
>
> *(k) "personal information" means information about an identifiable individual;*
> *... .*

[para 17] The question of whether information relating to police officers as it is found in the context of the database is their personal information is a complex one. It must be addressed having regard not only to what the database contains, but also to the stated purpose for which it was compiled, as quoted above.

[para 18] Earlier cases have held that the characterization of information can depend on its context, and that the same information that may be personal information as it is found in one context may not be personal information in another context.

[para 19] For example, in Order P2009-009, I held that recorded information about the thoughts and actions of a psychologist relative to a particular person she was treating were not the psychologist's personal information in the context of the treated person's "treatment file", but the same information was the psychologist's personal information when she incorporated it into her response to the College of Psychologists to a complaint the treated person had made to the College about the psychologist.

[para 20] In Order P2007-002, referring to Order F2004-026 (para 109-113), the Adjudicator held that "a record of what a public body employee has done in their professional or official capacities is not personal or about the person, unless that information is evaluative or is otherwise of a 'human resources' nature, or there is some other factor that gives it a personal dimension".

[para 21] Turning to the database, the original e-mail supplied by the Complainant referred to excessive use of force and misconduct in describing the contents. The fuller account of the database given by the Organization is worded more neutrally, and refers to misconduct only in the final clause. However, because the information in the database has been placed there to help with defence work, I assume that most of it is such as might reflect on the officers negatively. Defence work by its nature seeks to undermine the efforts of officers to provide the foundations for the prosecution of offences, and therefore naturally focuses on the aspects of their work performance where they have or

have arguably fallen short. It is quite likely that some or even much of the information would be recorded in critical language, or would involve critical statements – for example, referring to 'misconduct' rather than conduct.

[para 22] Information of the type just described either has already had a negative effect on the officer (in the case of disciplinary or criminal proceedings in which findings were made against the officers) or has the potential to do so if it has the potential to be used in such a proceeding. Such effects are clearly personal to the officer, and information about these effects is the officers' personal information.

[para 23] At the same time, however, information about what officers have, or have allegedly, done in the performance of their work responsibilities is, according to the Organization, placed in the database for the purpose of helping accused persons to defend themselves against offence proceedings. Presumably, therefore, it is such information as could be used to undermine the credibility of a police officer who is giving evidence against the accused, or that describes actions taken by an officer that could otherwise assist in the defence.

[para 24] The actions taken by police officers in performing their work responsibilities are commonly relevant to the prosecution of offences. Police work includes not only investigating offences, but also providing evidence about the results of the investigation, as well as, in some circumstances, creating or influencing the creation of relevant information. It is a routine aspect of the work of police officers that information about actions they take in discharging their duties, both relative to a particular prosecution and relative to earlier cases, will be introduced as evidence in an offence proceeding.

[para 25] There is a strong argument, therefore, that information showing what a police officer did in the course of performing work responsibilities, which is collected, used or disclosed for defending a charge in offence proceedings, is not, in that defence context, in itself information about the officer personally, even though some of it may be or in a sense be evaluative of their work performance. Despite the fact that what is collected or used or introduced into the offence proceeding may reflect on the officer negatively, this fact is in itself irrelevant to the proceeding; the nature of the conduct is important not because it reveals something about the officer, but because it helps to determine how information in the offence proceeding that was in some way associated with the officer's conduct is to be treated in the proceeding. For example, if a police officer fails to establish the continuity of an item of evidence, or it is shown that an officer failed to advise a suspect of their right to counsel or elicited a confession by force, the evidence may not be admissible in the proceeding. Any effect on the officer's personal life from the introduction of information about the officer's conduct into an offence proceeding will be merely incidental to, and beside the point of, introducing it for the purposes of the defence.

[para 26] An analogy to this reasoning may be drawn in any number of working situations. Actions that people take in performing their work will often have different

outcomes depending whether they were done well or badly, or whether they conformed to a defined standard. Thus, for example, a decision made by an adjudicator in this office may be made on the basis of faulty reasoning. If the decision is overturned by a reviewing court on the basis that it was unreasonable, and the associated order does not therefore take effect, it does not follow that the contents of the order become the personal information of the decision-maker.

[para 27] If, in contrast, the information is used in such a way that the person performing the work is him or herself being evaluated, and the action that was taken is judged as having been done well, badly or indifferently for a purpose that is personal to the person (for example, if this is done for a human resources purpose, or has become the subject of a complaint), the very same information may, as already noted, have a personal aspect. There are many orders from other jurisdictions that illustrate this 'dual' approach to the question of whether the information of police officers is or is not their personal information. See, for example, Ontario Order P-721, and other orders citing this order in support of the same principle. In some of these cases, the question that is asked is whether the information reveals something personal about the person.

[para 28] Returning to the database, based on the Organization's description, it contains not only information about what officers did or allegedly did in the course of performing their employment duties. Insofar as the database contains *records or reports of* disciplinary or criminal or civil proceeding against officers and their outcomes, or related information, it also contains information about the consequences to officers that flowed from their actions. The latter, although also work-related, could fairly be said to be the personal information of the officers. However, as just discussed above, information as to how an officer discharged their work duties when it is to be used for the purpose of defending against an offence proceeding is a work-related use of records of their work, and is not personal information of the officer in that context.[1]

[para 29] In my view, the most satisfactory way to characterize information in the database about past proceedings against officers is to say that the same information – as to what the police officer did – has both a non-personal and a personal aspect.

[para 30] The very fact of what the officer did is not their personal information – it is their discharge of their work and of their duties to the public as a member of a public institution. This could be said of any records that reveal nothing other than what was done – for example, a video recording of an incident, or a factual account from an observer.

---

[1] A record of a disciplinary proceeding may be relevant to a defence in its entirety even though it is introduced for the purpose of revealing what a police officer did (which is important in turn to determine what effect the thing done is to have on the outcome of the proceeding). For example, the outcome of a disciplinary proceeding would shed light on what was done insofar as it reveals the conclusions of the person who heard direct evidence about the conduct. Similarly, the nature of the penalty imposed on an officer at the conclusion of a proceeding would reveal the view of the decision-maker as to the strength of the evidence and the egregiousness of the conduct, thereby telling something about the conduct itself.

[para 31] However, if the information that is entered is a record or report of a disciplinary process, it does not come in pure form – it comes associated with personal information as well. Information in the database that reveals what was done by the officer *but that at the same time* reveals something that is personal to the officer – for example, the fact that a disciplinary proceeding was conducted and that particular conclusions were drawn, or that a penalty was imposed (which might speak to the conduct itself insofar as it shows how egregious the person who heard direct evidence saw it to be), has both non-personal and personal aspects which are inextricably interwoven. Since the personal information revealing what was done cannot be separated from the pure fact of what was done, such information must be regarded in totality as having a dual – non-personal as well as personal – character.[2] A similar duality might exist in relation to an entry that both records what was done or allegedly done by an officer, and that has a personal aspect for some other reason, for example, that it was highly publicized.

[para 32] I turn next to the information in the database that is placed there to be used for "other litigation or law enforcement purposes". The respondent Organization has not positively asserted that such information has been placed in the database for the purpose of taking actions against individual police officers. Indeed, insofar as the database is meant to be a repository for information that may become useful in future, it is not clear to me that information that is relevant to the imminent initiation and pursuit of an action against an officer by the law firm or one of its clients would necessarily be placed in the database *for that purpose*. Nonetheless, there is a possibility that this is among the "other" purposes of which it has spoken in the more general terms just quoted. As well, it may, possibly, also be placed in the database for future, as yet unknown, actions against officers. While acknowledging that these possibilities are somewhat speculative, I will comment on them here for the sake of efficiency (though if they are not borne out in fact, the related conclusions can be discounted).

