ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2017-87

December 18, 2017

EDMONTON POLICE SERVICE

Case File Number F7687

Office URL: www.oipc.ab.ca

Summary: The Complainant complained to the Commissioner that the Edmonton Police Service (the Public Body) had accessed information regarding two criminal investigations in which he had been the subject as a youth, in addition to other information regarding police investigations of which he had been the subject, and disclosed this information to his employer. He also raised the issue that the Public Body had used information of this kind to create a police information check (PIC) and a vulnerable sector check (VSC), and that the PIC and VSC created by the Public Body resulted in the termination of his employment, even though he does not have a criminal record and has never been convicted of a criminal offence. He complained that the Public Body's use and disclosure of his personal information contravened Part 2 of the *Freedom of Information and Protection of Privacy* Act (the FOIP Act).

The Adjudicator determined that the Public Body had not established that it had identified the information it would use or obtained the consent of the Complainant to use his personal information to create the PIC and VSC within the terms of section 39(1)(b) of the FOIP Act and section 7 of the Regulation. She also found that the disclosure of the Complainant's personal information to his employer was not authorized by Part 2 of the FOIP Act. The Adjudicator directed the Public Body not to use and disclose the Complainant's personal information contrary to the terms of the FOIP Act in the future.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 39, 40, 41, 72, 94; Freedom of Information and Protection of Privacy

Regulation, Alberta Reg 186/2008 s. 7; Security Services and Investigators (Ministerial) Regulation, Alta Reg 55/2010, the Transportation Network Companies Regulation, Alta Reg 100/2016, *Body Armour Control Act*, SA 2010, c B-4.8; **CA:** *Criminal Code*, R.S.C. 1985, c C-46; *Criminal Records Act*, R.S.C. 1985, c C-47 s. 6.3; *Youth Criminal Justice Act* S.C. 2002, c. 1, ss. 115, 118, 138

Authorities Cited: AB: F2008-029

Cases Cited: *Tadros v. Peel (Police Service)* 2009 ONCA 442;

I. BACKGROUND

[para 1] On November 12, 2013, the Complainant made the following complaint to the Commissioner:

> It is my concern that there has been unauthorized access and disclosure of my personal information resulting in a violation of the FOIP act. Furthermore, the information provided was both inaccurate and misleading resulting in the applicant's termination from his place of employment wherein he worked for 11 years. Please review the information provided which clearly demonstrates violation of both internal policies of the public body as well as provisions of the FOIP act.
>
> The response provided by the public body indicates numerous requests for internal access to information dated 13-Feb, 05. The indicated reason for the request is "Review for duty to warn employer". Section 32(1) of FOIP permits for same wherein there are public safety concerns and risk is imminent. The applicant has but one assault charge with no convictions on his criminal record. Given same, and the latency with respect to the applicants police involvement (most recently 7 years ago) neither threshold with respect to immanency and/or public safety concerns appear to be met. There cannot be a pattern of behavior without convictions, as judgment was passed, and the allegations were unsubstantiated, and found not to have occurred. Furthermore, given the public body (EPS) itself found the occurrences to be without merit (as evidenced by their refusal to charge and/or inform the subject of the occurrence) inclusion of these events would seem highly prejudicial. Nevertheless an internal review of the applicant's personal information would seem neither indicated nor warranted. Quite simply, for the review to have merit the head of the public body would have had to believe, on reasonable grounds, that the disclosure would avert or minimize an imminent danger to the health or safety of any person. There does not appear to be imminent danger in this scenario.
>
> Documentation provided demonstrates a pattern of engagement with the applicant's employer contrary to FOIP policy. One such communication (EPS FOIP 255) demonstrates same wherein the EPS member not only suggests "I can request the files from central registry" but also solicits the "thoughts" of the applicant's employer as to how best to proceed.
>
> On EPS FOIPP 253 the public body not only discloses the personal information of the applicant to an external agency they elaborate and provide further information, and pass judgment on same. "It does appear he has some history with sexual assault allegations as well as an assault charge...no conviction... involving a client; Was kind of an FYI: either he has had multiple false allegations against him or he has been able to skirt the system on convictions".
>
> Information contained within the public body's database (about the applicant) which is shared with external agencies is inaccurate, unsubstantiated, without merit, prejudicial and misleading. To include occurrences on one's criminal record check which law enforcement themselves deem baseless would seem improper and contrary to the spirit of the judicial system. A criminal

> records check allows for the tracking and provision of any illegal activities that have been found to occur beyond a reasonable doubt. To allow the disclosure of police involvement (at the arbitrary discretion of the public body) and information the public body itself investigated and/or chose not to, would not appear to meet even a balance of probabilities threshold. This circumvention with fiatic indiscretion, and without oversight, directly impacted the applicant, resulted in termination from his place of employment and is likely to preclude future vocational/occupational endeavors. This information needs to be redacted as (indicated on the top portion of EPS FOIPP 6) the applicant has no criminal convictions, conditional and absolute discharges and related information in Canada's national repository for criminal records. Disclosure of police files which do not pertain to court dispositions is prejudicial, misleading and contravenes the virtues of jurisprudence and ethical practice.

[para 2] The Complainant complained to the Commissioner that the Edmonton Police Service (the Public Body) had accessed information regarding youth matters, and other information regarding police investigations in which he had been the subject, and disclosed this information to his employer, which then terminated his employment. He also raised the issue that the Public Body had used information of this kind to create a police information check, and that this police information check resulted in the termination of his employment, even though he does not have a criminal record.

[para 3] The Commissioner authorized a mediator to investigate and attempt to settle the issues raised by the Complainant. This process was unsuccessful and the Commissioner delegated her authority to me to conduct an inquiry in relation to the issues raised by the Complainant.

[para 4] On July 14, 2015, the Registrar of Inquiries issued a notice of inquiry. The notice states that the issue for the inquiry is the following:

> Did the Public Body disclose the Complainant's personal information in contravention of Part 2 of the Act?

[para 5] The Complainant made submissions for the inquiry.

[para 6] On August 21, 2015, the staff sergeant who accessed the Complainant's personal information and disclosed it to the Complainant's employer applied to become an affected party and requested that the matter be put in abeyance as the Public Body was conducting its own investigation into her disclosure of the Complainant's information. She stated that she was concerned that evidence she provided in one proceeding could be used in the other, as a result of both proceedings taking place at the same time.

[para 7] In a letter dated August 21, 2015, the Public Body supported the staff sergeant's application to be considered an affected party and to request that the matter be held in abeyance. The Public Body also stated:

> In addition, [the Complainant] has made submissions with respect to the type of information maintained by the EPS in the EPS database and the information that is provided in connection with a police information check. Those issues were not the subject of the OIPC's investigation and would also appear to be beyond the scope off this inquiry. Please confirm.

[para 8] I determined that the staff sergeant was not an affected party to the inquiry as the FOIP Act gives me no power to make orders in relation to individuals or employees, such as the staff sergeant. An inquiry into a complaint under the FOIP Act is an inquiry as to whether a public body has acted in compliance with the restrictions on collection, use, and disclosure established by the Legislature in the FOIP Act. However, I placed the inquiry in abeyance as the staff sergeant's evidence was likely to be relevant to the inquiry and it was possible that she would be reluctant to swear an affidavit explaining her actions made on behalf of the Public Body if she were concerned that it would be used in a complaint investigation regarding those same actions conducted by the Public Body.

[para 9] With regard to the issue in relation to police information checks, I said in my letter of September 3, 2015:

> The issue for inquiry is whether the Edmonton Police Service disclosed [the Complainant's] personal information in contravention of Part 2 of the [FOIP Act]. The circumstances giving rise to the complaint are those laid out in [the Complainant's] complaint of November 12, 2013.

[para 10] On October 20, 2016, the Public Body informed the office that it was ready to proceed. On December 5, 2016, I wrote to the parties and provided a new schedule for making submissions. The Public Body was given until January 6, 2017 to make its initial submissions.

[para 11] Once I reviewed the initial submissions of the parties, I wrote to the parties on January 19, 2017. I explained that I was adding the issue of the Public Body's use of the Complainant's personal information from the Edmonton Police Reporting and Occurrence System database (EPROS) as I now realized that the Complainant had originally complained about the Public Body's access of his information from this database and that this issue had not been addressed in the notice of inquiry.

