Office of the Information and Privacy Commissioner for Nova Scotia
Report of the Commissioner (Review Officer)
Catherine Tully

REVIEW REPORT 16-14

December 6, 2016

Department of Justice

Summary: Government departments collect substantial amounts of personal information on citizens. They employ staff who are trusted to access this personal information so the staff can do their jobs. But staff are not given access rights to databases of personal information so they can satisfy their curiosity. Any staff access to personal information must be authorized by the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*). In this case, the Commissioner finds that a number of correctional officers accessed the personal information of the complainant in a workplace database out of curiosity. The Department of Justice (Department) failed to establish that the officers' access to the data was necessary for the work-related duties of the officers. The Commissioner recommends further training.

Information was also accessed by other Department staff as part of an investigation into an alleged improper relationship between the inmate and a correctional officer. In those instances, the Commissioner noted that a Department's ability to use personal information in a way that differs from the reasons why it was originally collected is limited by *FOIPOP*. Any additional uses of personal information must be reasonably connected to the purpose for which the information was collected in the first place. The Commissioner considers that the system was intended to ensure that inmates are treated fairly and in accordance with court orders. The system was also used to ensure the safety of other inmates, staff and the public. The Commissioner finds that an investigation into an improper relationship between an inmate and a correctional officer was directly related to ensuring that the inmate would be treated fairly in any future involvement with the facility, and that the facility remained safe. As a result, the Commissioner finds that the Department was authorized to use the complainant's personal information to complete the investigation.

Statutes Considered: *Correctional Services Act*, SNS 2005, c 37, ss. 20, 21, 39; *Correctional Services Regulations*, NS Reg 99/2006, s.17; *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25, s. 41; *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, s. 34; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5, ss. 26, 34-41, 45; *Privacy Review Officer Act*, SNS 2008, c 42, ss. 5, 6.

Authorities Considered: **Alberta**: Orders F2010-014, 2011 CanLII 96622 (AB OIPC); F2015-27, 2015 CanLII 77917 (AB OIPC); **British Columbia:** Orders F07-10, 2007 CanLII 30395 (BC IPC); F2015-27, 2013 BCIPC 4 (CanLII); **Nova Scotia**: Review Report 16-06, 2016 NSOIPC 6 (CanLII); Ontario: Investigation Report I93-009M, 1993 CanLII 4934 (ON IPC).

Other Sources Considered: British Columbia FOIPPA Policies and Procedures Manual, s. 32: http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/use-personal-information; Correctional Services Policy & Procedure, Subject No. 5.00.00, Investigations s. 6.1.1.; Service Alberta FOIP Guidelines and Practices: http://www.servicealberta.ca/foip/documents/chapter7.pdf.

INTRODUCTION:

[1] The complainant, a former inmate at a correctional facility, complained that employees of the facility had been accessing data about him in the Justice Enterprise Information Network (JEIN) after he was no longer incarcerated. The complainant believed that this was a violation of his privacy rights under the *Freedom of Information and Protection of Privacy Act*.

ISSUE:

[2] Was the use of the complainant's personal information in the Justice Enterprise Information Network between June 13, 2011 and August 8, 2012 authorized under s. 26 of the *Freedom of Information and Protection of Privacy Act*?

DISCUSSION:

Background

[3] In June 2011 the complainant was released from a correctional facility in Nova Scotia. He never returned to that facility. However, three months later, as a result of information he received in a court hearing, the complainant became convinced that a correctional officer had accessed information about him in the JEIN system even though he was no longer incarcerated in the local facility. He complained directly to the superintendent of the facility who advised that he should put his complaint in writing.

[4] In November 2011 the complainant filed an access to information request. He requested in particular access to a list of any person who had accessed his personal information in the JEIN system. The JEIN system is one of the main systems used by adult correctional facilities in Nova Scotia.

[5] On August 8, 2012, after reviewing information he received in response to his access to information request, the complainant filed a privacy complaint with the Department of Justice. His complaint was that staff at one particular correctional facility (facility) had accessed his record in JEIN after he was no longer in custody at the facility and that such access was therefore not authorized under the *Freedom of Information and Protection of Privacy Act*. A table supplied to the complainant in response to his access to information request summarized access

to his record in JEIN by Correctional Services staff. The table did not specify who accessed the information or what part of Correctional Services they worked in.

[6] The focus of the privacy complaint was on the time period between June 13, 2011 and August 8, 2012 and related only to access to the record by staff located in one particular correctional facility.

[7] In response to the complaint, the Department produced a new JEIN audit report for the relevant time period and identified eight staff members from the correctional facility who it said accessed the complainant's personal information in JEIN during the 14 month period in question. In October 2012 the Department assigned two investigators to conduct an internal investigation into the alleged privacy breach. The investigators interviewed each of the individuals identified as having accessed the complaint's JEIN record between June 13, 2011 and August 8, 2012.