[para 33] As already discussed above, in my view, a disciplinary, civil or criminal proceeding taken against an officer is personal to them even though it relates to their employment and may, in the case of a disciplinary matter, also be conducted in their

---

[2] This analysis is somewhat similar to a distinction that has been drawn between, on the one hand, allegations or evidence as to what was done by the officer, and on the other, the conclusions or comments of investigators or decision maker about was done and evaluations or consequences flowing therefrom. For example, in Ontario order MO-2025, the adjudicator suggested that factual information given by an individual describing how they carried out professional or employment duties was not personal information of the person, while evaluative comments about the quality or propriety of that conduct by the investigator were personal information. In my view, such distinctions may be impractical because there are no firm lines between them. For example, a statement by a witness that an officer used excessive force is both factual and evaluative. Furthermore, I reject the idea that the fact a person did something badly (or well) is their personal information, but what the thing that was done consisted of is not. Again, the two may be impossible to separate. In my view, where what was done is inseparable from the associated personal information, it must be characterized in its totality, as having a dual aspect.

I note as well, in relation to the reasoning in MO-2025, that whether an evaluation or comment is personal to the person also depends on the context. Thus, an evaluation of work may be done to make work-related decisions, in which case it may not be personal any more than the original work was.

working sphere. Thus any information in the database as to how police officers fulfilled their employment responsibilities that is entered for the purpose of initiating or pursuing such an action is, in my view, information about the officer and is their personal information. (Again, insofar as it is records their performance of their work, it also has a non-personal aspect.)

[para 34] In view of the foregoing considerations, I cannot, by reference only to the description provided by the respondent Organization of the contents of the database, characterize it in its entirety as either personal or not. In my view, based on the foregoing discussion as well as earlier decisions that deal with information of a dual character, I find that the information in the database that reveals only what the officers did in discharging their employment roles is not their personal information in the context of its entry in the database for the purpose of defence proceedings. Information that reveals what was done but at the same time, inextricable from the former, reveals something that is personal to the officer, has a dual character of both personal and non-personal information. Any information entered into the database as part of the process of advancing legal proceedings against the officers themselves on the basis of their conduct, or is entered as a resource for any such future proceedings, is their personal information. In my view, police officers' registration numbers (which were specifically raised by the Complainant as constituting personal information) are also personal or otherwise depending on the context in which they appear, as discussed above.

[para 35] The information that I have discussed above that is not, in my view, personal information, is not subject to the Act – which governs the collection, use and disclosure of personal information only. Therefore, I can make no findings relative to it. However, as I have just explained, some of the information in the database is personal information of police officers, and some of it has both a personal and non-personal aspect. For the latter types of information, I must decide how the provisions in the Act governing the collection use and disclosure of personal information apply in this case. The discussion that follows applies only to any information in the database falling into categories that I have categorized as personal information of officers. It is important to remember, for the purposes of the remainder of the discussion, that it may be the case that most of the information in the database that I would find to be personal or have a personal aspect is also information that is contained in records of disciplinary, criminal or civil proceedings against officers. As such, much of this information would fall into the categories of information in court records, or publicly-available information. This would make the collection, use and disclosure of the information either outside the scope of the Act by reference to section 4(3)(k) in the former case, or authorized by sections 14(e), 17(e) or 20(j) in the latter. Possibly, therefore, the remainder of the discussion relates, as a practical matter, to only a relatively small proportion of the information in the database

C) Are the records excluded from the application of PIPA by section 4(3)(k)?

[para 36] Section 4(3)(k) reads:

> *4(3) This Act does not apply to the following:*

> *(k) personal information contained in a court file, a record of a judge of the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta or The Provincial Court of Alberta, a record of a master in chambers of the Court of Queen's Bench of Alberta, a record of a sitting justice of the peace or a presiding justice of the peace under the Justice of the Peace Act, a judicial administration record or a record relating to support services provided to the judges of any of the courts referred to in this clause;*

[para 37] Section 4(3)(k) excludes "personal information contained in a court file" from the application of PIPA.

[para 38] In *Alberta (Attorney General)* v. *Krushell,* 2003 ABQB 252, the Court addressed a similar provision, section 4(1)(a) of the *Freedom of Information and Protection of Privacy Act.* The Court held that information in criminal dockets fell within section 4(1)(a) because this information originated from court files. Justice Bielby stated:

> … the mere fact it is extracted from those files and appears in a different format does not change the purpose of the legislation, which is to exclude the information contained in those materials from the ambit of the Act. The purpose of the Legislature was to exclude the information, not merely the paper format in which some of it originally appears. Whether it is contained in a physical paper file, or is removed from that file to another format it is excluded from production under the Act.

[para 39] Orders F2004-030 and F2007-021 held that records in the possession of a public body, the content of which match records in a court file, do not fall within section 4(1)(a) of the FOIP Act unless the information has been taken or copied from the court file.

[para 40] In my opinion, given the foregoing, section 4(3)(k) excludes the personal information in the database that is found in or consists of a copy of court transcript or a court decision which is found in a court file, or of any other information in the database of which court files are the source. Therefore, I may make no finding relative to any of the personal information in the database that falls into this category.

D) Are the records excluded from the application of PIPA by section 4(5)(a) or 4(5)(b)?

[para 41] Sections 4(1), 4(5)(a) and 4(5)(b) read:

> *4(1) Except as provided in this Act and subject to the regulations, this Act applies to every organization and in respect of all personal information.*
>
> *4(5) This Act is not to be applied so as to*
>
> *(a) affect any legal privilege,*
>
> *(b) limit the information available by law to a party to a legal proceeding, or*

(c) limit or affect the collection, use or disclosure of information that is the subject of trust conditions or undertakings to which a lawyer is subject.

Section 4(5)(a)

[para 42] Section 4(5)(a) states that PIPA should not be applied "so as to affect any legal privilege". It seems possible that this provision would bear on the question of whether information subject to legal privilege is to be provided on an access request. However, I do not see how, at least in the present case, it bears on the matter of a complaint that information (even if subject to legal privilege) has been collected, used or disclosed contrary to the terms of the Act. Though the Act permits collection use and disclosure of information that is reasonable for an investigation or legal proceeding, some of which may be privileged, none of the provisions of the Act explicitly or implicitly speak to whether personal information that is subject to legal privilege can be collected, used or disclosed.[3] As well, a finding could be made as to whether a complaint (regarding the collection use or disclosure of privileged information) is borne out without contravening the privilege or affecting the privileged status of the information.

Section 4(5)(b)

[para 43] Section 4(5)(b) states that PIPA is not to be applied so as to "limit the information available by law to a party to a legal proceeding."

[para 44] One interpretation of the provision is that it is meant to clarify the relationship between the exceptions to access that are found in provisions in the Act that create entitlements to access, and the existence of mechanisms in court and tribunal processes whereby litigants may obtain and provide information in court and legal proceedings. In other words, the provision is meant to clarify that the statutory exceptions which preclude access to information under access to information legislation have no bearing on the availability of information for court and tribunal proceedings via the mechanisms that exist relative to those proceedings. Under this interpretation "available by law" is taken to refer to other legal processes by which litigants may gain access to information for introduction into legal proceedings. The great majority of cases which have considered provisions such as section 4(5)(b) have considered their application in the context of requests for access. In these cases, courts or tribunals have commented that the effect of the provision is that though information may be unavailable on an access request because it falls within one of the statutory exceptions, this has no bearing on whether the information is available by the processes by which litigants, courts or tribunals gain access to information for the purposes of court or tribunal proceedings.