[para 12] The parties provided further submissions. After reviewing the submissions and the Complainant's complaint, it became clear that the issue of the Public Body's use of the Complainant's personal information in compiling the PIC / VSC was of primary concern to the Complainant and that this issue was not encompassed by the issue originally set for the inquiry as to whether the Public Body had disclosed his personal information. I made this determination because the PIC / VSC was created using information from the Public Body's files and then given to the Complainant to provide to his employer, rather than provided directly to the employer. As a result, the Public Body's actions in relation to the Complainant's personal information in compiling the PIC may be considered a "use" of the information under section 39 of the FOIP Act.

[para 13] I advised the parties that I was now adding the issue of whether the Public Body's use of the Complainant's personal information to compile the PIC / VSC was in compliance with the FOIP Act. I also asked the Public Body for information regarding its authority to produce PICs and VICs and its policies surrounding them.

[para 14] The Public Body provided additional evidence and submissions.

[para 15] The Complainant applied to provide a portion of his final rebuttal submissions *in camera*. The Public Body objected to this application. I decided that I would accept the *in camera* portion of the Complainant's submissions *in camera*.

[para 16] The Complainant also submitted a rebuttal submission detailing his legal arguments. He exchanged this submission with the Public Body.

II. ISSUES

Issue A: Did the Public Body use the Complainant's personal information? If yes, did it do so in compliance with, or in contravention of, section 39 of the FOIP Act?

Issue B: Did the Public Body disclose the Complainant's personal information in contravention of Part 2 of the FOIP Act?

III. DISCUSSION OF ISSUES

Issue A: Did the Public Body use the Complainant's personal information? If yes, did it do so in compliance with, or in contravention of, section 39 of the FOIP Act?

[para 17] Section 39 of the FOIP Act establishes the circumstances in which a public body may use personal information. It states, in part:

> *39(1) A public body may use personal information only*
>
> > *(a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,*
> >
> > *(b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or*
> >
> > *(c) for a purpose for which that information may be disclosed to that public body under section 40, 42 or 43.*
>
> *[…]*
>
> *(4) A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.*

[para 18] Issue A, which addresses the Public Body's use of the Complainant's personal information, has two discrete components: first, whether the Public Body's access of the Complainant's personal information in the course of its investigation into an individual to whom it refers as Male X was done in compliance with section 39, and

second, whether the Public Body's use of the Complainant's personal information from EPROS and other sources to compile the PIC was done in compliance with section 39.

[para 19] I turn now to consideration of whether the Public Body's uses of the Complainant's personal information comply with the terms of the FOIP Act.

Was the Public Body's access and use of the Complainant's personal information in the course of its investigation into an individual, to whom it refers as Male X, done in compliance with section 39?

[para 20] The Public Body argues that section 39(1)(a) authorized the staff sergeant's use of the Complainant's personal information in EPROS. Cited above, section 39(1)(a) authorizes the use of personal information if the use is consistent with the Public Body's purpose in collecting the personal information.

[para 21] Section 41 of the FOIP Act establishes when a use is consistent. It states:

> *41 For the purposes of sections 39(1)(a) and 40(1)(c), a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure*
>
> *(a) has a reasonable and direct connection to that purpose, and*
>
> *(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.*

[para 22] The staff sergeant who accessed the Complainant's personal information and then disclosed it to the Complainant's employer states in her affidavit:

> On January 4, 2013, while assigned to Child Protection and working at the Zebra Centre, I was investigating allegations that a male, hereinafter referred to as Male X, had committed a sexual assault against a youth. Male X was not [the Complainant].
>
> Upon reviewing the investigation file, I noted that Male X had previously told his ex-wife that he had been sexually assaulted by his male employer when he was a youth. I queried Male X's name in EPS' internal database, the Edmonton Police Reporting and Occurrence System ("EPROS"), and discovered an allegation of sexual assault made by Male X from 1992 which had been investigated by the EPS.
>
> EPROS provides information pertaining to the EPS investigation and does not show the outcome of any court proceedings related to the EPS investigation.
>
> I opened the 1992 occurrence involving Male X and found that [the Complainant] was listed as the accused in that matter […]
>
> I opened the records on EPROS for [the Complainant] and noted that EPROS listed [the Complainant] as an accused / subject / suspect in four sexual assaults (1992, 1995, 2003, and 2006) and as an accused in an assault in 2006 […]

> I also noted that EPROS listed [the Complainant's] employer as [the facility]. However, I did not know if his employment information was accurate.
>
> [The facility] is a residential group care treatment facility designed to meet the therapeutic needs of high risk adolescents. It provides longer-term mental health supports and services for children with complex needs and helps them transition to the community.
>
> [The facility] is a regional service offered and operated by [the Government of Alberta] […]
>
> Upon learning of this information, on or about January 4, 2013, I spoke to [an employee of the Complainant's employer], [an investigator] working at the Zebra Centre whom I had previously partnered with on investigations, about the process around staff being employed with [the Complainant's employer].

[para 23] In her May 15, 2017 affidavit the staff sergeant explained:

> As part of searching EPROS regarding the investigation into Male X, I was looking into his history with police. I queried Male X's name in EPROS and discovered a sexual assault reported by Male X from 1992 which had been investigated by the EPS.
>
> In continuing to search, I opened the 1992 occurrence involving Male X and found that [the Complainant] was listed as the accused in that matter.
>
> At this stage in my investigation into Male X, I wanted to continue to uncover as much information as possible and to assess whether this was the sexual assault that Male X had previously told his ex-wife about. I determined it was necessary to review the records in EPROS related to [the Complainant] as part of my investigation into Male X.
>
> Accordingly, I opened the accessible records on EPROS for [the Complainant] and noted that EPROS listed [the Complainant] as an accused / subject / suspect in four sexual assaults (1992, 1995, 2003, and 2006) and as an accused in an assault in 2006.

[para 24] On July 19, 2017, I asked the Public Body:

> How did looking up [the Complainant's] personal information on EPROS (other than the 1992 incident) enable the Public Body to conduct a "fulsome investigation" into a sexual assault alleged to be perpetrated by Male X? Why could [the staff sergeant] not search for other information involving Male X if her purpose was to ensure that she had located the right incident?

[para 25] The Public Body responded on September 11, 2017:

> As stated by [the staff sergeant], she determined it was necessary to review the records relating to the Complainant to uncover as much as possible and to get complete and accurate information for her investigation.
>
> […]
>
> As stated in the EPS's submissions dated January 13, 2017:
>
> The FOIPP Act is not intended to impede authorized law enforcement activities or to prevent the use of personal information for the purposes of law enforcement investigations and proceedings. As stated on multiple occasions, an Adjudicator will not second guess the work of police if they are doing police work.

[para 26] I take the Public Body's point that investigators must be free to use any information they consider pertinent in the course of policing, even if that information subsequently proves not to be pertinent at all. Use of information gathered in one investigation to determine whether it is relevant to the other investigation would be directly and reasonably related to the purpose in collecting the information within the terms of section 41(a).

[para 27] However, the evidence of the staff sergeant is ambiguous as to her purpose in accessing the Complainant's personal information other than the 1992 matter. I make this observation on the basis that while she states that she reviewed the information as part of her investigation in relation to Male X, she also states that she noted the name of the Complainant's employer and then contacted the employer and discussed the information she had reviewed with an employee of the employer with whom she had worked in the past. It appears possible from the evidence of the staff sergeant that she reviewed the files from 1995, 2003, and 2006, at least partly for the purpose of determining whether the Complainant worked at the facility and to determine whether to bring it to the Complainant's employer's attention. If so, then the purpose in using the personal information in the EPROS files would not necessarily be a policing purpose, despite the Public Body's arguments to the contrary, or one that is consistent with the Public Body's purpose in collecting the Complainant's personal information as part of the investigation in 1992.

[para 28] In response to my question as to why it was necessary to review the Complainant's files from 1995, 2003 and 2006 in relation to the investigation into Male X, the Public Body essentially directed me back to the affidavit that gave rise to my question. My question was posed after reading both affidavits, and being left in uncertainty that the review of the 1995, 2003, and 2006 matters was related to the investigation of Male X. As cited above, section 41 of the FOIP Act establishes that a use of personal information is consistent with a public body's purpose in collecting personal information when the purpose of the use had a reasonable and direct connection to the purpose for the collection.

[para 29] I accept that it is possible that the staff sergeant, although she does not say so, reviewed the EPROS entries from 1995, 2003 and 2006 to see if the files to which they refer might be likely to shed light on the 1992 matter. If this was her purpose, then this purpose meets the requirements of section 41, in that it would be a use of personal information with a reasonable and direct connection to the Public Body's purpose in collecting the Complainant's personal information, and the use would be necessary for her to conduct the investigation into Male X reasonably. The requirements of section 39(1)(a) would be met in relation to such use.

