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

REVIEW REPORT 16-06

July 11, 2016

Department of Justice

Summary: The applicant complained that his employer, the Department of Justice (Department), accessed information regarding criminal charges against him in the Department's own computer system and so violated his privacy rights. The Commissioner determines that the access was necessary for the purposes of maintaining the security of the correctional system. Therefore, in the narrow circumstances of this case, the new use of the data by the Department was authorized.

Statutes Considered: *Correctional Services Act*, SNS 2005, c 37, ss. 5, 6; *Correctional Services Regulations*, NS Reg 99/2006, ss. 5, 8; *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. 3, 24, 26, 27, 28, 45*; Privacy Review Officer Act*, SNS 2008, c 42, ss. 5, 6.

Authorities Considered: Alberta: Orders 2000-002, 2000 CanLII 28694 (AB OIPC); F2010-014, 2011 CanLII 96622 (AB OIPC); F2015-27, 2015 CanLII 77917 (AB OIPC); **British Columbia:** Orders F07-10, 2007 CanLII 30395 (BC IPC); F13-04, 2013 BCIPC 4 (CanLII); **Ontario:** Investigation Report I93-009M, 1993 CanLII 4934 (ON IPC).

Other Sources Considered: British Columbia FOIPPA Policies and Procedures Manual, Section 32 - Use of Personal Information, Last updated: July 20, 2007: http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/use-personal-information; *Concise Oxford English Dictionary* (New York: Oxford University Press, 2011), "access", "collection", "use"; Deloitte, Report on Nova Scotia's Adult Correctional Facilities, Nova Scotia Department of Justice, October 29, 2008: https://www.novascotia.ca/just/global_docs/Deloitte%20Report%20-%20NS%20Correctional%20Facilities%20Nov08.pdf; Nova Scotia, "Nunn Commission of Inquiry: Spiralling out of control: lessons learned from a boy in trouble: Report of the Nunn Commission of Inquiry." The Honourable D. Merlin Nunn, Retired Justice of the Supreme Court of Nova Scotia, Commissioner, December 2006: http://novascotia.ca/just/nunn_commission/_docs/Report_Nunn_Final.pdf; Service Alberta FOIP Guidelines and Practices (2009), Chapter 7 - Protection of Privacy: http://www.servicealberta.ca/foip/documents/chapter7.pdf.

INTRODUCTION:

[1] The applicant is a former employee of the Department of Justice (Department). In June of 2010 he made an access to information request for records about him held by his employer. The records were in relation to an investigation into his conduct which eventually lead to his dismissal. Contained in the response to his access request were documents that related to the prosecution of a charge that was laid against him. He objected to the collection of records relating to the prosecution because he said all of the proceedings had not concluded at the time of the Department's investigation. He filed a privacy complaint with the Department. In a follow up conversation with the Department, the applicant focussed his concerns on the use of the Justice Enterprise Information Network (JEIN) to gather information about the criminal charges against him. In response to the complaint the Department stated that the access to information from the JEIN system in the course of the investigation was authorized under the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*). The applicant disagreed and filed a request for review with this office.

ISSUES:

[2] There are four issues under review:

1. Was there a collection of personal information?
2. If so, was the collection authorized by s. 24 of *FOIPOP*?
3. Was there a use of personal information?
4. If so, was the use authorized by s. 26 of *FOIPOP*?

DISCUSSION:

Background

[3] In March of 2010 the applicant, then a corrections worker, was charged with a criminal offence by the RCMP. In keeping with the requirements of the Correctional Services Code of Conduct, the applicant informed his employer about the charges. In response, the Department conducted an investigation that eventually lead to the applicant's dismissal in June of 2010. Following that decision, the applicant sought access to the contents of his personnel file seeking documents in relation to the investigation.