[para 45] It is an open and largely novel question, therefore, whether section 4(5)(b) is also meant to have the effect that provisions that control the collection, use and disclosure of information by organizations are not to be applied if applying them would mean that someone who wishes to introduce information into a court or tribunal proceeding would be prevented from collecting, using or disclosing the very information that they need in the proceeding. If section 4(5)(b) is to be interpreted in this way, it is

[3] Section 38.1 speaks to legal privilege, but relates only to disclosures of information to the Commissioner.

also necessary to ask what "available by law" is meant to convey in the context of such an interpretation. Possibly, section 4(5)(b) is to be read as affirming the ability to collect, use and disclose information, but only such information as was available to the party by the operation of a law or a legal process.[4] Alternatively, given that information that is relevant to a legal proceeding may be admitted and considered by a court or tribunal, disallowing such information to be entered into the database, or to be used or disclosed for the purposes for which it was collected, could be said to entail limiting the information "available by law (including the common law that allows the reception by courts of relevant evidence) to a party to a legal proceeding".[5]

[para 46] It is not necessary for me to decide which of these interpretations is correct, however. This is because the interaction between the collection, use and disclosure of information, and the need to have information for use in investigations and legal proceedings available, is specifically addressed in sections 14(d), 17(d) and 20 (m) of the Act. I will consider these sections further under Issue E3, below.

E) Was the information collected, used or disclosed in contravention of, or in compliance with, section 7 of the Act? (Section 7 prohibits collection, use or disclosure of personal information unless either the Complainant consents in accordance with section 8, or the Organization has authority under sections 14, 17 or 20 to collect use and disclose without consent. It also prohibits collection from a source other than an individual unless the individual consents.)

[para 47] Section 7 reads:

> *7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,*
>
> > *(a) collect that information unless the individual consents to the collection of that information,*
> >
> > *(b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source[6],*

[4] Examples would be information that is to be provided to a party before a criminal trial according to the rules for advance disclosure of prosecution evidence, or that becomes the subject of a court or tribunal order for production, or that is in the possession of a witness who has been given notice to attend a proceeding to give testimony. On this interpretation, section 4(5)(b) would not apply, for example, to anecdotal information on the database concerning a police officer that the defence would wish to introduce into a criminal trial where the source of that information is not via any legal requirement or legal channel.

[5] In Order H2004-005, the Commissioner considered a somewhat similar provision under the *Health Information Act* which provides that the Act does not limit the information otherwise available by law to a party to legal proceedings. In discussing this provision, the Commissioner appeared to conclude that "available by law" embraced the idea of information available by reference to the common law as well as statutory law. However, it does not follow from this that "*available by* law" covers information, even though intended to be introduced into a legal proceeding, that is provided voluntarily rather than through some compulsory mechanism for obtaining evidence.

[6] Section 12 contains an exception to this limitation.

(c) use that information unless the individual consents to the use of that information, or

(d) disclose that information unless the individual consents to the disclosure of that information.

(2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

(3) An individual may give consent subject to any reasonable terms, conditions or qualifications established, set, approved by or otherwise acceptable to the individual.

1. If the Organization is collecting, using or disclosing personal information as defined in PIPA, did the persons whose information is contained in the database consent to its collection, use or disclosure?

[para 48] There is no information or evidence in this inquiry to suggest that the individual police officers whose personal information has been included in the database have consented to the collection, use or disclosure of their personal information by the Organization.

2. If the Organization is collecting, using or disclosing personal information as defined in PIPA, does it have the authority to do so without consent, as permitted by section 14(e), 17(e) and 20(j) (the information is publicly available)

[para 49] Sections 14(e), 17(e) and 20(j) permit an organization to collect, use and disclose personal information without consent if the information is publicly available. These sections read:

14 An organization may collect personal information about an individual without the consent of that individual but only if one or more of the following are applicable:

…

(e) the information is publicly available; … .

17 An organization may use personal information about an individual without the consent of the individual but only if one or more of the following are applicable:

…

(e) the information is publicly available; … .

20 An organization may disclose personal information about an individual without the consent of the individual but only if one ore more of the following are applicable:

…

(j) the information is publicly available … .

[para 50] Section 7(d) and 7(e) of the PIPA regulations define the term "publicly available" as including a record of a quasi-judicial body, or information contained in a publication. These sections read:

> *7 For the purposes of sections 14(e), 17(e) and 20(j) of the Act, personal information does not come within the meaning of "the information is publicly available" except in the following circumstances:*
>
> *...*
>
> *(d) the personal information is contained in a record of a quasi-judicial body but only if*
>
> *(i) the record is available to the public, and*
>
> *(ii) the collection, use or disclosure of the information relates directly to the purpose for which the information appears in the record;*
>
> *(e) the personal information is contained in a publication, including, but not limited to, a magazine, book or newspaper, whether in printed or electronic form, but only if*
>
> *(i) the publication is available to the public, and*
>
> *(ii) it is reasonable to assume that the individual that the information is about provided that information;... .*

1) Record of a quasi-judicial body

[para 51] There are three criteria under section 7(d):

> (a) the personal information must be contained in a record of a "quasi-judicial body",
> (b) the record must be available to the public, and
> (c) the collection, use or disclosure must relate directly to the purpose for which the information appears in the record.

a) Quasi-judicial body

[para 52] In Order 99-025, the Commissioner addressed section 4(1)(b) of the FOIP Act. He held that in order to determine whether an entity is acting in a judicial or "quasi-judicial capacity", the following non-exhaustive list of factors should be weighed and evaluated:

> i) Is there anything in the language in which the function is conferred or in the general context in which it is exercised which suggests that a hearing is contemplated before a decision is reached?
>
> ii) Does the decision or order directly or indirectly affect the rights and obligations of persons?
>
> iii) Is the adversary process involved?

iv) Is there an obligation to apply substantive rules to many individual cases rather than, for example, the obligation to implement social or economic policy in a broad sense?

[para 53] The Organization states that it collects electronic copies of, or provides internet links to, the decisions of the designated officers and decisions of the Law Enforcement Review Board (LERB) under the *Police Act*. It appears that both the LERB and designated officers act in a quasi-judicial capacity, as demonstrated by the following:

i) the LERB and the designated officers are given the power to conduct hearings (sections 20(1), 45(2) and 45(3) of the *Police Act*),

ii) the hearings directly affect the rights and obligations of persons,

iii) these bodies apply substantive rules to many individual cases, and

iv) the hearings involve an adversarial process under which witnesses can be compelled to testify (sections 20(1)(c) and 45(3) of the *Police Act*).

b) Available to the public

[para 54] I take notice of the fact that decisions of the LERB since 2002 are posted on the website of the Board. As well, decisions of disciplinary hearings under the *Police Act* since 2007 are posted on the website of the EPS (although I note that is not the case for decisions relating to the members of the Calgary Police Service).

c) The collection, use and disclosure relates directly to the purpose for which the information appears in the record

[para 55] In my view, decisions under the *Police Act* are published (and appear in the "record") in order to provide transparency and openness to the proceedings. As the individual officers are named on the websites referred to, it is also to make the public aware of cases in which individual officers have been found to have engaged in, or have been cleared of, misconduct. The latter purpose, in my view, embraces the purpose of permitting persons who have been charged with offences to use any relevant information from the proceedings in defending against the charges, as well as (with the exception discussed in the next paragraph) for the purpose of bringing actions or instituting proceedings against police officers.