[para 30] With regard to any use by the staff sergeant's use of the Complainant's personal information to determine whether he worked at the facility and to decide whether to inform the Complainant's employer about the information she had accessed, I find that his issue is better addressed under ISSUE B, which asks whether the Public

Body's disclosure of the Complainant's personal information was in compliance with the requirements of Part 2 of the FOIP Act.

Was the Public Body's use of the Complainant's personal information to compile the PIC in compliance with section 39?

[para 31] In answering this question, it is first necessary to define and differentiate the systems that release information in the custody or control of law enforcement for the purpose of ensuring the suitability of candidates and incumbents for employment working with vulnerable individuals. There are two main systems for releasing such information operating in Alberta: the first is set out in the federal *Criminal Records Act*. The RCMP follows the model set out in the *Criminal Records Act*. The second release system is created by policy adopted by the Alberta Association of Chiefs of Police. The Public Body follows the policy adopted by the Association of Chiefs of Police.

The system under the Criminal Records Act

[para 32] Section 6.3 of the *Criminal Records Act*, R.S.C. 1985, c. C-47 establishes a process for performing a criminal record check when the applicant for the check is seeking a position, or has a position, of trust or authority in relation to a child or vulnerable person. Under section 6.3(2), the Commissioner of the Royal Canadian Mounted Police may make a notation regarding convictions for various sexual offences in the *Criminal Code*, RSC 1985, c.C-46. Under section 6.3(7) a police service is authorized to disclose the notation regarding the applicant to the applicant's employer (if the employer is an organization responsible for the well-being of a child or vulnerable person and the applicant has consented to the disclosure).

Police Information Checks and Vulnerable Sector Checks pursuant to Alberta Association of Chiefs of Police Policy

[para 33] The Public Body provided for my review a resolution passed by the Alberta Association of Chiefs of Police for the year 2013 (the resolution was subsequently updated) dealing with the provision of PICs and VSCs to employees or prospective employees for the purpose of providing such checks to their employers or prospective employers. The resolution also addressed the kinds of information from police files these checks would include, and the fees police services would charge for providing the checks in 2013[1]. The resolution describes the information that will be included in a standard check and in a vulnerable sector check.

[para 34] According to the resolution, information about an applicant would be searched in local police records, the JOIN database, and CPIC. For a standard information check, the kinds of personal information located in these sources that would be included in the check would include information about convictions, specific sentences, alternative measures, pending / outstanding charges, including criminal and / or relevant charges, outstanding warrants, findings of "not criminally responsible – mental disorder",

[1] The PIC in this case was created in 2013.

court orders, and all information in police files considered relevant. The joint resolution also states: "When applicable, any involvement while a youth will be disclosed clearly identifying such matters as Youth".

[para 35] A vulnerable sector information check (VSC) would include the foregoing information but also include information falling within the terms of section 6.3 of the *Criminal Records Act*, should any such information exist.

The Public Body's process for completing PICs and VSCs

[para 36] The Public Body compiles personal information in its files (EPROS) and from the Justice Online Information Network (JOIN) and the Canadian Police Information Centre (CPIC) to prepare the PIC. It charges a PIC applicant fees for preparing the PIC. The PIC is intended for the collection and use of a PIC applicant's employer or prospective employer in determining whether the applicant is suitable for employment. However, the PIC is never provided directly to the employer, but is provided to the applicant.

[para 37] The former Manager of the Public Body's Police Information Check Section swore an affidavit on September 8, 2017 regarding the PIC process in 2013, the year in which the PIC that is the subject of the complaint was created. It states:

> In 2013, a Police Information Check could result in the following information being included on a Police Information Check Certificate:
>
> a) criminal records and/or convictions;
> b) absolute and/or criminal discharges;
> c) alternative measures, adult diversions program involvement, or stays or proceedings;
> d) pending/outstanding charges;
> e) Court orders; and
> f) Police files/information
>
> If any of the above information was included in a Police Information Check Certificate arising from a request for a Police Information Check, the Certificate was only provided to the applicant. It was never shared with a third party by the PICS or the EPS.
>
> Individuals applying for a Police Information Check who may be in a position of trust or authority with vulnerable members of society are required to undergo a broader Vulnerable Sector Police Information Check. Vulnerable persons are those who are in a position of dependence or others such as children, people with disabilities, or the elderly.
>
> It is the responsibility of the organization or person responsible for the vulnerable persons to indicate that an applicant must seek a Vulnerable Sector Police Information Check. The PICS then verifies if the position is one that requires a Vulnerable Sector Police Information Check.
>
> If the position does not meet the requirements, the EPS will not conduct a Vulnerable Sector Police Information Check.
>
> […]

> The EPS obtains express written consent from the applicant prior to the use of any personal information as part of a Vulnerable Sector Police Information Check.

[para 38] The Manager describes the processes by which PICS are created and explains how it is decided that personal information will be incorporated in a PIC. He states:

> Similarly, for Police Files/Information, the Procedures stated "all police information or files that possess information that is relevant to the Police Information request will be included as relevant information. The applicant will be designated as the 'subject' of these reports".
>
> In addition, the Procedures provided "when applicable, any involvement while a youth will be disclosed clearly identifying such matters as Youth".
>
> In 2013, it was not the case that information about an individual that existed in a police file was automatically relevant information for the purposes of a Police Information Check. The PICS Supervisor was responsible for reviewing the information in police files to make a determination with respect to relevance.
>
> If the PICS Supervisor determined that the police file contained relevant information, the PICS Supervisor could recommend that such information be included on the Police Information Check Certificate. This recommendation then had to be reviewed by the PICS Manager.
>
> Information in the police file was only included if the PICS Manager agreed that the information was relevant and that it should be included on the Certificate.
>
> Determining whether information contained in a police file was relevant information for the purposes of a Police Information Check required that both the PICS Supervisor and the PICS Manager review and assess the information in the police file and evaluate whether the information was relevant in the context of the request for the Police Information Check.
>
> In making this determination, the PICS Supervisor and PICS Manager considered the nature and responsibilities of the position, the individuals who the applicant would be interacting with, the frequency and recency of the occurrences, and any pattern of behavior resulting in a risk to public safety.
>
> During the Relevancy Review process, the PICS Supervisor and the PICS Manager could seek legal advice from an EPS Legal Advisor to assist in determining what information should be included.
>
> As such, the determination of whether information contained in a police file was relevant information was a matter that required the PICS Supervisor and the PICS Manager to assess the information and make a decision based on professional knowledge and experience, discussions with each other, advice received from the EPS legal advisors when appropriate, and the Resolution and Procedures.
>
> If it was determined by the PICS Manager that there was relevant information from police files to include, then the applicant would be designated as the "subject" of the occurrences and the information would be included on the Police Information Check Certificate.
>
> Accordingly, an individual may not have "cleared" a Police Information Check if the individual had previously been the subject of a police investigation, regardless of whether the investigation was ongoing, suspended, or closed, and regardless of whether or not the complaint that led to the investigation resulted in charges or a conviction.

> Where a police file contained information about an individual, that individual could only "clear" a Police Information Check if the PICS Manager determined, based on the assessment and in accordance with the Resolution and Procedures, that information about the individual contained in a police file was not relevant information for the purposes of the Police Information Check request.
>
> The number of applicants who had non-conviction information from police tiles included on a Certificate as a result of it being relevant was low. During my time with the PICS, I estimate that approximately 12 applicants per year had non-conviction information from a police file included in a Police Information Check Certificate.

[para 39] The Manager states the following regarding the vulnerable sector PIC process:

> Both types of [PICs] involve a check of three law enforcement databases: EPS local records (EPROS); Justice OnLine Information Network (JOIN) Alberta court records' and Canadian Police Information Centre (CPIC) national police records. For Vulnerable Sector Police Information Checks, the CPIC check includes a check for pardons in the National Repository of Criminal Records. If these databases include relevant information, that information is provided to the applicant.

What is a police service's legal authority to compile a PIC?