[4] The Department responded to the access to information request in August of 2010. In his review of the material disclosed to him, the applicant found information that lead him to believe that the Department, in conducting its investigation, had accessed the JEIN Offender Summary in relation to charges against him. In addition, he found three court related documents in the file that he believed should not have been obtained by the Department:

- A court log dated June 2, 2010 at 14:36 listing two charges against the applicant, the outcome of the criminal hearing, the sentencing date, the identity of the Crown and Defence and the fact that the Defence requested a PSR or pre-sentence report.
- A copy of an unsigned undertaking.
- A copy of an unsigned Order for preparation of a report.

[5] The Department responded directly to the applicant on November 17, 2010 stating that the information that was accessed in the JEIN system consisted of the date on which the applicant was charged with the offence "as well as any relevant court dates." The Department concluded that the access to the JEIN system was authorized under *FOIPOP*. In responding to the applicant's complaint, the *FOIPOP* Administrator states that the complaint was focussed solely on the authority to access the JEIN system. The Department did not address any issues raised in relation to the court documents found on the file.

Privacy Complaint Procedure

[6] 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]

[7] Section 24 of *FOIPOP* sets out the three circumstances in which a public body may collect personal information:

> 24(1) Personal information shall not be collected by or for a public body unless
> (a) the collection of that information is expressly authorized by or pursuant to an enactment;
> (b) that information is collected for the purpose of law enforcement; or
> (c) that information relates directly to and is necessary for an operating program or activity of the public body.

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

> 26(1) 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.

[9] "Compatible" purpose referred to in s. 26(1)(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

[1] *Privacy Review Officer Act* (*PRO)* s.5(2).
[2] *PRO* s. 6(2).

(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.

Burden of Proof

[10] 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 complaint 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]

1. Was there a collection of personal information?

[11] Upon receipt of the applicant's complaint, the public body treated his complaint as a collection complaint and evaluated its authority to access data in the JEIN system under s. 24 of *FOIPOP*.

[12] In his submissions, the applicant continued to make reference to the three court documents and to comments found in various emails sent to him in response to his access request. None of these matters were considered by the Department in response to his original privacy complaint. As Review Officer, I may only exercise the power to conduct a review and make recommendations on a complaint that has been the subject of an internal review procedure. In this case, the internal review and subsequent correspondence from the Department is focussed only on the appropriateness of the access to the JEIN system by the Department employee tasked with investigating the applicant. Therefore, this review report is focussed only on the issue of whether or not the access to the JEIN system was authorized under *FOIPOP*. However, as noted below, the Department concedes that the information contained in these court documents is accessible in the JEIN system. Therefore, I will evaluate the authority to access this type of information below.

[13] The Department confirmed that one individual tasked with conducting the investigation into the applicant's conduct (the investigator) did access the JEIN system on May 18 and 19, 2010. In its initial response to the applicant on November 17, 2010 the Department confirmed that the information that was accessed in the JEIN system included the information contained in the three documents of concern to the applicant. In this case, the investigator accessed the JEIN Offender Summary for the applicant which provided: name, date of birth, case number, charges, the offence date, the outcome of the offences, appearance dates and locations, orders in relation

[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.

to the offences including an order for the preparation of a report, and the details of an undertaking.

[14] The first issue in any privacy complaint is whether or not any "personal information" within the meaning of *FOIPOP* is involved.

[15] Personal information is defined in s. 3(1) of *FOIPOP* and provides in part:

> 3(1) In this Act
> (i) "personal information" mean recorded information about an identifiable individual, including
> (i) the individual's name, address or telephone number,
> (vii) information about the individual's educational, financial, criminal or employment history.

[16] As noted above, the information accessed by the investigator included name, date of birth and information in relation to criminal history. I find that all of this information qualifies as "personal information" within the meaning of *FOIPOP*.

[17] The next issue is whether in accessing information in the JEIN system, the investigator "collected" personal information within the meaning of *FOIPOP*.

[18] The Department says that the JEIN system is "Nova Scotia's integrated, single software application that is used in multiple divisions of the Department of Justice."[5] The Department further noted that, "the Courts portion of the system is a case management system for court proceedings. The Corrections portion of the system is used to manage offenders either in a facility setting or while on some sort of community supervision."[6]

[19] In this case, the JEIN system then was the Department's own database in which it stored information for the use of its employees. The individual who accessed the applicant's personal information in this case was an employee of the Department, acting in the course of his employment, when he performed the search.