[para 56] The *Police Act* contains an exception to the information that may be used in the latter of the ways just described, and, therefore, the purpose for the publication of the information does not extend to this exception. Section 51 of the *Police Act* states that if a police officer provides evidence during a hearing or appeal under the *Police Act*, that evidence or a voluntary explanatory report shall not be used or received against the police officer in any civil proceedings or in any proceeding under any other Act, except in the

prosecution for or proceedings regarding perjury or the giving of contradictory evidence.[7] Thus, with respect to the evidence of the police officer that is the subject of a disciplinary charge, the purpose of disclosing the information given by the officer arguably cannot be that of using the information to pursue or further pursue actions, whether civil, criminal or disciplinary, against the officers who were the subject of the disciplinary proceedings. (While it is not clear if information derived from such information could be so used, and as well, the same information might be usable by the defence for the purpose of assisting with further investigations into the conduct of the officer, it is arguable that section 51 is to be taken as an indicator that the *publication* of any such information provided by a police officer is not intended to be used against a police officer in any way.)

[para 57] Because the Organization in this case is located in Edmonton, it seems probable that a considerable portion of the information in the database will fall within the terms of section 7(d) of the regulation. However, the exception will not cover disciplinary decisions from other police forces that do not have a similar publication policy. As well, it will not cover any decisions in the database relating to discipline of the local police force that are not published.

2) Personal information contained in a publication

[para 58] In order to fulfill section 7(e) of the PIPA regulations, three criteria must be fulfilled:

> a) the personal information must be contained in a publication;
> b) the publication must be available to the public; and
> c) it is reasonable to assume that the individual that the information is about provided the information.

[para 59] The Organization states that it collects newspaper articles and letters to the editor. In my view, it is probable that some of these newspaper articles and letters to the editor would fulfill these three criteria.

---

[7] Section 51 provides:

> *51 Where a police officer or peace officer appointed under the Peace Officer Act give evidence during*
>
> *(a) a hearing under this Act, or*
>
> *(b) an appeal under this Act arising out of a hearing referred to in clause (a),*
>
> *that evidence, or an explanatory report made to an investigator on a voluntary basis by a police officer in respect of whom an investigation is being carried out if it tends to incriminate him or her, subject him or her to punishment or establish his or her liability, shall not be used or received against the police officer or peace officer appointed under the Peace Officer Act in any civil proceeding or in any proceeding under any other Act, except in a prosecution for or proceedings in respect of perjury or the giving of contradictory evidence.*

[para 60] Newspaper articles and letters are generally contained in a publication that is available to the public, and thus the first two criteria would likely be fulfilled for this category of information in the database. However, the third criterion – that the information be about the individual who provided it – would be met with respect to only some of the articles and letters. If it is clear from or could clearly be inferred from the content of the article or letter that the individual police officer provided the information, section 7(e) of the PIPA regulations would be fulfilled. However, it seems probable that there would be many instances of articles containing personal information relating to police officers' conduct in which the information in the article or letter was not, or was not all, provided by the individual officer. In such a case, section 7(e) would not apply to such information. In order to determine whether section 7(e) applies, each article or letter to the editor would have to be reviewed individually.

3. If the Organization is collecting, using or disclosing personal information as defined in PIPA, does it have the authority to do so without consent, as permitted by section 14(d), 17(d) and 20(m) (the collection, use and disclosure is reasonable for the purposes of an investigation or legal proceeding)

[para 61] Sections 14(d), 17(d) and 20(m) permit an organization to collect, use and disclose personal information without consent if the collection, use and disclosure is reasonable for an investigation or legal proceeding. These sections read:

> *14 An organization may collect personal information about an individual without the consent of that individual but only if one or more of the following are applicable:*
> *...*
> *(d) the collection of information is reasonable for the purposes of an investigation or a legal proceeding; ... .*
>
> *17 An organization may use personal information about an individual without the consent of the individual but only if one or more of the following are applicable:*
> *...*
> *(d) the use of the information is reasonable for the purposes of an investigation or a legal proceeding; ... .*
>
> *20 An organization may disclose personal information about an individual without the consent of the individual but only if one or more of the following are applicable:*
> *...*
> *(m) the disclosure of the information is reasonable for the purposes of an investigation or a legal proceeding; ... .*

[para 62] The term "investigation" is defined in section 1(f) of PIPA as follows:

> *1 In this Act*
>
> *,...*
>
> *(f) "investigation" means an investigation related to*
>
> *(i) a breach of agreement,*

(ii) a contravention of an enactment of Alberta or Canada or of another province of Canada, or

(iii) circumstances or conduct that may result in a remedy or relief being available at law,

if the breach, contravention, circumstances or conduct in question has or may have occurred or is likely to occur and it is reasonable to conduct an investigation; ….

[para 63] The term "legal proceeding" is defined in section 1(g) of PIPA:

1 In this Act,

…

(g) "legal proceeding" means a civil, criminal or administrative proceeding that is related to

(i) a breach of an agreement,

(ii) a contravention of an enactment of Alberta or Canada or of another province of Canada, or

(iii) a remedy available at law; … .

[para 64] It is unquestionably the case, in my view, that if a legal proceeding has been initiated or a particular proceeding is reasonably anticipated, and the Organization or another law firm acting on behalf of a client requires information such as that in the database for the purpose of participating in the proceeding, for example, for helping a client to defend a charge, or for use as a starting point for further investigation for the purposes of such a defence, sections 14(d), 17(d) and 20(m) permit the collection, use and disclosure of relevant personal information where this is done at the time the charge had already been laid or was reasonably anticipated. (I take collection, use or disclosure of information that is useful in the sense of being relevant to an investigation or legal proceeding, insofar as each of these actions is reasonably required for the investigation or legal proceeding, to also be "reasonable for the purpose" within the terms of these provisions.)

[para 65] With respect to disclosure, it is not, in my view, necessary that the disclosure contemplated in section 20(m) be done by or on behalf of the person defending a charge or instituting the proceeding; the disclosure can also be done by an organization to such a person. It would, therefore, permit such disclosure of information in the database by the Organization to another person or law firm who was contemplating or initiating the legal proceeding. I reach this conclusion on the basis that the Act contains no express limitation, in contrast to a similar provision in the FOIP Act which permits disclosures by public bodies for use in legal proceedings, but only proceedings to which the Government of Alberta or the public body who is doing the disclosing is a party. As well, I note that in Order H2004-005, already discussed above, a provision of the *Health Information Act* permitting disclosure "for the purpose of a court proceeding" was held to permit disclosure by a custodian to a party in the proceeding where the custodian was herself not a party.

[para 66] As well, it seems clear to me that the provisions would also apply to information that is collected, used or disclosed by a law firm acting on behalf of a client for the purpose of deciding whether to initiate a legal proceeding against a police officer (which is, arguably, a type of "investigation") and for initiating the proceeding.

[para 67] However, a key question in the present case is whether the provision is applicable to information in the database (assuming there to be such) which was collected, used or disclosed at a time at which no investigation or legal proceeding had yet begun, or at a time at which it was not known whether a future investigation or legal proceeding would ever begin. A related question is whether information that was used for an existing proceeding can be retained in the database for future use in as yet unknown proceedings after a first proceeding has been concluded.