[para 40] Three Alberta enactments contain reference to "police information checks". They are: the Security Services and Investigators (Ministerial) Regulation, Alta Reg 55/2010, the Transportation Network Companies Regulation, Alta Reg 100/2016, and the *Body Armour Control Act*, S.A. 2010, c B-4.8. These statutes refer to "police information checks" but do not define them. While these enactments create requirements for individuals to include "police information checks" in applications, the enactments do not indicate where the police information check is to be obtained or provide power to an entity, such as a police service, to create them. I am unable to identify a source of provincial or federal statutory authority for an Alberta police service to create PICs and VSCs as they are currently being created. From the Public Body's evidence, I understand it relies on the resolution of the Alberta Association of Chiefs of Police and the consent of applicants under the FOIP Act as authority to create PICs and VSCs for applicants who pay the fees it sets for this service.

[para 41] The Public Body does not argue that creating a PIC is a consistent use of the Complainant's personal information within the terms of section 39(1)(a) and section 41 of the FOIP Act, but relies instead on section 39(1)(b) in which a public body may use personal information for a purpose that is inconsistent with its purpose in collecting the information, provided the subject of the information identifies the personal information to be used and consents to the public body's use of the information for the inconsistent purpose.

[para 42] Section 7 of the Freedom of Information and Protection of Privacy Regulation (the Regulation) prescribes the form consent is to take within the terms of section 39(1)(b) of the FOIP Act. It states, in part:

7(2) The consent of an individual to a public body's using or disclosing any of the individual's personal information under section 39(1)(b) or 40(1)(d) of the Act

(a) must meet the requirements of subsection (4), (5) or (6) and

(b) must specify to whom the personal information may be disclosed and how the personal information may be used.

[…]

(4) For the purposes of this section, a consent in writing is valid if it is signed by the person who is giving the consent.

(5) For the purposes of this section, a consent in electronic form is valid if

(a) the head of the public body has established rules respecting the purposes for which consent in an electronic form is acceptable,

(b) the purpose for which the consent is given falls within one or more of the purposes set out in the rules mentioned in clause (a),

(c) the public body has explicitly communicated that it will accept consent in an electronic form,

(d) the consent in electronic form

(i) is accessible by the public body so as to be usable for subsequent reference,

(ii) is capable of being retained by the public body, and

(iii) meets the information technology standards, if any, established by the public body,

(e) the consent in electronic form includes the electronic signature of the person giving the consent,

(f) the electronic signature

(i) is reliable for the purposes of identifying the person giving the consent, and

(ii) meets the information technology standards and requirements as to the method of making the signature and as to

the reliability of the signature, if any, established by the public body,

and

(g) the association of the electronic signature with the consent is reliable for the purpose for which consent is given.

(6) For the purposes of this section, a consent that is given orally is valid if

(a) the head of the public body has established rules respecting the purposes for which consent that is given orally is acceptable,

(b) the purpose for which the consent is given falls within one or more of the purposes set out in the rules mentioned in clause (a),

(c) the public body has explicitly communicated that it will accept consent that is given orally,

(d) the record of the consent

(i) is accessible by the public body so as to be usable for subsequent reference, and

(ii) is capable of being retained by the public body,

(e) the public body has authenticated the identity of the individual giving consent, and

(f) the method of authentication is reliable for the purpose of verifying the identity of the individual and for associating the consent with the individual.

[para 43] The Public Body used information about three allegations against the Complainant to create the PIC. It used information about two youth matters to create the VSC. Of the two youth matters, one matter did not result in charges or a conviction; the other matter resulted in an absolute discharge.

[para 44] The Public Body provided a copy of the consent form the Complainant provided in relation to the PIC it completed. This consent states:

I hereby give consent to the Edmonton Police Service to conduct a search for:

1. criminal records and/or convictions of any kind which relate to me;
2. absolute and/or conditional discharges of any kind which relate to me;
3. alternative measures and / or adult diversion involvement of any kind which relate to me;
4. warrants of any kind which relate to me;

> 5. police files, from any law enforcement agency, Canadian or otherwise, which relate to me; and
> 6. pardons or record suspensions of any kind pursuant to the *Criminal Records Act*, which relate to me. [my emphasis].

I further agree that I remise, release, and forever discharge the Edmonton Police Service, the Chief of Police of the Edmonton Police Service, the Edmonton Police Commission, and their administrators, successors, assigns, agents, officers, servants and employees from any and all manner of actions, suits, debts, dues, general damages, special damages, pecuniary damages, costs, interest, claims and demands of every nature and kind at law or in equity under any statute, including but not limited to direct or consequential loss, occasioned by me or my legal representatives, heirs, assigns or agents, arising or in any way related to the police information check process described above.

I understand that any information provided by me for the purposes of this police information check, including fingerprints, may be used or disclosed for law enforcement purposes. The information collected on this form and as part of the police information check process will be collected, used, and disclosed in accordance with the *Freedom of Information and Protection of Privacy Act* or as otherwise provided by law.

Before signing this Police Information Check Waiver, I have fully informed myself of the content and meaning and understand the content and meaning. Must be signed in the presence of appropriate agency personnel.

[para 45] The VSC portion of the consent form states:

> This area must be completed if you are applying for a position with a person or organization responsible for the well-being of one or more "children" or vulnerable persons. If the position is a position of authority or trust relative to those children or vulnerable persons, you consent to a search being made in criminal records to determine if you have been convicted of a sexual offence listed in the schedule to the *Criminal Records Act* which have [*sic*] been subject to a pardon or record suspension.
>
> […]
>
> I consent to a search being made in the automated criminal records retrieval system maintained by the Royal Canadian Mounted Police to determine if I have been convicted of, and been granted a pardon or record suspension for any of the sexual offences that are listed in the schedule to the *Criminal Records Act*.
>
> I understand that, as a result of giving this consent, if I am suspected of being the person named in a criminal record for one of the sexual offences listed in the schedule to the *Criminal Records Act* in respect of which a pardon or record suspension was granted or issued, that record may be provided by the Commissioner of the Royal Canadian Mounted Police to the Solicitor General of Canada, who may then disclose all or part of the information contained in that record to a police force or other authorized body. That police force or authorized body will then disclose that information to me.

[para 46] The Public Body states:

> The processing of the Complainant's requests for Police Information Checks was in accordance with the Resolution and the Procedures.

> The Resolutions and Procedures stated that information in police files that was relevant to the Police Information Check could be disclosed. This was also included in the Request Form and waiver and the waiver and consent signed by the Complainant.

[para 47] The Manager states in his affidavit:

> The EPS incorporated the Resolution [of the Alberta Association of Chiefs of Police] into its disclosure guidelines, which in 2013 were found in the EPS Police Information Checks Procedures (the "Procedures") and which were also reflected in the "Waiver" found on the form submitted by an applicant requesting a Police Information Check.

Did the Complainant identify the personal information the Public Body used in the PIC and consent to the Public Body's use of that information?

[para 48] Cited above, section 39(1)(b) establishes that an individual must identify the information that the Public Body will use and consent to the Public Body's use of that information before the Public Body may use it. The question becomes what it means to "identify" personal information within the terms of this provision and to what extent a PIC applicant can be said to consent to the Public Body's use of the information the applicant has identified.

[para 49] The word "identified", which appears in section 39(1)(b), typically means "established the identity of", where it takes a direct object, as it does in this section. Essentially, section 39(1)(b) requires an individual to establish the identity of the information, or name the information, a public body may use, and consent to that use in the manner prescribed in the Regulation.

[para 50] The consent form the Complainant signed authorizes the Public Body to *search for* information regarding criminal records and / or convictions of any kind related to the Complainant, absolute discharges and / or conditional discharges of any kind related to the Complainant, alternative measures and / or adult diversion involvement related to the Complainant, warrants of any kind related to the Complainant, police files related to the Complainant, and record suspensions of any kind pursuant to the *Criminal Records Act* relating to the Complainant.

[para 51] The consent form the Complainant signed does not, where the form refers to files, detail the kinds of information that are the subject of the search. Moreover, it does not address the use the Public Body will make of any information that it might locate, if it does locate information in its search. While the Public Body argues that the terms of the resolution of the Alberta Association of Chiefs of Police (the resolution) and its procedures are "reflected" in the consent form, I am unable to identify any clause in the consent that refers to the resolution. In addition, the waiver does not indicate that the person signing it has read the resolution or knows anything about the Public Body's PIC procedures, and so a PIC applicant cannot be said to know that the Public Body would search for various kinds of records not forming part of a criminal record and also include them in the PIC if it considered them relevant. A PIC applicant could reasonably believe, from the wording of the form, that the Public Body would search for information

regarding a criminal record and that it was searching through the records the form lists in order to find reference to one.