[8] The Department's interview notes indicate that individuals were not specifically asked about access to the JEIN record during the time after the complainant left the custody of the correctional facility. Rather, the question posed to each was "Have you ever accessed the JEIN file of [the complainant]?" Each individual was also asked the reason for his or her access to the JEIN file and whether he or she shared the information with anyone. The investigation report does not analyze whether or not the statements of the eight employees are accurate or supported by the system audit report.

[9] The investigators' report summarizes the responses of each employee and concludes that there was no evidence to indicate that any correctional facility employees disclosed information obtained through JEIN records to any person outside of the Department of Justice. The only apparent source of evidence with respect to disclosures of information was that investigators asked each person if he or she had further disclosed personal information and each responded that he or she had not. The investigators made no finding or conclusion as to whether or not the accesses to the system were authorized.

[10] On December 19, 2012 the information access and privacy administrator (IAP administrator) wrote to the complainant and advised, "We have determined that your privacy was not breached. There was no unauthorized access of your personal information…the staff at [correctional facility] who accessed your personal information when you were not in custody did so in the course of their duties." The IAP administrator also advised the complainant that the two individuals he believed had specifically accessed his personal information in JEIN did not access the complainant's JEIN account at all during the 14 month period at issue.

[11] On February 2, 2013 the complainant filed a request for review of his privacy complaint with this office. He asked us to investigate his complaint that staff at the facility had accessed his personal information in JEIN when he was no longer in custody. He was concerned that staff had accessed his current street address and were looking at where he worked. He believed the access was unauthorized because he was no longer in custody at the correctional facility and had not been in custody at that facility since June 13, 2011.

Privacy complaint procedure

[12] It is the *Privacy Review Officer Act* (*PRO*) that sets out the oversight powers of this office and the rights of individuals to file a complaint where they believe their privacy rights have been violated. *PRO* requires that individuals first bring their complaints to the attention of the public body to give the public body an opportunity to respond.[1] If the matter does not resolve following the use of the internal privacy complaint procedure of the public body, then the Commissioner, as Privacy Review Officer, may conduct a review of the privacy complaint. The process to be followed in the formal review is the same process as is used to conduct reviews of a decision of a public body in response to an access to information request.[2]

Burden of proof

[13] Section 45(1) of *FOIPOP* sets out the burden of proof. However, the provisions of *FOIPOP* adopted for the purposes of *PRO* do not include s. 45(1).[3] The Notice of Formal Review advised the parties that *FOIPOP* is silent on the issue of burden of proof. In the absence of a statutory burden of proof, there is an evidentiary burden on the person who lodges the complaint. The usual principle of "she who alleges must prove" applies. This is an evidential burden, not a legal burden, and it requires only that the complainant provide sufficient evidence of the alleged collection, use or disclosure of personal information. Such evidence may be satisfied without doing anything other than pointing to evidence already on the record. Once the evidentiary burden is satisfied, the burden shifts to the public body to establish that it had the authority for the collection, use or disclosure at issue.[4]

Investigation process

[14] In conducting our review of this complaint we gathered information from the complainant regarding the basis for his belief that access to his JEIN record was unauthorized. He supplied us with copies of documents he received in the response to his access to information request that he believed supported his contention that unauthorized access was occurring. We also obtained copies of:

- the Department's system detailed audit report;
- the Department's investigation report from the fall of 2012 (including interview notes);
- the Department's privacy breach report including internal emails regarding the investigation;
- relevant policies and legislation;
- a list of all of the complainant's court dates between June 13, 2011 and August 8, 2012;
- a list of the all of the complainant's incarceration dates between June 13, 2011 and August 8, 2012.

---

[1] *Privacy Review Officer Act* (*PRO)* s.5(2).

[2] *PRO* s. 6(2).

[3] Section 6(2) of *PRO* provides that ss. 34 to 41 of the *Freedom of Information and Protection of Privacy Act*, and related provision in that *Act*, apply mutatis mutandis to a review under *PRO*.

[4] This approach in privacy complaint matters is consistent with, for example, BC OIPC Order F13-04 at para 5. This approach is also consistent with the approach in Alberta. See for example Alberta OIPC Order F2010-014 at paras 5-7.

[15] In addition, we conducted in-person interviews of the facility superintendent, a director of Correctional Services and the IAP administrator for the Department.

Was the use of the complainant's personal information in the Justice Enterprise Information Network between June 13, 2011 and August 8, 2012 authorized under s. 26 of the *Freedom of Information and Protection of Privacy Act*?

[16] The first issue in any privacy complaint is whether or not any "personal information" within the meaning of *FOIPOP* is involved. It is s. 3(1) of *FOIPOP* that sets out the definition of personal information.