[para 68] I discussed a similar question in a different context in Order P2008-008[8], as follows:

> **55** I begin by asking whether the provision is to be read restrictively such that it is triggered only when an actual investigation is underway, or when steps have already been taken to initiate a legal proceeding, and the collection of information begins thereafter. Two broader interpretations are possible: one is that the provision may also apply where a particular investigation or legal proceeding relative to certain facts is contemplated or likely, but has not yet begun; the final and broadest interpretation is that the provision may apply where there is merely a possibility that there will be an investigation or legal proceeding, depending on whether or not facts that would give rise to either of these occur in future.
>
> **56** I reject the first, restrictive, interpretation as too narrow. The provision uses the phrase "reasonable for the purposes". It seems reasonable that if an investigation or legal proceeding is reasonably expected because certain facts have happened or may have happened, evidence may be collected, used or disclosed for its purposes even though the investigation or legal proceeding has not technically begun.[4] Thus, in my view, as long as it is reasonable to do so, collection of information may be done for the purposes of an investigation or legal proceeding that relates to particular, existing facts (known or otherwise), though the investigation or legal proceeding has not yet commenced. This conclusion is in accord with the decision of Hart, J. in *Canada Safeway Ltd. v. Shineton*, [2007] A.J. No. 1477, at paras 60 and 61 (a decision reviewing Order P2005-004), in which the court held that section 20(m) covers the provision of information to an investigator for the purposes of initiating an investigation. Thus I accept that the provision may apply in the circumstances described under the first of the broader interpretations.
>
> **57** The situation is different where the investigation or proceeding will take place only if certain facts happen which have not yet happened and may not happen. I note that the provision itself has no temporal restriction, but arguably "an investigation or legal proceeding" refers to an existing or pending proceeding rather than one that is conditional on particular facts happening that may never come to pass.
>
> **58** In this regard, I find some assistance in the definition of the term "investigation" that is found in section 1(f). This section provides:

[8] This order dealt with video recordings of a picket line made by a union during a strike. An application for judicial review has been brought for this order.

> *1 In this Act,...*
>
> > *(f) "investigation" means an investigation related to*
> >
> > > *(i) a breach of agreement,*
> > >
> > > *(ii) a contravention of an enactment of Alberta or Canada or of another province of Canada, or*
> > >
> > > *(iii) circumstances or conduct that may result in a remedy or relief being available at law,*
> >
> > *if the breach, contravention, circumstances or conduct in question has or may have occurred* ***or is likely to occur*** *and it is reasonable to conduct an investigation; ...* [emphasis added]

Under this definition, an investigation may relate to circumstances or conduct that "is likely to occur". Thus section 14(d) permits information to be collected where it is reasonable to do so for the purposes of an investigation that is into circumstances or conduct that have not occurred but are likely to occur. On the theory that a parallel degree of uncertainty is permissible for the "legal proceeding" condition, information can also be collected before the fact where that information will be relevant to a legal proceeding, should it occur, that is likely to occur because the facts or circumstances grounding such a proceeding are likely to happen.

59 I accept the broadest of the possible interpretations of the provision. In my view the inclusion of the phrase "reasonable for the purpose" takes the place of any temporal restriction, allowing information to be collected in the appropriate circumstances even though an investigation or legal proceeding may never take place in fact. It strikes me as prudent and therefore reasonable to collect information which could avoid contests, in the context of an investigation or legal proceeding that is reasonably likely to arise over contentious facts which would be hard to establish through witness testimony. As there was a reasonable likelihood of incidents on the picket line that could lead to a police investigation and law enforcement proceedings, and as a Labour Relations Board or court proceeding relative to the conduct of the picketing was reasonably forseeable, an investigation or legal proceeding was reasonably likely to arise in the circumstances of the present case.

[para 69] I adopt this reasoning for the present case.

[para 70] I will deal first with the application of this provision to information in the database that has been placed there for the purpose of using it in the defence of charges. According to my analysis under Issue B, it is likely that at least some of the information in the database is not the personal information of police officers, and hence this discussion does not apply to that part of the information. However, it does apply to any information in the database falling into categories that I have categorized as the personal information of officers (and that does not meet the terms of section 4(3)(k) (information in a court record) or sections 14(e), 17(e) and 20(j) (publicly available information).

[para 71] I find (as already stated at para 64) that collection, use or disclosure of personal information that is reasonable for the purpose of defending a charge, where this is done at the time the charge had already been laid or was reasonably anticipated, is authorized by sections 14(d), 17(d) and 20(m).

[para 72] However, given the description of the database that the respondent Organization provided, it seems likely that the database contains information about past events which have the potential to be used in the course of defending against a charge, but at the time of its entry into the database, the charge has neither been laid, nor is any particular charge, relative to any particular defendant, then anticipated. In other words, it seems probable that there is information relative to particular officers that was placed there as a general resource, unconnected to any particular client file and unrelated to an existing or pending proceeding, but is included for use in the event that the officer who is the subject of the information becomes involved in a future case. For such information, its relevance to a legal proceeding would depend on the happening of future events.

[para 73] Based on my conclusions in Order P2008-008, I must ask whether, for any such item of information, there is a reasonable likelihood that a legal proceeding will arise relative to which such information will be relevant because the facts or circumstances grounding such a proceeding are likely to happen.

[para 74] To answer this question, I return to my earlier comments about the work of police officers. As I noted above, the actions taken by police officers in performing their work responsibilities are commonly relevant to the prosecution of offences as well as to their defence. Police work includes not only investigating offences, but also providing evidence about the results of the investigation, as well as, in some circumstances, creating or influencing the creation of relevant information. It is a routine aspect of the work of police officers that information about actions they take in discharging their duties, both relative to a particular prosecution and relative to earlier cases, will be introduced as evidence.

[para 75] Thus, in my view, if information as to the manner in which a particular police officer has carried out their work exists in the database, it is highly likely that as a matter of course, that information will become relevant to future cases in which they are involved. I do not rule out the possibility that there could be exceptional items of information – for example, such as are unlikely to have any relevance to future events because they arose in highly unique circumstances, or when the information is relative to a particular officer or former officer relative to whom there is no possibility that they may be involved or give evidence in future cases. However, I believe that in the normal course, the happening of future events relative to which offence proceedings would arise, to which such information would be relevant, would be very likely. Similar to what I said in Order P2008-008, it strikes me as not only permissible but prudent to collect relevant information (and to use and disclose it for the same purpose) to provide the basis on which courts can make findings as to credibility, and related issues relating to police conduct, in the future prosecution and defence of charges.

[para 76] Based on these conclusions, I find that the collection, use and disclosure of personal information relating to police officers' discharge of their duties, that would be relevant in defences against future legal proceedings that are likely to arise because it is likely the officer will become involved in offence proceedings in the future, is

"reasonable for the purpose" of these future proceedings, and falls within the terms of sections 14(d), 17(d) and 20(m). Therefore, as long as this eventuality continues to be reasonably likely, it is, in my view, permissible for the Organization to collect the personal information and to enter it into the database, to use and disclose it as required, as well as to disclose it to other individuals or law firms who reasonably require it for the purpose of defending against offence proceedings.

[para 77] I am strengthened in this view by cases discussing the rights of individuals under section 7 of the Charter to make a full and fair defence to charges against them (see for example *R.* v. *McNeil*, [2009] S.C.J. No. 3). While by reference to the *Administrative Procedures and Jurisdiction Act,* R.S.A. 2000, c.A-3, I do not have the power to make decisions on constitutional questions, my interpretation of PIPA should follow Charter principles.[9] In my view, interpreting sections 14(d), 17(d) and 20 (m) to permit collection, use and disclosure of personal information that is reasonably likely to be relevant to the defence in offence proceedings that are likely to arise in future, in the sense described in the preceding paragraph, best accords with the importance accorded by the Charter, as interpreted by the courts, to the right to make full answer and defence.