[para 52] The resolution of the Alberta Association of Chiefs of Police itself does not indicate what kinds of information are in police files, what kinds of information in police files it considers relevant, or the process by which a police service will determine the relevance of any information located. The consent form reflects the resolution in the sense that it does not contain information explaining these details either. While the Complainant's consent authorized the Public Body to search for police files, it is unclear from the form what information police files contain, what types of personal information the Public Body intended to use, and how it intended to use it.

[para 53] In addition, as a PIC applicant would not necessarily know what personal information the Public Body has access to, and what it intends to use to complete the PIC, it cannot be said that the form signed by a PIC applicant "identifies" information as required by section 39(1)(b). In my view, the use of the term "identified" in section 39(1)(b) means that the person who will identify information and consent to the use of information, is, at the very least, aware of the existence of the information and knows what use the Public Body will make of it, such that the applicant can be said to have identified the information and consented to its use for a particular purpose within the terms of section 39(1)(b).

[para 54] For the waiver to enable an applicant to identify personal information within the terms of section 39(1)(b) of the FOIP Act, the Public Body must describe in greater detail the information will use to create the PIC so that the applicant is in a position to know what items of the applicant's personal information the Public Body has in its custody or control it will use. Once the Public Body locates information about an applicant that it believes should be included in the PIC or VSC and decides which part of the information it considers it necessary to use, it must then describe or show that information to the applicant so that the applicant may then identify the information and consent to the use the Public Body intends to make of the information. If an applicant is unaware of the information that will be used, and is given no choice to say yes or no to its use, then an applicant cannot be said to have consented to the use of the information.

[para 55] In this case, I am not satisfied that the Complainant identified the information the Public Body intended to use to create the PIC. The consent form he signed not does not acknowledge that he is aware of the existence of the personal information the Public Body intended to use, or that he is aware of the kinds of information in police files that could be considered relevant and included in the PIC, or even that information about police investigations not resulting in charges or convictions could be included in the PIC. Finally, I note that the consent form does not refer to the use the Public Body intended to make of the Complainant's personal information if it located any.

Did the Complainant identify the information that the Public Body used to complete the VSC?

[para 56] Cited above, the consent the Public Body requires a VSC applicant to sign refers only to information regarding a record suspension for sexual offences listed in the schedule to the *Criminal Records Act*. As the Public Body confirmed in its submissions in response to my questions (paragraphs 116 – 120), it did not include information regarding record suspensions in the PIC and VSC, but information about "allegations and non-convictions". It stated at paragraph 50 of its September 11, 2017 submissions:

> The VS certificate listed the three investigations referred to in the PIC Certificate, plus one in 1992 and one in 1995 […]

The VSC consent signed by the Complainant (part 4 of the Police Information Check application form), and which the Public Body provided for my review, makes no reference to information about using investigations, allegations and non-convictions as information that would be included in a VSC. Instead, it describes the kinds of information that may be included in a vulnerable sector search under the *Criminal Records Act*. As a result, I find that the Complainant did not identify the information the Public Body used to create the VSC in even a general sense.

[para 57] In addition, given that I find that "identifying" personal information requires identifying the particular information that will be used, I find that the Complainant did not identify the information the Public Body used, as it did not describe the allegations and non-conviction information it intended to use to create the VSC when the Complainant completed the application.

Did the consent signed by the Complainant meet the requirements of section 7 of the Regulation?

[para 58] The Public Body states in its September 11, 2017 submission:

> Pursuant to s. 7(2) of the Regulation, the consent of the individual to the use of the individual's personal information must meet the requirements of ss. 7(4), (5), or (6) of the Regulation and must specify to whom the personal information may be disclosed and how the personal information may be used.

[para 59] Section 7 of the Regulation, to which the Public Body refers, establishes the manner in which consent is to be given. Cited above, section 7(2)(b) of the Regulation requires that consent *specify how the personal information may be used*.

[para 60] The term "specify" means "name or mention expressly"[2]. While the PIC waiver signed by the Complainant refers to a search for information of general kinds being conducted, the waiver does not refer to the information that is located and considered relevant by the Public Body being included in a PIC.

[2] Katherine Barber Ed. *Canadian Oxford Dictionary*, 2nd Edition, (Don Mills; Oxford University Press, 2004) p. 1496

[para 61] The Regulation uses the definite article "the" to describe personal information in section 7(2)(b). This use of the definite article suggests that the Regulation was intended to indicate that an individual is to identify specific personal information that a public body may use ("*the* information"), rather than general types of information the existence of which the individual may not even be aware ("any information" or "information)". As noted above, the waiver signed by the Complainant refers to general kinds of information for which the Public Body will search, but it does not indicate the information the Public Body has, or the information the Public Body will actually use, or specify the use the Public Body will make of such information. An applicant might not understand from the waiver what personal information the Public Body has in its custody or control or that it would be used to create a PIC. In some cases an applicant may be aware that the Public Body is likely to have a file about him or her, but in other cases, the applicant may not be aware that the Public Body received allegations about him or her or considered him or her a suspect and created a file.

[para 62] For the reasons above, I find that the signed waiver the Public Body obtained from the Complainant does not meet the formal requirements imposed by section 7 of the Regulation.

[para 63] I find that the Complainant did not consent to the Public Body's use of his personal information to create the PIC or VSC within the terms of section 39(1)(b) of the FOIP Act or section 7 of the Regulation. As I find that the Public Body used the Complainant's personal information without valid consent in circumstances where it was required to obtain his consent to use it, I intend to order the Public Body to cease using the Complainant's personal information in its custody or control in contravention of the FOIP Act.

[para 64] I acknowledge that if the Public Body amended its process so that it showed a PIC / VSC applicant the information it intended to include in the PIC / VSC, prior to creating the PIC / VSC, the applicant might not consent to the creation of the PIC / VSC. In such a case, the Public Body could not create the PIC / VSC and an employer might not be able to obtain information necessary for determining whether the employee is suitable for employment in the vulnerable sector. Neither the employer nor the public body could compel the employee in such a case to obtain a PIC / VSC, given that there is no statutory authority to create or require a PIC / VSC as the Public Body is presently providing them, except possibly under the statute and regulations expressly referring to "police information checks". (If consent is compelled, there may be a question of whether consent has been obtained.) However, there are clearly circumstances in which an employer in the vulnerable sector may need to know an employee's personal information contained in police files, despite the fact that an employee does not consent to the Public Body including the information in a PIC / VSC. If the Public Body were to rely on section 39(1)(a) to use personal information to create PICs / VSCs it would not need consent; however, it would be required to establish that it is using the information for a purpose that has a real and direct connection to its purpose in collecting the information, and is necessary for performing its statutory duties within the terms of section 41 of the FOIP Act. That may be too onerous a burden for the Public Body to meet in relation to

some of the information the Public Body currently includes in PICs / VSCs. In any event, its current program is based on consent.

[para 65] I recommend to the Public Body that it redesign its PIC / VSC process and consent forms to enable an applicant to identify the personal information it will use to create the PIC / VSC and to consent to its use to create the PIC / VSC in order to meet the terms of section 39(1)(b). However, I accept that there will be circumstances in which an applicant may not consent to the creation of the PIC / VSC and the Public Body will not have authority to create one, even in situations where the employer may need to obtain the information that would be included in the PIC / VSC, but for the lack of consent. In my view, the ability to address and resolve the problems I have identified with the PIC / VSC process lies with the Legislature.

The Tadros Decision

[para 66] The Public Body drew my attention to *Tadros v. Peel (Police Service)*, 2009 ONCA 442 in which the Ontario Court of Appeal determined that information about withdrawn criminal charges, which had been included in a vulnerable sector search performed by the Toronto Police Service, formed part of an applicant's criminal history and was properly disclosed. The Ontario Court of Appeal found that the respondent in that case had consented to the use of his criminal history to create the vulnerable sector search and that it should have been evident to the respondent that withdrawn charges formed part of his criminal history. The Court reviewed the consent form, which stated:

> I HEREBY REQUEST THE TORONTO POLICE SERVICE TO UNDERTAKE A POLICE REFERENCE CHECK ON ME BY SEARCHING THE APPROPRIATE DATA BANKS, BOTH NATIONAL AND LOCAL TO WHICH THE SERVICE HAS ACCESS AND PROVIDE ME WITH A SUMMARY OF ANY INFORMATION REVEALED PURSUANT TO THE POLICE REFERENCE CHECK PROGRAM. IN THE EVENT NO INFORMATION ABOUT ME IS FOUND AS PART OF THAT CHECK, I CONSENT TO THE TORONTO POLICE SERVICE DISCLOSING THAT FACT TO THE ORGANIZATION IDENTIFIED BELOW. IN THE EVENT THAT PERTINENT INFORMATION IS PROVIDED TO ME, I CONSENT TO THE TORONTO POLICE SERVICE DISCLOSING THAT FACT TO THE ORGANIZATION IDENTIFIED BELOW.