[20] *FOIPOP* does not define the words "access", "collection" or "use". The Concise Oxford English Dictionary defines "access", "collect", "collection" and "use" as follows:

> Access – n. 1. the means or opportunity to approach or enter a place. The right or opportunity to use something or see someone. 2. retrieval of information stored in a computer's memory.
>
> Collect – v. 1. bring or gather together. Systematically seek and acquire.
>
> Collection – n. 1. the action or process of collecting. 2. a group of things collected or accumulated.

[5] Provided in a letter dated March 24, 2011 from the Department of Justice to the OIPC.
[6] Provided in a letter dated May 22, 2015 from the Department of Justice to the OIPC.

> Use – n. 1. the action of using or state of being used. The ability or power to exercise or manipulate something.

[21] "Collection" and "access" are not synonymous. Collection refers to a public body having obtained the personal information in the first instance – that is gathered or acquired the information. "Access" refers to the internal retrieval of that information including the opportunity to use something. Accessing information is the ability to manipulate data – even if just to the extent that you view or print the data. Each "access" of personal information within a public body is not a new "collection" for the purposes of s. 24 of *FOIPOP*. Nor is there a new collection within programs of a public body that share the personal information, as here.[7]

[22] There is no evidence or allegation that the investigator who accessed the applicant's data in this case was not otherwise regularly authorized to view and use data from the JEIN system of the type at issue here. In addition, the information necessary for the investigator to conduct the search (employee name and date of birth) was information already in the possession of the Department as the applicant was an employee at the time of the search.

[23] Based on the meanings of "access", "collection" and "use", and consistent with a number of findings in other jurisdictions,[8] I find that the access into the JEIN system by the investigator in this case was not a new collection of the applicant's personal information.

[24] It is therefore not necessary for me to consider the arguments the Department made in support of its retrieval of the information, viewed as a 'collection'.

2. If so, was the collection authorized by s. 24 of *FOIPOP*?

[25] Since I have determined that there was no collection of personal information in this matter, I will not consider this issue.

3. Was there a use of personal information?

[26] The Department concedes that the investigator accessed the applicant's personal information in the JEIN system. As noted above, an access to personal information within a Department's computer system by the Department employee in this case was a use of the personal information.

4. If so, was the use authorized by s. 26 of *FOIPOP*?

[27] The Department states that the use was authorized under s. 26(a) (original or compatible purpose) and 26(c) (for a purpose for which the information may be disclosed) of *FOIPOP*.

Original or compatible purpose uses s. 26(a)

[28] 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 Department states that the use of the applicant's personal information in the JEIN system in this case was for a compatible purpose.

---

[7] As stated in Alberta Order 2000-02 at para. 99.

[8] See for example Alberta Order F2015-27 at paras. 10-11 and Alberta Order 2000-02 at paras. 99-101.

[29] Section 28 of *FOIPOP* defines what a compatible purpose is. This provision is virtually identical to definitions of "consistent purpose" in the Alberta and British Columbia public sector privacy legislation.[9] 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.

[30] Clearly, in order to evaluate whether the new use was for a compatible purpose, I must know both the original purpose for the collection of the data accessed from the JEIN system and the purpose for the new use when it was accessed in this case.

[31] The Department states that the purpose of the JEIN system is as an integrated criminal case management system that provides users with the ability to manage their authorized portion of cases as they are processed through the Justice System. The Courts portion of the system is a case management system for court proceedings. The Corrections portion of the system is used to manage offenders either in a facility setting or while on some sort of community supervision. In 2008 Deloitte completed a report on Nova Scotia's adult correctional facilities. In that report it describes the JEIN system as follows:

> JEIN is Nova Scotia's integrated, single software application that is used in multiple divisions of the Department of Justice, correctional facilities, the courts, and community corrections. JEIN provides a means to capture and share information between administrative staff, correctional staff, sheriffs, police, court administrators, and can be used for prisoner tracking, records management and information management.[10]