[17] The Department concedes that the audit report completed in response to this complaint confirms that eight employees of the correctional facility accessed the complainant's personal information in JEIN between June 13, 2011 and August 8, 2012. The audit report does not identify exactly what type of personal information was accessed but in general, the information available in JEIN includes such things as name, date of birth, physical description, charges, appearance dates, outcomes, and conditions for release. I agree with the Department and the complainant that this information qualifies as personal information within the meaning of *FOIPOP*. Therefore the only issue is whether or not the access by each of the eight individuals was authorized under *FOIPOP*.

[18] Access to personal information within a Department's computer system by a Department employee authorized to view and use data within the system is a use of personal information for the purposes of *FOIPOP*.[5]

[19] Section 26 of *FOIPOP* governs use of personal information:

> 26 A public body may use personal information only
>
> (a) for the purpose for which that information was obtain or compiled, or for a use compatible with that purpose;
>
> (b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use; or
>
> (c) for the purpose for which that information may be disclosed to that public body pursuant to sections 27 to 30.

[5] See NS Review Report 16-06 at paras 19-23 for a discussion of why accessing data within a database in these circumstances is a use for the purposes of *FOIPOP*. I have adopted that reasoning here.

[20] In its initial response to the complainant's privacy complaint the Department simply stated that the access was authorized because it was done in the course of the duties the individuals who had accessed the relevant JEIN records. In response to the Notice of Formal Review, the Department provided more detail on the authority it says these individuals had to access the information. The Department provides three reasons for why the eight individuals accessed the complainant's JEIN record during the 14 month time period at issue:

1. to supervise the complainant in custody;
2. for the purpose of planning for the housing of the complainant, taking into account in particular conflicts involving two staff members; and
3. to investigate one of its staff for an inappropriate relationship with the complainant.

[21] Further, the Department argues that these three uses were authorized under s. 26(a) and 26(c) of *FOIPOP*.

[22] While the Department did not identify which users were accessing the data for which reasons, the eight employees themselves identified the purposes for their accesses when they were interviewed in October 2012. In addition to the reasons provided by the Department in its submissions, witnesses also stated that they looked at the record out of curiosity, for training purposes, and in response to requests by their superiors.

[23] In the interview by Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) investigators the superintendent of the correctional facility and a director of Correctional Services confirmed that the purpose for access to the JEIN system in this case was related to an investigation of a staff member and to plan for the housing of the complainant, taking into account particular conflicts involving two staff members.

Scope of access

[24] The audit report lists all accesses to the complainant's JEIN record during the relevant time period. On some days more than one person accessed the record, and sometimes one person accessed the record multiple times in one day. Where there is a very short time period between the accesses the Department explained that this indicated the user was simply switching between screens. Sometimes the timing between the accesses by one user on one day is such that it is clear that there was more than one access session. For example, one user accessed five screens on one day. Two screens at 11:17 a.m. and 11:19 a.m., two further screens at 12:44 p.m. and 12:45 p.m. and one screen at 2:38 p.m. I considered this to constitute three access sessions.

[25] Using this method, I determined that the eight different users from the facility engaged in 42 separate access sessions (involving 72 screens) during the time period in question.[6]

1. Was the use authorized as an original use purpose under s. 26(a)?

[26] In accordance with s. 26(a), a public body may use personal information for the purpose for which it was obtained or compiled or for a use compatible with that purpose. The

[6] I will provide the Department with my breakdown of the number of accesses by each identified user so that the Department can fully understand the findings contained in this report as they apply to individual employees.

Department states that when the information in this case was used as part of planning for the housing of the complainant, such use was for the reason the information was compiled. The Department points out that some of the information was accessed because the complainant had to have special custody arrangements in place because of his involvement with two employees.

[27] Witnesses for the Department stated that JEIN is a case management system inside Correctional Services. It manages an offender from first entry, through courts and probation. Access is compartmentalized by role.

[28] In previous Review Report 16-06 I reviewed the purposes for the JEIN system and concluded that the original purposes for the JEIN system are all in relation to the criminal justice system and include:

- integrated criminal case management,
- case management for court proceedings,
- management of offenders either in a facility setting or on some sort of community supervision,
- prisoner tracking,
- information management, and
- records management.[7]

[29] Clearly one of the purposes for gathering information about offenders is to manage them within a facility setting. I accept that any access by the eight employees that is directly related to and necessary for planning for the housing of the complainant is an original use and one authorized by s. 26(a) of *FOIPOP*.

Correctional officers– 18 access sessions

[30] As noted above, the Department cited three reasons for access to the complainant's JEIN record:

1. to supervise the complainant in custody;
2. for the purpose of planning for the housing of the complainant, taking into account in particular conflicts involving two staff members; and
3. to investigate one of its staff for an inappropriate relationship with the complainant.