[para 78] It does not follow from this conclusion that every item in the database that is personal information about police officers' work performance is information that would be relevant in future legal proceedings that are likely to arise. The provisions cover only such information as reasonably falls into this category. Collection, use and disclosure of personal information of police officers is justifiable by reference to this provision only to the extent this is so. The Organization must make serious and careful judgments in making entries into the database to ensure that only personal information falling into this category is entered and not non-credible allegations or other frivolous material that an impartial person would not judge as reasonably relevant for use in a defence against a future offence proceeding.[10] (Whether any given item of personal information is potentially relevant to a defence or an action against an officer can only be assessed on a case-by-case basis. As I will explain in the final portion of this order, the Organization must itself insure that the principles discussed in this order are met for all the entries.)

[para 79] I note that some of the information in the database may not be such as would necessarily be introduced as evidence for the purpose of a defence in an offence proceeding, but rather may only be such information as provides the starting point for an investigation to determine whether such further information exists. A hypothetical

---

[9] This means that if a provision is equally capable of different interpretations, the decision maker must choose the interpretation that best accords with constitutional norms. See *R .v. Zundel,* [1992] 2 SCR 731 at 771:

> *…where a legislative provision, on a reasonable interpretation of its history and on the plain reading of its text, is subject to two equally persuasive interpretations, the Court [and in this case this tribunal] should adopt that interpretation which accords with the Charter and the values to which it gives expression.*

[10] I emphasize again that this discussion is limited only to information that is both personal to the officer (as discussed earlier at paras 28 to 31) and that falls neither into the 'court record' nor 'publicly available' categories.

example might be a reasonably credible allegation by someone that a police officer had used excessive force in arresting him (which might at the outset, depending on the circumstances and without more, not be substantiated to a sufficient degree that it would necessarily be accepted by a court). The existence of this information in the database might be the trigger for a further investigation that discovers further and conclusive evidence. (Conversely, it might prove to be false, and lead nowhere.)

[para 80] I do not believe that it would be appropriate to impose a standard for the collection, use and disclosure of such information that it can be shown to be relevant to a defence in the sense of being relevant and admissible evidence in the offence proceeding itself. This is because setting the bar that high would mean that useful starting points or leads for an investigation which could uncover such relevant and admissible information might thereby be made unavailable. I believe that any item of information that raises a reasonable possibility that further such evidence could be found is "reasonable for the purposes of an investigation". In saying this I am implicitly accepting that the work of a lawyer in representing a client can include not only assembling evidence provided by the client and presenting it to the court, but also looking or helping look for additional evidence to support the client's case. Support for the view that such information is relevant to a defence is found in the McNeil case cited above, at para 45. Speaking of the types of evidence that are relevant for disclosure purposes, the Court said:

> As we have seen, likely relevance for disclosure purposes has a wide and generous connotation and includes information in respect of which there is a reasonable possibility that it may assist the accused in the exercise of the right to make full answer and defence. In considering the ambit of the information that can assist in the trial, regard must be given to the particular issues in the case and to the governing rules of evidence and procedure. This does not mean that only material that would be admissible at trial should be produced. Material that would not, on its own, be admissible may nonetheless be of use to the defence, for example, in cross-examining a witness on matters of credibility or in pursuing other avenues of investigation.[11]

[11] I have noted the discussion in the McNeil case as to police conduct-related information that is to be disclosed by the police to the Crown for the purposes of meeting the Crown's first party disclosure obligations, and decisions of Alberta courts interpreting and applying this case, some of which have rejected arguments that certain types of information, such as expunged records or allegations of misconduct that are dismissed, fall within the first party rule. What must be produced to an accused by the Crown and by the police through the Crown is not the same question as what information relating to police officers, assuming it to be already available to the Organization from some source, may be retained, used and shared by it. The question in the present discussion is what conduct-related personal information of police officers might reasonably be collected, used or disclosed for the purposes of an investigation or legal proceeding. The comments from McNeil that are significant for this order in my view are as to the type of information the Court regarded as likely relevant for assisting in a defence (which the Court said had a "wide and generous" connotation, and which included information useful as a starting point for investigation). Some of the reasons given by the Alberta courts for rejecting the application of the first party rule to certain categories of conduct-related information take into account additional factors beyond that of whether the information could be useful to the defence. I do not believe these criteria come into play in determining what information is useful as relevant, and hence reasonable for the Organization to collect, use or disclose or to enter and retain in its database, for the purposes of an investigation or legal proceeding.

[para 81] As well, I note that in contrast to the FOIP Act, which permits disclosures of personal information for the purpose of investigations by police, PIPA contains no restrictions as to who, within the terms of the Act, is to conduct investigations. This is also implicit in the fact that investigations in PIPA are not restricted to law enforcement, but may also be in relation to other types of legal proceedings, including civil proceedings. Thus, lawyers may conduct investigations within the terms of the Act, or assist their clients in doing so.

[para 82] Again, however, it does not follow that any and all anecdotal information or information, even that unlikely to be substantiated, will meet the criterion of reasonable for the purpose; the information must be such that its potential use for the purpose is understandable.

[para 83] I turn to the information in the database that is placed there to be used for "other litigation or law enforcement purposes". As noted earlier at para 32, the Organization has not positively asserted that such information has been placed in the database for the purpose of taking actions against individual police officers. However, for the sake of efficiency, I will comment on the application of the Act to this possibility.

[para 84] I have noted the argument of the complainant that sections 14(d), 17(d) and 20(m) cannot be relied on by the Organization in this situation because there is a legal process for dealing with police misconduct, and it is up to the police to investigate and prosecute officers who may have engaged in misconduct. However, the disciplinary process in question, by its own terms, can be initiated by way of a complaint. Thus there is a role in this process for private citizens, who may engage the services of a law firm to advise them as to whether, and how, to initiate the police disciplinary process and to marshal relevant evidence for their complaint.

[para 85] I note as well that potentially, it could be the law firm itself that brings a complaint, or it may be an individual who is a member of the law firm, in which case it may be unclear whether that person is acting in his or her personal or their professional capacity. Again, the law firm could be acting on behalf of one of its members. I do not regard these distinctions as material, as I believe it is open to both an individual and an organization to initiate the police disciplinary complaint process.[12]

[para 86] I have concluded above that information relating to police officers in the context of disciplinary proceedings or the prosecution of charges against them is the personal information of the officers, and there has been no suggestion that any of the officers have given consent. Thus, in my view, in order for the Organizations' collection, use and disclosure of information for this purpose to conform with the Act (unless the information falls into the 'court records' or 'publicly available' categories) authority must be found in sections 14(d), 17(d) and 20(m).

[12] The *Police Act* permits "persons" to bring complaints, as distinct from "individuals". As a law firm is a "person" under the law, it appears that it may bring a complaint.

[para 87] Sections 14(d), 17(d) and 20(m) speak of "an investigation or legal proceeding". Civil and criminal actions against police officers are legal proceedings. As well, former orders of this office have held that professional disciplinary proceedings are legal proceedings within the terms of the Act. In my view, if a lawyer or law firm, whether acting on behalf of a client or member, or on their own behalf, in trying to determine whether such a proceeding should be initiated, or is taking steps to initiate it, whether by bringing a civil action or by bringing a complaint in the police disciplinary process, these provisions permit the collection, use and disclosure of personal information of the officer by the lawyer or law firm that is reasonable for this purpose, and would accordingly permit entry and retention in the database for the period in which the decision is being made and the action is being pursued, to the extent this is reasonable for this purpose. (In this context, I am contemplating that the database is being used for temporary storage of information, in contrast to the creation of a resource for future potential actions against officers.) As well, as already discussed, section 20 would permit disclosure of such information from the database to some other person or law firm contemplating or initiating such an action.