[para 67] The Ontario Court of Appeal allowed the police service's appeal in the foregoing case.

[para 68] The Complainant states in his submission of September 25, 2017:

> The most distinguishable difference between that matter and the current inquiry is that, in the former, not only was a charge laid, but the appellant in that matter entered into a plea bargain and accepted a peace bond. Furthermore, there was a record of these events which took place in a courtroom which omitted any expectation of privacy.

[para 69] I agree with the Complainant that *Tadros* is distinguishable, and agree that the criminal history set out in the *Tadros* case is different than the information about the Complainant in police files. However, I find that this case is primarily distinguishable on the basis of the consent that was signed. As noted above, the consent form used by the

Public Body and signed by the Complainant does not identify the personal information that will be used or explain how it will use personal information or what information it intends to use to create the PIC or VSC. The Court of Appeal in *Tadros* was able to determine that the respondent in that case had been given adequate information to understand that information about withdrawn charges formed part of his criminal history, and that he knew of the charges. The Court considered that the clarity of the wording of the consent form enabled the respondent to understand how and to whom his personal information would be disclosed. I have found above that the consent form signed in this case does not contain such clarity with regard to the Public Body's use of the Complainant's personal information.

Conclusion

[para 70] To conclude, I find that the Complainant did not consent to the Public Body's use of his personal information within the terms of section 39(1)(b).

Issue B: Did the Public Body disclose the Complainant's personal information in contravention of Part 2 of the FOIP Act?

[para 71] The Public Body concedes that the staff sergeant disclosed the Complainant's personal information on January 4, 2013 to an employee of the Complainant's employer with whom she had worked in the past at the Zebra Centre. The staff sergeant disclosed the Complainant's last name, birthdate, and information regarding two youth matters; one which took place in 1992 when the Complainant was fifteen and the other, which took place in 1995 when he was seventeen. The staff sergeant also disclosed details of three allegations that had been made against the Complainant as an adult in 2003 and 2006.

[para 72] The Public Body argues that sections 40(1)(c), (e), (i), and (ee), authorized the disclosure of the Complainant's personal information to an employee of the Complainant's employer in the circumstances I have described.

[para 73] I will now consider each of these provisions to determine whether they authorize the disclosure of the Complainant's personal information to the employee of the Complainant's employer.

Section 40(1)(c)

[para 74] Section 40(1)(c) states:

> *40(1) A public body may disclose personal information only*
>
> > *(c) for the purpose for which the information was collected or compiled or for a use consistent with that purpose […]*

[para 75] Section 41 of the FOIP Act establishes the circumstances in which a use or disclosure is consistent with a public body's purpose in collecting personal information. It states:

> *41 For the purposes of sections 39(1)(a) and 40(1)(c), a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure*
>
> *(a) has a reasonable and direct connection to that purpose, and*
>
> *(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.*

[para 76] The Public Body argues in its initial submission of January 13, 2017:

> Pursuant to section 40(1)(c) of the FOIPP Act a public body may disclose personal information for the purpose for which the information was collected or compiled or for a use consistent with that purpose.
>
> […]
>
> The EPS collected and disclosed the Complainant's personal information for law enforcement purposes and as such the disclosure was authorized by section 40(1)(c) of the FOIPP Act.
>
> […]
>
> The Complainant's personal information was collected by the EPS for the detection and prevention of crime, the enforcement of law, and the preservation of the peace and maintenance of public safety. Therefore, it was collected for a law enforcement purpose and was authorized by section 33(b) of the FOIP Act.
>
> […]
>
> Policing encompasses "those activities carried out, under the authority of a statute, regarding the maintenance of public order, detection and prevention of crime or the enforcement of law." As previously recognized by the OIPC, police officers are charged by statute, the *Police Act*, with the preservation and maintenance of the public peace and the prevention of crime.
>
> […]
>
> "Peace officer" is defined in section 1(j) of the *Police Act* as a "person employed" for the purposes of preserving and maintaining the public peace".
>
> Section 41(1)(a) of the *Police Act* also provides that the chief of police of a police service is responsible for the preservation and maintenance of the public peace and the prevention of crime within the municipality.
>
> As indicated in the evidence of [the staff sergeant], the personal information of the Complainant, consisting of his name, date of birth, workplace, and criminal history was contained EPS records pertaining to EPS criminal investigations. All of this is personal information that is clearly related to the EPS' investigations into allegations of sexual assault

and assault, determining whether a crime had been committed, and identifying the individuals involved in the alleged criminal activity.

All of the Complainant's personal information was collected in the course of, and for the purpose of, investigating and preventing crime, enforcing the law, and preserving the peace and maintaining public safety.

[…]

As indicated by [the staff sergeant], the Complainant's personal information was disclosed to [the Complainant's employer] to take whatever action it deemed appropriate in protecting children […] Her purpose for disclosing the personal information was to maintain the public peace and to ensure the safety of the public, specifically the children at [the facility].

[para 77] The affidavit of the staff sergeant dated January 12, 2017 states:

As part of fulfilling my role as a police officer in preserving and maintaining the public peace and safety and preventing crime, as well as my specific role as a member of the Zebra Centre tasked with protecting children, I determined that it was necessary to collaborate and share the information with [the Ministry that employed the Complainant to work at the facility] to maintain the public peace and to ensure the safety of children in Edmonton.

[para 78] In her affidavit of January 12, 2017, the staff sergeant states:

I also noted that EPROS listed [the Complainant's] employer as the [facility]. However, I did not know if his employment information was accurate.

[…]

I verbally asked [the employee] if [the Complainant's employer] was aware of a male named [Complainant's last name] who may be working at [a facility operated by the employer].

[The employee] requested that I provide her with [the Complainant's] date of birth and asked what I saw that was concerning.

On or about January 4, 2013, I verbally provided [the employee] with [the Complainant's] date of birth and advised that he was the accused / subject / suspect in four sexual assaults (1992, 1995, 2003 and 2006) and that he was accused in an assault in 2006.

[para 79] An email dated January 8, 2013 written by the staff sergeant to both the employee of the Public Body to whom she disclosed the Complainant's personal information and the employee's manager states:

Re: [the Complainant]

It's not new … this was investigated when it was reported in 1995. We are just unaware of the outcome. It appears as though he has no record so he was either absolutely discharged or the charges were dropped.

It does appear that he has some history with sexual assault allegations as well as an assault charge … no conviction… involving a client.

Was kind of an FYI … either he has multiple false allegations against him or he has been able to skirt the system on convictions…. [my emphasis]

[para 80] In her subsequent affidavit dated May 15, 2017, the staff sergeant states:

> As indicated in my Affidavit sworn on January 12, 2017, and as part of fulfilling my role as a police officer in preserving and maintaining the public peace and safety and preventing crime, as well as my specific role as a member of the Zebra-Child Protection Centre tasked with protecting children, I determined that it was necessary to collaborate and share the tombstone data regarding [the Complainant] with [his employer].
>
> It was later determined that it was necessary to obtain further information on [the Complainant] to ascertain whether public safety was at risk as a result of [the Complainant's] employment with [the Ministry that employed the Complainant to work at the facility].
>
> Accordingly, on January 31, 2013, I consulted with an EPS lawyer. Following that, on February 5, 2013, I requested five police files relating to [the Complainant] from EPS Central Registry.
>
> […]
>
> I was required to request the files from EPS Central Registry because I was not able to access the detailed information from the files on EPROS. Generally, EPROS does not provide detailed information (i.e. written report) for files created prior to 2008.
>
> […]
>
> I believed it was necessary to access and review the files to determine if they included any information that was relevant to my duties to warn [the Ministry that employed the Complainant to work at the facility]. As indicated in my request to EPS Central Registry for the police files […], the files were requested for a "review for Duty to Warn employer".

[para 81] The Public Body states in its submissions of September 11, 2017:

> [The staff sergeant] subsequently retrieved five police files to consider whether a duty to warn existed as a result of the information that she learned. Accordingly, the duty to warn is only relevant insofar as it relates to [the staff sergeant's] subsequent review of the Complainant's files to determine whether the EPS was obliged, at common law or further to s. 32 of the FOIPP Act, to make further disclosure. Ultimately, after further consultations, the EPS determined that the duty to warn was not triggered in this case.