[31] According to the evidence provided, correctional officers were only authorized to access the JEIN system for the purpose of planning for the housing of offenders or for supervising them when they are in custody. Supervision purposes were not relevant in this case because the complainant was not in custody during the time period in question. The Department provided no evidence that correctional officers were tasked with assisting with any investigation of other employees in this case.

[7] NS Review Report 16-06 at para 38.

[32] Therefore, the only possible authority for access to the JEIN record by correctional officers during the time period in question was for the purpose of planning for the housing of the complainant.

[33] The correctional officers were each interviewed and all identified their authority for accessing the complainant's JEIN record as planning for the housing of the complainant. One correctional officer admitted to being curious; several mentioned an interest in the conflict the complainant had with staff of the facility.

[34] Based on the evidence provided, correctional officers accessed the complainant's JEIN record a total of 18 times[8] between June 13, 2011 and August 8, 2012.

[35] With respect to planning for housing of inmates, the superintendent explained that the process involves first looking at the court docket via JEIN to see who is listed for an appearance on any given day. The court docket is in a different area of JEIN and does not form part of an individual's JEIN record. If staff require more information about an individual listed on a docket they must then access that individual's JEIN record. It is only when they take this second step that they are able to access more detailed information about the nature of the case and any conditions regarding release or imprisonment. In addition, in this case, it was only when staff accessed the complainant's JEIN record using this second step that the access appeared in the JEIN audit that revealed the 18 access sessions by correctional officers during the 18 month period.

[36] The superintendent explained that because the correctional facility is so small, the docket planning is shared among all staff. Correctional officers are involved in the planning; they determine if there are any alerts, conflicts, incompatibles or no-contact conditions. These types of circumstances arise when there is a peace bond between inmates or between an inmate and an employee where there is conflict between prisoners (witnesses and co-accused), or where there are family relationships between inmates and staff among, other things. The alert indicates a conflict or non-compatibility that must be properly managed. In a small province with limited staff this is not an unusual issue.

[37] The superintendent acknowledged that generally the plan was to house the complainant in another facility should the complainant be given a period of incarceration. However, there could have been times when this would not be possible due to space constraints and so the plan was to house the complainant in segregation if the need arose. If this were to occur, staff would need to make sure that there was room in segregation and that the correctional officers assigned and available had no conflict with the prisoner. By checking the docket this allowed staff to anticipate this need.

[38] The Department provided us with a list of all of the complainant's court dates during the time period in question (June 13, 2011 to August 8, 2012). The complainant was never housed at the correctional facility in question here during this time period. However, he did have a total of twenty four hearing dates during that time period and one brief incarceration in another facility.

[8] The audit document indicates the 18 access sessions occurred on 14 different days and involved 26 screens.

Given the superintendent's description of the planning process, if the purpose for the access was to plan for housing, then the access for this purpose would occur on the day the complainant appeared on a docket because if a housing need were going to arise, it would be on the hearing day. Further, the superintendent indicated that when correctional officers accessed this information they did so because they "needed to plan their day."

[39] When the complainant appeared on a docket it would be necessary to access the record specific to the complainant to determine if there were any incompatibilities and to determine if it appeared likely that the complainant would need to be housed in the facility.

[40] Of the 18 accesses by correctional officers only five occurred on the complainant's court appearance dates. One correctional officer, who admitted to also being curious, accessed the complainant's record on 10 different days and only one of those dates coincided with a hearing date. Four access sessions occurred on that date. Others looked less often. One correctional officer only looked once, at one screen, and only on a scheduled appearance date.

[41] The Department's evidence was that it is also possible that local police or sheriffs could simply show up at the facility with an individual who required temporary placement or they might call ahead with a plan to bring the individual to the institution. In those cases, correctional facility staff would have to look up the individual to determine if there were any incompatibilities that required management. In this case, there was no evidence that the facility received such a call during the time period in question. The complainant was incarcerated at a different facility for six days during the relevant time period but there was no evidence of any requests for placement at the facility in question here. There is no evidence that a need for accommodating the complainant arose on any other date during the 14 months in question.

[42] Based on the evidence before me, I conclude that 13 of the 18 accesses to the complainant's JEIN record by correctional officers were not authorized.[9] The evidence does not support that these 13 access sessions were necessary for the management of housing issues related to the complainant. He had no court appearance scheduled on the access dates and so there was no chance that he would be sent by the court to the facility on that day. There was no evidence that either local police or sheriffs requested that the complainant be temporarily housed in the facility during this time period. Rather, based on the Department's own investigation, the most likely reason for these accesses was curiosity related to the complainant's conflicts with employees of the facility.