[para 88] With respect to any information relating to particular officers that is not related to any existing or reasonably contemplated legal proceeding against an officer, or where such a proceeding has concluded, the question is, again, whether the circumstances are such that there is a reasonable likelihood relative to any such information that a legal proceeding against the officer will arise in future relative to which it will be relevant.

[para 89] In contrast to my findings as to information in the database that may in future become relevant to defence proceedings, there is not, in my view, a parallel degree of likelihood, in the abstract, that the information will be relevant to a proceeding against an individual officer that will be initiated at some unknown point in the future. It seems to me that if a proceeding were merited on the basis of the existing information and available evidence, it would be initiated, and if were not merited, there would be no reason to believe that such a proceeding would be initiated in future. (There may, however, be exceptions to this general assertion, for particular factual circumstances in which there is some impediment to a proceeding that is likely to be eliminated in future.)

[para 90] Thus, in my view, unless an action against a police officer has already been taken or it is reasonably in contemplation that it will be taken in the foreseeable future, collection of personal information in the database relating to the officer's conduct solely for the purpose of possibly initiating a proceeding at some future point would not be authorized by reference to sections 14(d), 17(d) and 20(m).

[para 91] In saying this, I acknowledge that information that could potentially give rise to a proceeding taken against an officer would likely at the same time be relevant to future defence proceedings that are likely to arise (in the manner discussed above at paras 73 to 77), and thus its entry and retention in the database may be justified for the defence purpose even if it is not justified for the purpose of potential but unknown future proceedings against an officer.

[para 92] I note that the Complainant made a number of arguments in his submission to the effect that particular types of investigations and legal proceedings that might arise within the scope of the terms "investigation" (as defined in section 1(f)) and "legal proceeding" (as defined in section 1(g)) – for example, proceedings in relation to "a breach of an agreement" – would not be engaged by the use of the information in the database. While I accept these arguments, they do not detract from the fact that the definitions of the terms also embrace investigations and proceedings of the types discussed above. Sections 1(f) and 1(g) indicate that investigations and legal proceedings within the terms of the Act may also be in relation to contraventions of enactments (which would include offence proceedings against clients of the Organization and disciplinary proceedings against officers) and remedies available at law (which would include civil actions against officers).

[para 93] I turn finally under this heading to information that the Organization stated is used for unknown "litigation or law enforcement purposes". Without further information, I cannot respond as to whether I would regard these other purposes as falling within the phrase "reasonable for the purposes of an investigation or legal proceeding". As the Organization has the burden of showing it has authority for its collection of personal information into the database, and its use and disclosure of this information to others, I can only conclude that, apart from the purposes I have already canvassed and found to be authorized purposes, the Organization has not demonstrated its authority to collect, use and disclose such information. Thus if it is collecting, using or disclosing the personal information of police officers in the database (that is neither in the "court records' nor 'publicly available' categories) for some other purposes, it may not do so.

[para 94] Before concluding this part of the discussion, I note that the Organization has told me that it shares information from the database with other lawyers. In my view, the same limitations (discussed at para 78 above) that apply in terms of entering information in the database, apply in deciding whether to share the information. Any parts of the personal information of officers can be shared by reference to sections 14(d), 17(d) and 20(m) only where the information is such as can be reasonably regarded as useful and relevant for defending against a proceeding or initiating an existing or currently-contemplated action against an officer. It would not be permissible to share information which consists of allegations that are not credible or would be impossible to substantiate, or other frivolous material that it would be unreasonable to believe has some basis in fact. It must also be evident how this information could be relevant to the defence or to the action. As well, the recipients of the information can only be the persons who will use the information for the purpose of legal proceedings. Indeed, to the extent the database contains officers' personal information (that does not fall into the 'court records' or 'publicly available' categories), the database must be kept secure and inaccessible to personnel within the law firm who do not need to collect, use or disclose it for the purpose of investigations or legal proceedings within the terms discussed above.

[para 95] I also acknowledge the Complainant's point that section 33 of the Act requires that organizations make reasonable efforts to ensure that personal information in their possession is accurate and complete. I have already said that questionable, anecdotal material that does not appear to be potentially capable of substantiation should not be

entered. However, section 33 does contain the qualifier that the accuracy requirement is only that the information be accurate to the extent reasonable for the organization's purposes. As the Act authorizes collection for the purposes of an investigation, information that is reasonably likely to be useful in an investigation may be collected, used and disclosed even though its accuracy cannot be established with certainty at the start (and indeed may never be proven), and the same would be true for information that is sufficiently credible to enter it in a proceeding, even though it might later prove to be false. While some degree of credibility is required, flexibility is also required, given the purposes for which such information can be used under the Act.

[para 96] I note in concluding this section that the Intervenor, the Criminal Trial Lawyers' Association, observed that the information in question in this case is of the kind that is exchanged on a regular basis in an informal and anecdotal fashion amongst lawyers for future use, and suggested that it is reasonable for lawyers to do this, and therefore to also create a databank of such information. While it may be neither practical nor desirable to try to monitor conversations between lawyers, the database is clearly within the reach of the Act. I agree that it would be undesirable if PIPA were to stand in the way of the exchange of useful information for criminal defence work. I also believe, as just noted, that some flexibility as to content of the database is called for. However, this is not to suggest that the personal information in the database may include idle allegations or gossip. To meet the terms of sections 14(d), 17(d) and 20(m) in the context of defence work, the information must genuinely have potential utility for assisting clients.

H) Was the personal information collected, used or disclosed in accordance with, sections 11, 16 and 19 of the Act? (These sections require that collection, use and disclosure be only for purposes that are reasonable, and that it be reasonable for the purpose)

[para 97] Sections 11, 16 and 19 of the Act require that the collection, use and disclosure of personal information be only for purposes that are reasonable:

> *11(1) An organization may collect personal information only for purposes that are reasonable.*
>
> *(2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.*
>
> …
>
> *16 (1) An organization may use personal information only for purposes that are reasonable.*
>
> *(2) Where an organization uses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is used.*
>
> …

19(1) An organization may disclose personal information only for purposes that are reasonable.

(2) Where an organization discloses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is disclosed.

[para 98] The standard as to what is "reasonable" is set out in section 2 of the Act:

2 Where in this Act anything or any matter

(a) is described, characterized or referred to as reasonable or unreasonable, or

(b) is required or directed to be carried out or otherwise dealt with reasonably or in a reasonable manner,

the standard to be applied under this Act in determining whether the thing or matter is reasonable or unreasonable, or has been carried out or otherwise dealt with reasonably or in a reasonable manner, is what a reasonable person would consider appropriate in the circumstances.

[para 99] In Order P2008-008, at para 98, I said that it is implicit from its inclusion in sections 14(d), 17(d) and 20(m) that the purpose of conducting an investigation or legal proceeding is generally regarded as a reasonable one. In my view, defending against offence proceedings and bringing complaints or taking actions against police officers where such actions or complaints are potentially supportable are reasonable purposes. As well, collecting, using and disclosing information that is potentially relevant to these purposes is reasonable for the purpose.

[para 100] As for entry in the database, I have already explained my view that entering such data in the database for future defences is also reasonable, given the likelihood that any such information will be relevant to future offence proceedings in which an officer becomes involved. However, as also already explained, the same comments do not apply, in a general sense, with respect to entering and retaining information in the database for the purpose that it could be relevant to some future, but unknown, proceeding to be brought against a police officer. With respect to the latter, if the information is not used for a proceeding, it should not be retained *for such a purpose* by reference to sections 14(d), 17(d) and 20(m) unless there is some exceptional circumstance that would make such retention reasonable in a given case. (However, as already noted, given the likelihood that the same information will be relevant to both categories of purposes, entry and retention of the same information may nevertheless be justifiable for the purposes of conducting defences.)