[para 82] From the affidavit evidence, I conclude that the staff sergeant disclosed the Complainant's personal information to determine whether he was the person whose name she had researched in EPROS and to determine whether he worked at the facility. The email written by the staff sergeant following the disclosure characterizes the disclosure as "kind of an FYI". The email also indicates that the staff sergeant did not know whether false allegations had been made against the Complainant or whether he had "[skirted] the system" in some way.

[para 83] To have a reasonable and direct connection to a public body's purpose in collecting personal information within the terms of section 41(a), the purpose of the disclosure must be reasonably and directly connected to the purpose for which the Public Body was initially authorized to collect personal information. I accept that conducting an investigation into a possible offence and protecting children are activities that have a

reasonable and direct connection with each other, such that collection for one purpose and disclosure for the other meet the terms of section 41(a).

[para 84] However, it is insufficient under section 41 only that the purposes in collection and disclosure have a reasonable and direct connection. Section 41(b) requires that the disclosure be *necessary* for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.

[para 85] In Order F2008-029, the Director of Adjudication discussed the meaning of "necessary" in relation to a disclosure of information for the purposes of meeting the goals of a program of the Public Body. She said:

> […] I find that "necessary" does not mean "indispensable" - in other words it does not mean that the CPS could not possibly perform its duties without disclosing the information. Rather, it is sufficient to meet the test that the disclosure permits the CPS a means by which they may achieve their objectives of preserving the peace and enforcing the law that would be unavailable without it. […]
>
> […] Again, I find that "necessary" in this context does not mean "indispensable", and is satisfied as long as the disclosure is a significant means by which to help achieve the goals of the program.

I agree with the above reasoning. I accept that disclosure of the Complainant's personal information would be necessary if it could be established that it was a significant means by which the staff sergeant could achieve the goal of protecting children.

[para 86] I am unable to find, based on the staff sergeant's affidavit evidence, and the evidence of the emails between the staff sergeant and the employee of the Complainant's employer, that the disclosure was a significant means by which the staff sergeant could meet the objective of protecting children or that her goal of protecting children would be unavailable without the disclosure.

[para 87] According to the staff sergeant's affidavit, she disclosed the Complainant's last name, his date of birth and the allegations made against him between 1992 and 2006 to an employee of the Complainant's employer in 2013 so that the staff sergeant could determine whether an individual whose name she had come across in the course of an investigation into someone else worked at a particular facility. At the time the staff sergeant disclosed the details of the youth matters and allegations she had reviewed on EPROS, she did not know whether the Complainant worked at the facility. I am there unable to say that the staff sergeant made the disclosure to preserve the public peace or to protect children, as she did not have the necessary information to determine whether the disclosure could possibly have this effect. I am therefore unable to say that the staff sergeant disclosed the Complainant's personal information for the same purpose for which his personal information was originally collected.

[para 88] I note too that the staff sergeant characterized the disclosure to the employee as "kind of an FYI". This email, which is contemporaneous with the disclosure, does not indicate that the staff sergeant anticipated that the Complainant's employer

would or could act on the information she provided. Further, this email does not convey any sense that the Complainant's email information had been disclosed for a "law enforcement" purpose. Rather, it indicates that it had been disclosed for the employee's information.

[para 89] In addition, on February 5, 2013, the staff sergeant reviewed the files on which the EPROS notations were based to determine whether there was a duty to warn the Complainant's employer. From this action, I conclude that there was a process in place at the Public Body for determining whether there existed a duty to warn an employer. However, the initial disclosure to the employee was made prior to reviewing the records to determine whether there was a duty to warn the Complainant's employer.

[para 90] While the Public Body argues that the review for the duty to warn was limited only to whether there was a duty to warn regarding additional information in the files, I am unable to accept this argument. The additional information in the files would have assisted the staff sergeant to decide whether the Complainant was the subject of false allegations, whether he had "skirted the system", or whether the truth was likely to be something other than these two possibilities. The staff sergeant stated in her affidavit, "[g]enerally, EPROS does not provide detailed information (i.e. written report) for files created prior to 2008".

[para 91] Had the staff sergeant reviewed the files prior to making the disclosure to the Complainant's employer, she might have concluded, based on the detailed information in the files, that there was no duty to warn the employer. If there was no duty to warn the employer, making the disclosure could not serve the purposes of keeping the peace and protecting children.

[para 92] That the staff sergeant did not have detailed information when she made the disclosure is highlighted by her email in which she indicated that she did not know whether the Complainant had multiple false allegations made against him or had been able to "skirt" the system on convictions. In essence, the staff sergeant made the disclosure at a time when did not know whether the Complainant worked at the facility, and did not know whether her theories regarding his lack of a criminal record were true. Disclosing the allegations regarding the Complainant to the employee in order to determine whether he was the same person she had read about on EPROS was clearly unnecessary. This information could have been gained for the purpose of determining whether there was a duty to warn by providing only the Complainant's name and birthdate (to someone with authority to collect that information and disclose whether the Complainant worked there) and then following the process for determining whether there was a duty to warn described in her affidavit.

[para 93] Moreover, given the fact that the staff sergeant did not know at the time of disclosure whether the allegations she disclosed were false or true, and given that there was a process in place for determining whether there was substance to the allegations that would create a duty to warn the employer, which she did not follow when making the disclosure, I find that the disclosure of the allegations to the employee was unnecessary

and did not meet the terms of section 41(b). As a consequence, I find the disclosure to the employee of the Complainant's employer was not authorized by section 40(1)(c).

The two youth matters

[para 94] If I am wrong in reaching the above conclusions, it is necessary to address the two youth matters that were also disclosed to the employee. As noted above, the staff sergeant disclosed information regarding matters taking place in 1992 and 1995. The Complainant was a youth within the terms of the *Youth Criminal Justice Act*, S.C. 2002, c. 1(YCJA) at the time of these matters. Section 115 of YCJA authorizes police services to keep records of youth offences. It states:

> *115 (1) A record relating to any offence alleged to have been committed by a young person, including the original or a copy of any fingerprints or photographs of the young person, may be kept by any police force responsible for or participating in the investigation of the offence.*

[para 95] Section 118 of the YCJA states:

> *118 (1) Except as authorized or required by this Act, no person shall be given access to a record kept under sections 114 to 116, and no information contained in it may be given to any person, where to do so would identify the young person to whom it relates as a young person dealt with under this Act.* [My emphasis]

[para 96] Section 138 of the YCJA states:

> *138 (1) Every person who contravenes subsection 110(1) (identity of offender not to be published), 111(1) (identity of victim or witness not to be published), 118(1) (no access to records unless authorized)* [my emphasis] *or 128(3) (disposal of R.C.M.P. records) or section 129 (no subsequent disclosure) of this Act, or subsection 38(1) (identity not to be published), (1.12) (no subsequent disclosure), (1.14) (no subsequent disclosure by school) or (1.15) (information to be kept separate), 45(2) (destruction of records) or 46(1) (prohibition against disclosure) of the Young Offenders Act, chapter Y-1 of the Revised Statutes of Canada, 1985,*
>
> > *(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or*
> >
> > *(b) is guilty of an offence punishable on summary conviction.*

[para 97] Under section 118 of the YCJA, it is an indictable offence to provide information about a youth matter in police files to someone other than the youth, except in accordance with sections 114 – 116 of that Act. The YCJA does not contemplate disclosure of a youth's information in the circumstances the information was disclosed to the employee. In this case, the staff sergeant provided information about two youth matters to an employee of the Complainant's employer, the employee's supervisor, and

then a senior manager. She identified the Complainant to his employer as the youth who was the subject of two youth matters.

[para 98] As noted above, section 41 of the FOIP Act establishes that a purpose for disclosing personal information will be consistent if it has a reasonable and direct connection to the purpose in collecting the information and is necessary for performing the statutory duties of, or for operating a legally authorized program of the Public Body.

[para 99] The personal information was originally collected in the course of investigations regarding youth matters. Given the restrictions contained in the YCJA (and the former *Young Offenders Act)* regarding disclosure of such information, I do not believe that the information collected under these schemes could be disclosed to an employee "as an FYI" or for general policing purposes and be consistent with the purpose for which it was collected because of the restrictions on disclosure in the YCJA. In other words, the disclosure in the circumstances of this case is necessarily inconsistent with collecting information in order to investigate a youth matter within the legislative framework of the YCJA. Moreover, I do not accept that disclosing the Complainant's youth information was necessary for the purposes of performing the Public Body's statutory duties, given that doing so is not in accordance with its statutory duties under federal legislation.