[43] Based on the statements taken from the four correctional officers who accessed the complainant's JEIN record, it appears that there is some confusion on what exactly an authorized work-related purpose is. None of the materials supplied to this office regarding the JEIN system provide any detailed explanation or examples of authorized uses of JEIN. While I have found that 13 of 18 accesses to the complainant's JEIN record by correctional officers were not authorized, it is my opinion that the fault lies in the lack of training on this issue.

[9] For clarity, I will provide the Department with a list of the individuals, dates of access and conclusions on authority to access in each individual case.

[44] Therefore, I recommend that the Department prepare a clear guideline setting out authorized uses of JEIN and providing examples of unauthorized uses. Simply stating that it can only be used for work related purposes is insufficient guidance. For example, the guidance should be clear on when an individual no longer in custody may be searched in the JEIN system. Generally, such a search by correctional officers would be authorized if there is reason to believe that the individual is about to be housed at the facility. Such a reasonable belief would arise because the individual is on a court docket or because police or sheriffs have contacted the facility to advise that they are about to deliver the individual to the facility. Obviously the guidance should also be clear that curiosity is not an authorized basis for accessing the JEIN system.

Other staff – 24 access sessions

[45] Twenty four further access sessions[10] occurred during the relevant time period by four other staff. Of the remaining 24 accesses to the complainant's JEIN record, 11 access sessions occurred on an appearance date. For the reasons given above, the evidence supports that accesses on these dates were more likely than not related to concerns regarding the appropriate housing of the complainant. Therefore, I find that the 11 further accesses that coincided with appearance dates were authorized in this case.

2. Was the use authorized as a compatible purpose under s. 26(a)?

[46] Two final explanations were offered for access to the complainant's JEIN record. The Department states that when the information about the complainant was accessed as part of an investigation into a staff member, this was done for a compatible use purpose. One witness indicated that one reason for access was for training purposes.

[47] Section 28 of *FOIPOP* defines what a compatible purpose is.

[48] "Compatible" purpose referred to in s. 26(a) of *FOIPOP* is defined as follows:

> 28 A use of personal information is a use compatible with the purpose for which the information was obtained within the meaning of section 26 or 27 if the use
>
> (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 the information or to which the information is disclosed.

[10] The audit document indicates the 24 access sessions occurred on 19 days and involved 46 screens.

[49] This provision is virtually identical to definitions of "consistent purpose" in the Alberta and British Columbia public sector privacy legislation.[11] The core elements of Nova Scotia's compatible purpose provision are:

> (i) the use must have a reasonable connection to the original purpose,
> (ii) the use must have a direct connection to the original purpose, and
> (iii) the use must be necessary for performing statutory duties of or for operating a legally authorized program of the public body that uses the information.

[50] A use for a compatible purpose then would not be identical to the original intended purpose. If it were, there would be no need to refer to compatible purposes.[12]

[51] The superintendent indicated that an investigation was underway during the time period in question. It was in relation to the nature and extent of the relationship between the complainant and an employee.

[52] The superintendent confirmed that he asked two particular staff members to monitor the complainant's court dates due to the superintendent's investigation into the activities of the staff member. Further evidence supplied by the Department indicated that a third staff member who accessed the complainant's JEIN record was assigned duties in relation to this investigation. The activities of the staff member that were under investigation involved interactions with the complainant. According to the superintendent, there was information relevant to these interactions contained in the complainant's JEIN record. There were 13 accesses to the complainant's JEIN record by the superintendent and the three staff members delegated to assist with the investigation that did not coincide with court dates. Presumably[13] then, some or all of the 13 remaining accesses related to the investigation.

Necessary for performing statutory duties or for operating a legally authorized program

[53] The focus of the Department's submission was on the necessity of the information and its connection to a legally authorized program of the Department. Section 28(b) of *FOIPOP* requires that a compatible use is a use "necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses the information".

[54] Therefore, I will begin my analysis with this factor, keeping in mind that all three elements set out in s. 28 for compatible use must be present for such a use to be authorized.

---

[11] Alberta *Freedom of Information and Protection of Privacy Act* s. 41, British Columbia *Freedom of Information and Protection of Privacy Act* s. 34.

[12] The Office of the Information and Privacy Commissioner for Ontario pointed this out in IPC Investigation I93-0009M at p. 9 "…the Act includes provisions for the use of personal information for a consistent purpose, which would not be identical to the intended purpose for the collection. Our reasons for finding that a use is or is not reasonably compatible with the intended purpose are based on the specific circumstances in each case."

[13] The Department did not provide explanations for the authority for each of the accesses either by date or by staff member. The arguments offered were general.

[55] In its submissions, the Department states that s. 21 of the *Correctional Services Act* gives Correctional Services employees the authority to conduct investigations regarding the delivery of correctional services.

[56] In fact, s. 21 gives only an "inspector" such authority:

> 21(1) An inspector may conduct inspections, investigations and inquiries for the purpose of this Act.