[32] The Department states that the purpose for the use of the data in this case was to confirm the details of the criminal charge that the applicant had disclosed to the Department. That confirmation occurred in the broader context of an investigation into whether or not the applicant, as an employee of the Department, had met the requirements of his duties as set out in the *Correctional Services Act*, *Regulations* and Code of Professional Conduct. The investigation report itself, a portion of which the applicant received, states that the investigator was assigned to determine if the applicant had violated the Code of Professional Conduct. The Code of Professional Conduct is authorized under the *Correctional Services Act*, s. 6, and is set out in more detail in the *Correctional Services Regulations*, sections 14 – 20.

[33] In March of 2010, the applicant reported to the Department that he had been arrested and charged with offences by the RCMP. The applicant did so because s. 8 of the *Correctional Services Regulations* requires that an employee who is questioned or charged by police in

---

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

[10] Deloitte, Report on Nova Scotia's Adult Correctional Facilities, October 29, 2008 available online at: https://www.novascotia.ca/just/global_docs/Deloitte%20Report%20-%20NS%20Correctional%20Facilities%20Nov08.pdf

connection with alleged criminal activity must notify the Executive Director no later than 72 hours after the event.

[34] Having received this information, the Department states that it was authorized to then make inquiries and to investigate the possibility that the staff member was in violation of the *Correctional Services Act* and *Regulations*.

[35] The Department further states that the information in the JEIN system was used for a compatible purpose, "to maintain the security at one of the facilities that is part of the Justice System. In order to ensure facilities are secure, they must follow all their legislated and policy requirements. The purposes of the legislation and policies is to provide all offenders and employees a safe environment. This was not a check done on an employee just because they were an employee. The Department was acting on information that was supplied by the employee under the terms of their employment which is based in legislation."[11]

[36] The nature of the information accessed in the JEIN system (court dates, charges and outcomes) and the dates of access (immediately after a court appearance) both support the Department's submission that the JEIN system was accessed for the purpose of confirming information supplied by the applicant to the Department and for determining the outcome of the charges.

[37] The Department points to sections 5(a) of the *Correctional Services Act* and 5(2)(a) of the *Correctional Services Regulations* as setting out the standard that correctional officers cannot be charged with or convicted of a criminal offence. However, both sections state that they apply to "prospective" employees. The applicant was not a prospective employee at the time of the events in question; he was an employee, therefore these provisions do not apply in this case.

[38] In summary then, 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.

[39] In the applicant's case in particular, his personal information was obtained in the course of his interaction with the police and the court system and was entered into the JEIN system as part of the tracking of his criminal case. In my opinion, all of the purposes for the JEIN system were potentially engaged when the applicant's personal information was originally input into it.

[11] Provided in a letter dated May 18, 2016 from the Department of Justice to the OIPC.

[40] The purpose for the use of the applicant's personal information in the JEIN system at issue here was to confirm the details of a criminal charge against an employee and provided by that employee in keeping with the requirements of the *Correctional Services Regulations*. This is a narrow and precise new use of the JEIN system information.

[41] I noted above that in order for the use to be "compatible' three things must be true:

> (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.

[42] Section 26(a) of *FOIPOP* permits the use of information for the purpose for which it was obtained or compiled **or** for a use compatible with that purpose. 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]

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

[43] I have no hesitation in finding that the Department's investigation into whether or not there had been a violation of the Code of Professional Conduct was part of a legally authorized program or activity and that obtaining confirmation of the charges against the applicant and determining the outcome of those charges were both necessary for that investigation.[13]

[44] 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*:[14]

- 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.

---

[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 collection of personal information for potential use in investigating employee conduct has been found to be directly related to a public body activity or program, that is, its management of employment relationships in other cases. See for example BC Order F13-04 at para. 56 and Alberta Order F2015-27 at para. 33.

[14] BC Order F07-10.