[para 100] For the foregoing reasons, I find that the disclosures made by the staff sergeant on January 4, 2013 were not made for a purpose consistent with the Public Body's purpose in collecting the Complainant's personal information. As a result I find that section 40(1)(c) (and the other provisions of section 40) does not authorize the disclosure made by the staff sergeant to the Complainant's employer.

Section 40(1)(e)

[para 101] Section 40(1)(e) states:

> *40(1) A public body may disclose personal information only*
>
> > *(e) for the purpose of complying with an enactment of Alberta or Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada,*

[para 102] The Public Body argues in its initial submissions dated January 13, 2017:

> Section 40(1)(e) of the FOIPP act states that a public body may disclose personal information for the purpose of complying with an enactment of Alberta.
>
> The EPS had the authority to disclose the Complainant's personal information as the disclosure was for the purpose of complying with the *Police Act*, an enactment of Alberta.
>
> As set out above, the *Police Act* requires that the EPS preserve and maintain the public peace and prevent crimes. In appropriate circumstances, such as this one, these duties are fulfilled by disclosing information which acts as a warning to other public bodies or individuals.

> As also addressed above, the disclosure was made for the purpose of preserving the peace and maintaining the safety of children at [the facility], which is in compliance with the purpose of the *Police Act*.

[para 103] As detailed in my discussion of section 40(1)(c), the evidence establishes that the disclosure to the employee was made before the staff sergeant learned that the Complainant worked at the facility and was the same person she had read about in EPROS. Moreover, the disclosure was based on non-detailed historic information, and was made without determining whether the allegations recorded in EPROS were likely to be true or false or had any bearing on the Complainant's employment. When the staff sergeant reviewed detailed information that could potentially answer the question of whether the allegations were false, it was decided there was no duty to warn the employer regarding the substance of the allegations. I am therefore unable to find that the disclosure to the employee was made for the purpose of preserving the peace or maintaining the safety of children, as the staff sergeant simply did not have the necessary information to determine that the disclosure could serve this purpose when she made it.

Section 40(1)(i)

[para 104] Section 40(1)(i) states:

> *40(1) A public body may disclose personal information only*
>
> > *(i) to an officer or employee of a public body or to a member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed,*

[para 105] The Public Body argues that the Zebra Centre is a common or integrated program or service that brings public bodies (such as the Complainant's employer) "under one roof that are all committed to the same goal: providing a child-focused, child-friendly environment to nurture and protect abused children. The Zebra Centre's priorities are a child's wellbeing and finding truth and justice".

[para 106] The Public Body states in its initial submission of January 13, 2017:

> At the Zebra Centre there is joint planning between the various agencies and collaboration and coordination to deliver the common objective. Each agency names a liaison to work with the Chief Executive Officer and the Board of Directors, members of the agencies volunteer for the Board of Directors, and each agency participates in the governance and the management of operations.
>
> The level of collaboration between EPS Child Protection Section and [the Complainant's employer] at the Zebra Centre is particularly high as individuals from each agency work together in a case management model.

> The Zebra Centre is a single program or service that is provided or delivered by two or more public bodies.
>
> […]
>
> [The staff sergeant] disclosed the Complainant's personal information to [the employee], [the employee's manager], and [the senior manager], all of whom are employees of [the Complainant's employer] and who were involved with the Zebra Centre. She did not disclose the Complainant's information to anyone else.
>
> Accordingly, the disclosure was to an employee of another public body.
>
> The disclosure was necessary in order to further the Zebra Centre's objectives. It was also necessary in order for [the employee], [the employee's supervisor] and [the senior manager] to perform their duties at the Zebra Centre.

[para 107] On July 19, 2017, I asked the Public Body:

> Why was the information provided to [the employee]?
>
> What authority did the Public Body understand [the employee] to have to address the information it provided to her?

[para 108] In its submissions of September 11, 2017, the Public Body referred me to the staff sergeant's affidavit of January 12, 2017. It noted:

> [The staff sergeant] determined it was necessary to disclose this information to [the Complainant's employer] so that [the employer] could assess whether to take any steps with respect to the information provided. She understood that [the employee] would be in a good position to address the information since [the employee] had previously worked on investigations.

[para 109] I accept that the Public Body and other public bodies provide integrated services through the Zebra Centre. However, it has not been established in the evidence before me that the facility in which the Complainant worked was an integrated service provided through the Zebra Centre or that the Zebra Centre had any role in determining who the Complainant's employer, a provincial ministry, could hire or keep on staff. The Complainant was not an employee of the Zebra Centre.

[para 110] While some employees of the Complainant's employer may provide integrated services through the Zebra Centre, it does not follow that all aspects of the Complainant's employer's functions, such as labour relations, are offered through Zebra Centre or governed by participation at the Zebra Centre, or that an employee who provides services through the Zebra Centre would have any authority to address matters in the Government of Alberta, unrelated to the Zebra Centre.

[para 111] There is no evidence before me that the employee to whom the staff sergeant provided the information regarding the youth matters and allegations had any authority to investigate these matters and allegations, any authority to investigate the employees at the facility where the Complainant worked, or to determine whether the

Complainant was suitable as an employee of the Government of Alberta. I note that once the senior manager met with the staff sergeant to discuss the allegations made against the Complainant, that the employee to whom the information was originally provided was no longer included or copied regarding discussions of the Complainant by the employer. This also suggests that it was not part of the employee's function to investigate the Complainant's suitability for employment in the Government of Alberta.

[para 112] Finally, I note that the Complainant's employer required a PIC / VSC to be provided to it containing the information the staff sergeant had provided to the employee and the senior manager before the employer would act on the information. This circumstance argues against finding that it was necessary for the employee and the senior manager to receive the Complainant's personal information from the staff sergeant, given that the employer still required the information despite the fact that the staff sergeant had communicated it to the employee and the senior manager.

[para 113] As the powers and functions of the employee to whom the staff sergeant disclosed the Complainant's personal information have not been established for this inquiry, and as it has not been established that the Zebra Centre had any oversight over the Complainant's employment, I am unable to say that the disclosure was necessary for the delivery of the Zebra Centre's programs, or that it was necessary for the employee to perform her duties.

[para 114] For the foregoing reasons, I find that it has not been established that section 40(1)(i) authorizes the disclosure of the Complainant's personal information to the employee on January 4, 2013.

Section 40(1)(ee)

[para 115] Section 40(1)(ee) states:

> *40(1) A public body may disclose personal information only*
>
> > *(ee) <u>if the head of the public body believes</u>, on reasonable grounds, that the disclosure will avert or minimize* [my emphasis]
> >
> > > *(i) a risk of harm to the health or safety of a minor, or*
> >
> > > *(ii) an imminent danger to the health or safety of any person […]*

[para 116] In its submissions, the Public Body did not address the condition in section 40(1)(ee) that *the head of the public body* must first believe, on reasonable grounds, that the disclosure will avert or minimize the risk of harm or safety of a minor, or an imminent danger to the health or safety of any person. The Public Body did not provide evidence for the inquiry to establish that the Chief of Police determined that the disclosure would have this effect or delegated to the staff sergeant the authority to make this determination. Rather, the evidence before me, as discussed in relation to the

application of section 40(1)(c), above, that the staff sergeant disclosed the information about historical allegations made against the Complainant without determining whether the disclosure would serve to protect minors in circumstances where it was open to her to take steps to verify whether the disclosure would serve this purpose by reviewing the files to determine whether there was a duty to warn the employer, prior to making it.

[para 117] For this reason, I find that section 40(1)(ee) did not authorize the staff sergeant's disclosure of the Complainant's personal information.

Conclusion

[para 118] For the reasons above, I find that the disclosures made by the staff sergeant on January 4, 2013 were not authorized by a provision section 40 of the FOIP Act. I must therefore require the Public Body not to disclose the Complainant's personal information in contravention of the FOIP Act.

IV. ORDER

[para 119] I make this Order under section 72 of the Act.

[para 120] I require the Public Body not to use the Complainant's personal information in contravention of Part 2 of the Act.

[para 121] I require the Public Body not to disclose the Complainant's personal information in contravention of Part 2 of the Act.

[para 122] I require the Public Body to notify me and the Complainant within fifty days of receiving this order that it will comply with it.

_____
Teresa Cunningham
Adjudicator