[57] An "inspector" under the *Correctional Services Act* is an individual designated by the minister.[14] No evidence was offered to suggest that any of the eight individuals who accessed the complainant's JEIN record were at any time an inspector for the purposes of s. 21 of the *Correctional Services Act.* In my view, this provision is not relevant to the accesses made to the complainant's JEIN records in this case.

[58] The Department's submissions also point out that s. 17 of the *Correctional Services Act* Regulations sets out the rule requiring employees to maintain proper relationships with offenders. On the basis of these provisions, the Department concludes that in order to investigate and ensure its employees meet the requirements of their employment and that they perform their required duties, Correctional Services must have access to information that it holds that would be relevant to an investigation relating to compliance with the Regulations and the Code of Professional Conduct. While the Department emphasized the need for employee compliance with the Code of Professional Conduct, it did not point to any provision of the Code as being at issue in this case.

[59] The Department goes on to describe the responsibilities of the superintendent and his or her authority to delegate that responsibility as set out in Correctional Services policies and procedures. The superintendent's responsibilities are broad and include ensuring that employees are informed of their duties, obligations and expectations of their conduct, and providing such other correctional services as are required in accordance with the *Correctional Services Act* and Regulations.[15]

[60] The Department provided a copy of policy Subject No. 5.00.00 entitled, "Investigations, Inspections and Audits". That policy states that Correctional Services will conduct its own investigations as well as participate in and facilitate authorized investigations by other departments and agencies. Under the policy, superintendents or their designates are authorized to investigate any incident that appears to solely involve offenders and/or staff.[16]

[61] On the basis of the authorities noted above and cited by the Department, I am satisfied that when the superintendent initiated an investigation into a staff member's compliance with the requirements of s. 17(b) of the regulations he was performing his statutory duties. Likewise,

---

[14] *Correctional Services Act*, s. 20.
[15] *Correctional Services Act*, s. 39.
[16] Correctional Services Policy & Procedure, Subject No. 5.00.00, Investigations s. 6.1.1.

when the superintendent delegated duties relating to this investigation to his staff, they were also engaged in a legally authorized program within the meaning of s. 28(b) of *FOIPOP*.

[62] The remaining question for the first element of a "compatible use" is whether the information in JEIN was necessary for this legally authorized program.

Necessary

[63] Under *FOIPOP* it is appropriate to hold public bodies to a fairly rigorous standard of necessity. I agree with the following criteria with respect to the use of the word "necessary" in *FOIPOP*:[17]

- It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future.
- Nor is it enough that it would be merely convenient to have the information.
- The information need not be indispensable.
- In assessing whether personal information is necessary one considers the sensitivity of the information, the particular purpose for the use, and the amount of personal information used in light of the purpose for use.
- *FOIPOP*'s privacy protection objective is also relevant in assessing necessity, noting that this statutory objective is consistent with the internationally recognized principle of limited use.

[64] The superintendent gave evidence that he had information that a correctional officer had not been truthful about the officer's relationship with the complainant and that significant information directly related to this issue was contained in the complainant's JEIN record. A review of the JEIN record confirmed that the correctional officer had not been truthful and that a significant conflict of interest existed that had serious implications for the safety of staff and inmates at the facility.

[65] The intended use for the information was immediate. It was not merely a convenience to have the information although the information was not indispensable. That is, the superintendent could have conducted further interviews with the correctional officer. The information accessed were terms relating to the complainant's probation. This information is not highly sensitive. Considering all of these factors I conclude that the information accessed was necessary for performing the statutory duties of the superintendent within the meaning of s. 28(b) of *FOIPOP*.

Reasonable and direct connection to the original purpose

[66] The two remaining requirements for a use to be "compatible" is that the new purpose must have a reasonable and direct connection to the original purpose (s. 28(a)).

[67] I noted earlier that the original purpose for the collection of information into the JEIN system includes management of offenders in a facility, prisoner tracking and information management. The complainant's personal information was obtained in the course of his

[17] BC Order F07-10.

interaction with the police, the court system and the criminal justice system and was entered in the JEIN system as part of the tracking of his criminal cases. In my opinion, all of the purposes for the JEIN system were potentially engaged when the complainant's information was originally input into JEIN.

[68] The purpose for the new use of the complainant's personal information was to investigate potential incompatibilities between the complainant and two Correctional Services staff. In part, this information was intended to be used if the complainant ever returned to the facility to make housing arrangement decisions. In addition, the Department argues that the information was relevant to the issue of whether one of the employees was in compliance with behavioural standards set out in the *Correctional Services Act* Regulations.

[69] I have already determined that where the access sessions were directly related to assessing and planning for housing requirements for the complainant, this use was an original purpose use and one authorized under *FOIPOP*.