[45] In this case, the evidence establishes that the information used from the JEIN system consisted of court dates, charges and outcomes. The applicant had already disclosed some information regarding the charges. The Department could not reasonably rely solely on an employee's self-reporting in such a significant matter. Objective reliable evidence was necessary to establish the facts with certainty, particularly given that the information could be, and in this case was, used to terminate the applicant's employment. I find that while the information was sensitive, it was the minimum necessary to confirm the applicant's status with respect to the criminal charges that were, in turn, directly related to the applicant's suitability for continued employment as a corrections services worker. The applicant complained that the investigator was not authorized to access the data. In fact, the one and only person in this circumstance who had a need to access this particular data was the investigator. The information was directly related to and necessary for the task the investigator had been assigned.

[46] However, in order to use the JEIN system for this purpose, the use must also have had a reasonable and direct connection to the original purpose for the collection of information into the JEIN system. If it does not, then the Department must use another source – presumably a direct request for disclosure either from a police department or from the courts – to obtain the information it needed.

"Reasonable and direct connection"

[47] Is it reasonable for the Department to use the JEIN system for the purposes of investigating one of its own employees charged with a criminal offence? Is there a direct connection between such an investigation and the original purposes for which the applicant's information was input into the JEIN system?

[48] What is a "reasonable connection" in this context? In my view, "reasonable" means fair and sensible, suggesting sound judgement. "Direct" suggests a straightforward and clear connection.

[49] The Alberta government's FOIP Guidelines and Practices states that there is a reasonable and direct connection if there is a "logical extension of the original use."[15] 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."[16]

[50] 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.[17]

[51] 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

---

[15] Service Alberta FOIP Guidelines and Practices, p. 268 http://www.servicealberta.ca/foip/documents/chapter7.pdf.
[16] Service Alberta FOIP Guidelines and Practices, p. 295 http://www.servicealberta.ca/foip/documents/chapter7.pdf.
[17] 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.

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 concludes that the public body's purpose of investigating its employee's honesty did not have any reasonable and direct connection to any of the purposes for the system.[18] 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.

[52] In this case the Department argues that the purpose of the JEIN system is to be an integrated criminal case management system. Part of being processed through the Justice System, the Department argues, is that you could be managed by corrections 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.

[53] In December 2006, Justice Nunn released his extensive report relating to the release from custody of a young person whose criminal actions caused the tragic death of another person. Justice Nunn identified a number of contributing factors, one being the failure to share information in a timely and effective fashion. Recommendation 7 in his report addresses this issue:

> Recommendation 7 – The Department of Justice, in consultation with all of its key justice stakeholders, should consider enhancements to the JEIN system, including the possible development of electronic versions of Informations or other court documents, with the goal of increasing the effectiveness and efficiency of communication among justice partners and reducing the reliance on multiple forms of communication for delivery of crucial information.[19]

[54] The system then is also intended to increase effectiveness and efficiency of communication among justice partners.

[55] I am satisfied that as an information management system, the JEIN system is intended to support the security of the Justice System generally and the correctional system in particular. 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. I find then that the use of the JEIN

[18] Alberta Order F2015-27 at para. 31.
[19] Report of the Nunn Commission of Inquiry, December 2006: http://novascotia.ca/just/nunn_commission/_docs/Report_Nunn_Final.pdf.

system for the purposes of confirming information provided by a correctional employee in relation to a criminal charge was a compatible use within the meaning of s. 28 of *FOIPOP*.

[56] To be clear, this is a very narrow authorized consistent purpose and will only arise in the rare circumstance where a correctional services employee reports a criminal charge as required under the *Correctional Services Regulations*. The authorized use is limited to confirmation of the charges and the outcome of those charges in the JEIN system and then only by the individual authorized to conduct the investigation.

[57] Having determined that the use in this case was authorized by s. 26(a) of *FOIPOP*, I have not considered the Department's arguments with respect to the potential application of s. 26(c).

FINDINGS & RECOMMENDATIONS:

[58] I find that the use of the applicant's personal information in this case was authorized under s. 26(c) of *FOIPOP*.

[59] I recommend that the Department of Justice take no further action in this matter.

July 11, 2016

Catherine Tully
Information and Privacy Commissioner for Nova Scotia