Personal or domestic purpose

[para 101] Before concluding I will comment on another potential basis for resolving the issues in this inquiry, which was not raised by the parties. Two recent rulings of Canadian courts turn on the idea that when an individual retains the services of an organization in connection with the individual's participation in a legal action, the organization is acting on behalf of the individual, and hence is acting in a personal or domestic rather than in a commercial capacity.

[para 102] In one of the cases, *Ferenczy v. MCI Medical Clinics*, [2004] O.J. No. 775, decided by the Ontario Superior Court, a private investigator had been retained by the defendant to a legal action to obtain video surveillance evidence that would be relevant to the defence. The plaintiff argued that the evidence was inadmissible because it had been obtained in violation of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). The court held that whether the collection of the evidence violated PIPEDA did not affect the admissibility of the evidence, and that a complaint could be brought under PIPEDA to determine the privacy issue. However, in the course of reaching this conclusion, the court also determined that the collection, use or disclosure of the information did not violate PIPEDA. The court made the following statement:

> **30** One way to avoid this result [of PIPEDA's precluding collection by an investigator if information needed for a legal proceeding], and I conclude it is the correct interpretation of the Act, is to apply the principles of agency. On this analysis it is the defendant in the civil case who is the person collecting the information for his personal use to defend against the allegations brought by the plaintiff. Those whom he employs, or who are employed on his behalf, are merely his agents. On this analysis s. 4(2)(b) of the Act governs. That section reads as follows:
>
> > 4(2)
> >
> > This part does not apply to
> >
> > ...
> >
> > (b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose;… .
>
> The defendant through his representatives was employing and paying an investigator, to collect information for him. It is the defendant's purpose and intended use of the information that one should have regard to in determining the applicability of the Act. On the basis of this analysis I conclude that the defendant is not collecting or recording personal information in the course of commercial activity. He, through his agents, was collecting information to defend himself against the lawsuit brought by the plaintiff. This is a personal purpose in the context of the civil action brought against him by the plaintiff. In my view, this conclusion is consistent with the overall purpose of the Act which is aimed primarily at information collected as a part of commerce. Section 3 of the act reads as follows:
>
> > 3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[para 103] There is some room for argument, based on this reasoning, that a law firm that has been retained by a defendant in offence proceedings is likewise not acting in the course of commercial activity, but rather is acting on behalf of the individual in a

personal or domestic capacity. Section 4(3)(a) excludes from the application of PIPA the collection, use and disclosure of personal information that is solely for personal or domestic purposes of "the individual". It is not clear if it would be appropriate to read this provision as though it said "the individual or an organization acting on behalf of an individual" in circumstances in which an individual retained an organization to act on their behalf for any personal or domestic purpose. The alternative interpretation is that "the individual" is meant to refer only to individuals collecting, using and disclosing information on their own behalf, but would not cover organizations retained to deal with information in a manner which is purely personal or domestic from the individual's standpoint, but where the organization also has its own commercial motive.

[para 104] Similar reasoning as that in the Ferenczy case was employed by the Federal Court of Canada in *State Farm Mutual v. Privacy Commissioner of Canada* [2010] F.C. 736. However, a significant distinction between the latter case and the present situation is that the Court based its decision in part on the unacceptable result that would flow if individuals could not retain organizations to collect relevant evidence for the purpose of participating in civil legal proceedings. The same problem does not arise in this jurisdiction because under PIPA, information can be collected, used and disclosed if reasonable for the purposes of an investigation or legal proceeding. (Indeed, the court commented that its interpretation of PIPEDA was supported by the fact the two statutes are meant to be substantially similar.) While it is true that in Alberta, a similar conclusion can be achieved if section 4(3)(a) is read as though it embraced organizations acting on behalf of individuals for personal or domestic capacities, it is not necessary to take this view to achieve the desirable result in policy, because the legislation deals specifically with the handling of information for legal proceedings. Indeed, it is arguable that by including the provisions relating to investigations and legal proceedings, by implication, the legislature did not regard law firms or investigators acting on behalf of individuals in civil or criminal proceedings as acting outside the scope of the Act.

[para 105] I note as well that the reading section 4(3)(a) in this way would result in the position that not only organizations that act for the purpose of legal proceedings and related investigations would have no responsibilities under the legislation; the same would be true of any organizations that act on behalf of an individual for a personal or domestic purpose, This would be a significant result and one which, had the legislature intended it, might have been expressed specifically, rather than by way of the somewhat ambiguously-worded section 4(3)(a).

[para 106] If I were to decide the present issues on the basis of these considerations, it would also be necessary to take into account the fact that the database is created for future as yet unknown defences or (possibly) for future potential proceedings against police officers, which means that the situation at hand would not fall squarely into that considered in the cases just discussed – in which organizations were acting on behalf of clients. Furthermore, the reasoning may not apply where the organization is collecting information for advancing legal proceedings against police officers on its own behalf or on behalf of one of its members (should this happen in fact) rather than on behalf of a client.

[para 107] However, given the conclusions I have already reached, it is not necessary for me to undertake this analysis or to reach conclusions pursuant to it.

[para 108] Further, the parties have not had a chance to comment on this line of reasoning, and it would accordingly be inappropriate to base my decision upon it.

[para 109] However, if I were found to be wrong in my conclusion that the Act permits the Organization to make and retain entries in the database on the basis of the provisions discussed above, with the appropriate limitations, it would be necessary to consider whether this line of reasoning would support the same or a similar conclusion.

IV. ORDER

[para 110] I make this Order under section 52 of the Act.

[para 111] I make no order with respect to personal information that falls outside the Act under section 4(3)(k) (information in a court record).

[para 112] I make no order with respect to any information related to the performance of work by police officers that is not their personal information within the terms of the discussion under Issue B – which includes any information that is exclusively as to how they performed their work, and is not intertwined with information about matters that are personal to them.

[para 113] I confirm the decision of the Organization to collect, use and disclose, and to enter and retain in its database, any personal information of police officers that is publicly available within the terms discussed under Issue E2 above.

[para 114] I confirm the decision of the Organization to collect, use and disclose, and to enter and retain in its database, any personal information of police officers that is reasonable for the purposes of an investigation or legal proceeding within the terms discussed under Issue E3 above. This includes any information that would be reasonable, in terms of its relevancy, to collect, use and disclose to assist with an investigation for defending against an offence proceeding and for defending in an offence proceeding, for both existing and possible future offence proceedings. It also includes information that would be reasonable, in terms of its relevancy, to collect, use and disclose to assist with an investigation for initiating an action (whether civil, criminal or administrative) against an officer that is reasonably in contemplation and for pursuing such an action that is existing or reasonably in contemplation.

[para 115] I find that the Organization has not demonstrated its authority for entering or maintaining any personal information of police officers in the database that does not fall within paras 111, 113 or 114, and that it may not collect, use or disclose such information or enter it in its database, and it must destroy any such information currently in its database.

[para 116] I require the Organization to ensure that the remaining personal information in the database that does not fall within paras 111 and113 is secured in such a manner that it is not accessible to anyone other than to the persons who need to collect, use or disclose it for the authorized purposes described in para 114 above.

[para 117] I further order the Organization to notify me, in writing, within 50 days of receiving a copy of this Order that it has complied with the Order. The notice to me should include a description of what the Organization has done to comply with this Order.

Christina Gauk, Ph.D.
Director of Adjudication