[70] It is only the second potential use, investigating an employee's behaviour, that requires further analysis as a potential "compatible" use.

[71] Is there a reasonable and direct connection between the original purpose for collection of information into JEIN and the purpose of investigating an employee? In my view, "reasonable" means fair and sensible, suggesting sound judgement. "Direct" suggests a straightforward and clear connection.

[72] The Alberta government's FOIP Guidelines and Practices state that there is a reasonable and direct connection if there is a "logical extension of the original use."[18] Later, the authors state, "A consistent use should grow out of or be derived from the original use; it should not be an unrelated or secondary use of the information, otherwise known as 'function creep.'"[19]

[73] The British Columbia government also has a FOIPPA Policy Manual. That manual does not attempt to define consistent purpose outside of the exact wording of the *Act*, but does give an example of a consistent purpose: program evaluation.[20]

[74] In a recent decision by an adjudicator with the Alberta Office of the Information and Privacy Commissioner, a complainant objected to the use of the Alberta equivalent to the JEIN system for the purposes of confirming that the complainant was being honest about his or her criminal past. In that case, the public body said the purpose of its system was to track offenders and support probation officers, administrative staff, surveillance staff and correctional staff at adult and youth correctional centres. The adjudicator concluded that the public body's purpose of investigating its employee's honesty did not have any reasonable and direct connection to any

[18] Service Alberta FOIP Guidelines and Practices, p. 268 http://www.servicealberta.ca/foip/documents/chapter7.pdf.
[19] Service Alberta FOIP Guidelines and Practices, p. 295 http://www.servicealberta.ca/foip/documents/chapter7.pdf.
[20] British Columbia FOIPPA Policies and Procedures Manual, s. 32 at http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/use-personal-information.

of the purposes for the system.[21] It was significant in that case that the employee was obliged to provide a criminal record check which would itself provide objective evidence of a criminal record. On that basis, the adjudicator concluded that the public body had not provided any satisfactory explanation as to why and how the search of the public body's database could reasonably have been expected to help assess the complainant's honesty. The public body already knew the results of the criminal record check based on objective evidence.

[75] In this case, the Department submits that the purpose of the JEIN system is to be an integrated criminal case management system. Part of being processed through the justice system is that you could be managed by Correctional Services staff in facility settings. The staff in those facilities must meet the standards set in the *Correctional Services Act*, the *Correctional Services Regulations*, and the Correctional Services Code of Conduct if the facility is to remain secure. In essence, the Department argues that one of the core purposes of Correctional Services is to ensure facilities are secure, and as part of that system, the JEIN system likewise serves this purpose.

[76] I am satisfied that as an information management system, JEIN is intended to support the security of the justice system generally and the correctional system in particular. In Review Report 16-01 I concluded that, "The need to investigate correctional employees who report criminal charges is likewise based on the need to maintain the security of the correctional system by ensuring that the correctional workers are suitable for continued employment. I conclude that there is a fair, sensible and straightforward connection between these two purposes."[22]

[77] In this case, the issue was not potential criminal charges against a Correctional Services employee. A witness stated that an employee had failed to accurately report circumstances that created an incompatibility between the employee and the complainant. It was only when viewing the terms of the complainant's request to vary the terms of his release conditions (in the JEIN record) that the correct information was obtained. Witnesses gave evidence that incompatibilities create risks for inmates and staff if not properly managed.

[78] Is there a reasonable and direct connection between such an investigation and the original purposes for which the complainant's information was input into the JEIN system?

[79] I have no hesitation in concluding that there was a direct connection between the investigation in this case and the original purpose for the collection of the complainant's information into the JEIN system. In both instances, the purposes were to ensure the safety of inmates and employees, to say nothing of the public. Information gathered about the complainant in JEIN was intended both for his benefit in the sense of ensuring that he was treated fairly and in accordance with the orders of the court. But information was also gathered about the complainant in JEIN for the purpose of ensuring the safety of other inmates, staff and the public. The investigation into a correctional officer's relationship with the complainant was directly related to ensuring that the facility remained safe. That is why there is a provision in the *Correctional Services Act* Regulations specifically prohibiting relationships between inmates and

[21] Alberta Order F2015-27 at para 31.
[22] NS Review Report 16-06 at para 55.

ex-offenders. Such relationships compromise the employee's integrity and endanger the operation of the facility.

[80] Is there a reasonable connection between the two purposes? I find that there is. The information regarding the terms of the complainant's probation is maintained in JEIN to ensure that the conditions are complied with, but the conditions are imposed in the first place in part, to ensure the safety of the public. Where that information creates a new risk directly related to the safe operation of a correctional facility, I am satisfied that there is a fair and sensible connection between the original purpose for the collection and the new use in this case.

[81] I find that the use of the complainant's personal information in JEIN to investigate a correctional officer's compliance with the *Correctional Services Act* Regulation s. 17 was an authorized use pursuant to s. 26(a) of *FOIPOP*.

[82] I have two outstanding concerns regarding the use of JEIN information for the purpose of investigating correctional staff. According to policy Subject No. 5.00.00, all investigations will produce reports for the person authorizing the investigation. In this case, no investigation report was offered in evidence. It is unclear whether such a report exists or not. The policy itself makes clear that investigations will be guided and constrained by applicable legislation and policy and procedures on access and disclosure of information.

[83] On that basis, in order to ensure that all investigations are properly authorized and the reasons for the investigation are clearly delineated, I recommend that any investigation that involves access to JEIN for a "compatible purpose" as set out in s. 28 of *FOIPOP* should always result in a written report as set out in s. 10.1 of Correctional Services Policy & Procedures Subject No. 5.00.00.

Other purposes – training

[84] One staff member indicated that his or her access was also for the purposes of training because this staff member had the complainant's person number memorized. While the staff member does not elaborate on the exact training purpose, in the context it appears that the staff member's duties included training new and existing staff on the functionality of JEIN. This staff member was using live data for the purposes of this training. As with any other use, to be authorized, it must comply with the requirements of s. 26 of *FOIPOP*.

[85] Training was not the original purpose for the collection of the complainant's personal information in JEIN. Training is therefore a secondary use. To be an authorized use, it must therefore satisfy the three requirements of "compatible" purpose set out in s. 28 of *FOIPOP*.

[86] While training staff on the use of a system would clearly be a legally authorized program of the Department, in the absence of any evidence to the contrary, using live data to conduct training does not have a reasonable and direct connection to the original purpose for the collection of the complainant's data in JEIN. Further, use of live data for training is not necessary. It is a straightforward and commonly used strategy to develop dummy data for the purposes of conducting training.

[87] I find that any access of the complainant's JEIN data for the purposes of training was not an authorized use.

[88] I recommend that the Department cease the use of live data when training staff. If a training module does not already exist, I recommend that the Department develop a training module in JEIN made up entirely of dummy data.

Section 26(c) – Use for a purpose for which information may be disclosed

[89] The Department argues that the accesses to the complainant's information was also authorized by s. 26(c) of *FOIPOP*. The Department states that s. 26(c) authorizes the use because, "the access occurred as the result of obligations it has through Correctional Services legislation, policy and regulations in accordance with 26(c) of FOIPOP." It appears then that the Department believes that because it has a statutory basis for its programs that somehow this constitutes an authority to use personal information pursuant to s. 26(c) of *FOIPOP*. This is not the case.

[90] Section 26(c) is a provision added to access laws in order to allow public bodies who collect information from other public bodies to use that information only for the purpose it was originally disclosed. For example, public body #1 is involved in a court case and uses a subpoena to obtain personal information from public body #2. Public body #2 is authorized to disclose the information because s. 27(e) of *FOIPOP* authorizes disclosures for the purpose of complying with a subpoena. Public body #1 is then authorized to use the information it obtained only for its court case because s. 26(c) authorizes a use for the purpose the information was originally disclosed under s. 27.

[91] There was no evidence or argument that a disclosure authorized under s. 27 took place in this case. Therefore, s. 26(c) is not relevant and does not authorize any of the accesses that occurred.

FINDINGS & RECOMMENDATIONS:

[92] I find that:

1. There were 13 unauthorized accesses to the complainant's JEIN record by correctional officers that occurred on days when he did not have a court appearance. These accesses were not authorized under s. 26 of *FOIPOP*.
2. There were 16 authorized accesses to the complainant's JEIN record that occurred when he did have a court appearance schedule on the date the record was accessed. These accesses were authorized under s. 26(a) of *FOIPOP*.
3. The use of the complainant's personal information in JEIN to investigate a correctional officer's compliance with the *Correctional Services Act* Regulation s. 17 was an authorized use pursuant to s. 26(a) of *FOIPOP*.
4. Any access of the complainant's JEIN data for the purposes of training was not an authorized use under s. 26 of *FOIPOP*.

[93] I recommend that:

1. The Department prepare a clear guideline setting out authorized and unauthorized uses of JEIN. Pursuant to s. 5(1)(f) of the *Privacy Review Officer Act* the Department can consult with OIPC in the development of this guideline.
2. Any investigation that involves access to JEIN for a "compatible purpose" as set out in s. 28 of *FOIPOP* should always result in a written report as required by s. 10.1 of Correctional Services Policy & Procedures Subject No. 5.00.00.
3. The Department cease the use of live data when training staff. If a training module does not already exist, I recommend that the Department develop a training module in JEIN made up entirely of dummy data.

December 6, 2016

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

P-13-01