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

REVIEW REPORT 16-02

March 14, 2016

Department of Justice

Summary: After his release from a correctional facility, the applicant became concerned that facility staff were continuing to access his personal information without authorization. He therefore sought access to records about himself and a list of persons who had accessed his information in the correction system database. The Department of Justice ("Department") found a six page incident reporting form and an audit log. It withheld certain information citing three exemptions to disclosure: harm to the security of the system, endangerment of any person's life or safety and, unreasonable invasion of personal privacy.

The Commissioner finds that unique user IDs are an integral part of the system's security. As a result, she finds that disclosing user IDs in the audit log would increase the security risks to the correction system database and so recommends that the Department continue to withhold the user IDs. She further finds that the Department provided sufficient evidence to demonstrate that disclosure of two individuals' identities in the incident reporting form could reasonably be expected to cause them harm, and recommends the Department continue to withhold that information. However, for certain other information, the Commissioner finds the Department's evidence was insufficient to meet the reasonable expectation of harm test.

Finally, although the Department did not specifically cite the exemption for unreasonable invasion of personal privacy for all the severed personal information, the Commissioner finds that, because it is a mandatory exemption, she is required to consider whether it applies to the personal information in the record. She finds that disclosure of certain personal information would be an unreasonable invasion of privacy and recommends against disclosure.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, SNS 1996 c 165 ss. *3, 7, 15, 20, 45.*

Authorities Considered: Alberta: Investigation Report 2013 IR-02, 2013 CanLII 82405 (AB OIPC); **British Columbia:** Investigation Report F13-02, 2013 BCIPC 14 (CanLII); Orders F09-15, South Coast British Columbia Transportation Authority (Re), 2009 CanLII 58553 (BC IPC); F14-19, British Columbia Ferry Services Incorporated (Re), 2014 BCIPC 22 (CanLII); F14-21, Mission (District) (Re), 2014 BCIPC 24 (CanLII); F15-72, British Columbia (Public Safety) (Re), 2015 BCIPC 78 (CanLII); **Nova Scotia:** Review Reports FI-98-47, 1998 CanLII

2622 (NS FOIPOP); FI-99-41, 1999 CanLII 2466 (NS FOIPOP); FI-07-59, 2008 CanLII 50497 (NS FOIPOP); FI-08-107, 2010 CanLII 47110 (NS FOIPOP), FI-09-29(M), 2012 CanLII 44742 (NS FOIPOP), FI-10-71, 2015 CanLII 60916 (NS FOIPOP); FI-12-01(M), 2015 CanLII 54096 (NS FOIPOP); **Ontario:** Interim Order MO-3025-I, Ottawa Police Services Board (Re), 2014 CanLII 14791 (ON IPC); Orders M-933, Metropolitan Toronto Police Services Board (Re), 1997 CanLII 11842 (ON IPC); MO-1293, Toronto Police Services Board (Re), 2000 CanLII 21047 (ON IPC); MO-1698, Toronto Police Services Board (Re), 2003 CanLII 53796 (ON IPC); MO-1335, Toronto Police Services Board (Re), 2000 CanLII 20974 (ON IPC); MO-3072, Timmins Police Services Board (Re), 2014 CanLII 41422 (ON IPC); PO 3497, Ontario (Community Safety and Correctional Services) (Re), 2015 CanLII 32409 (ON IPC); Privacy Complaint MC13-46, Halton Catholic District School Board (Re), 2015 CanLII 13372 (ON IPC); **Saskatchewan**: Investigation Report 131-2015, Insurance (Saskatchewan) (Re), 2015 CanLII 62325 (SK IPC).

Cases Considered: *Dagg v. Canada (Minister of Finance*) [1997] 2 SCR 403; House, Re, 2000 CanLII 20401 (NS SC)**;** *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, [2014] 1 SCR 674, 2014 SCC 31 (CanLII); *Sutherland v. Nova Scotia (Community Services)*, 2013 NSSC 1 (CanLII).

Other Sources Considered: *Concise Oxford English Dictionary*, (12th ed) (New York: Oxford University Press, 2011); Deloitte & Touche LLP – **"**Report of the External Audit of 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; Michael Kasner, "User IDs and passwords: Equally important for access security" Tech Republic, July 19th, 2010 http://www.techrepublic.com/blog/it-security/user-ids-and-passwords-equally-important-for-access-security/.

INTRODUCTION:

[1] The applicant requested access to information from the Department of Justice ("Department") about himself including a list of anyone who had accessed his information in the JEIN system. The JEIN system is the Justice Enterprise Information Network and is one of the main systems used by Adult Correctional Facilities in Nova Scotia.[1]

[2] The applicant was provided with partial access to the records and was initially provided with only a summary of the accesses to his information in the JEIN system. Eventually he was also provided with a severed copy of the JEIN audit record (the JEIN Query Report) for the

[1] According to the Deloitte Report on Nova Scotia's Adult Correctional Facilities dated October 29, 2008, "It 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" https://www.novascotia.ca/just/global_docs/Deloitte%20Report%20-%20NS%20Correctional%20Facilities%20Nov08.pdf at p. 20.

relevant time period. As a result of the informal resolution process with this office, the records at issue were reduced to two documents: an incident reporting form and the JEIN audit record.

[3] The Department withheld information from the incident reporting form citing s. 20 (third party personal information) and s. 15(1)(e) and withheld the User IDs from the JEIN report citing s. 15(1)(e) and s. 15(1)(k) (harm to law enforcement) of the *Freedom of Information and Protection of Privacy Act* (*"FOIPOP"*).

ISSUES:

[4] There are two issues under consideration:

(a) Is the Department authorized to refuse access to information under s. 15 of *FOIPOP* because disclosure of the information would harm law enforcement as set out in s. 15(1)(e) and 15(1)(k)?

(b) Is the Department required to refuse access to information under s. 20 of *FOIPOP* because disclosure of the information would be an unreasonable invasion of a third party's personal privacy?

DISCUSSION:

Background

[5] The applicant was released from the Southwest Nova Scotia Correctional Facility ("SNSCF") on June 13, 2011. He became concerned that individuals at SNSCF were accessing information about him even though he was no longer incarcerated at that facility. As a result, on November 1, 2011 the applicant filed his access to information request for essentially any documentation mentioning him and for a list of persons who had accessed his information in the JEIN system. The applicant was not incarcerated between June 13, 2011 and Nov. 1, 2011. The applicant also filed a privacy complaint alleging that individuals had violated *FOIPOP* when they accessed his records in JEIN during this same time period. The privacy complaint is the subject of a separate investigation.

[6] The JEIN system is the Justice Enterprise Information Network and is one of the main systems used by Adult Correctional Facilities in Nova Scotia. The JEIN system is used by multiple divisions of the Department of Justice, correctional facilities, the courts and community corrections. It contains extensive and sensitive personal information regarding charges, court appearances, incarceration records including medical information, and community corrections information. The purpose of the system is to manage individuals' information throughout their interaction with the justice system in Nova Scotia.

[7] The first document subject to this review is an audit log generated from the JEIN system that shows who accessed the applicant's JEIN record and when. The Department withheld the user identification (User ID) of the individuals who accessed the applicant's JEIN record as reported on the audit log. The User ID consists of a series of characters. There are two types of

User IDs. Most of the User IDs consist of information sufficient to identify the user.[2] Some User IDs consist of a series of letters and numbers that cannot, on their face, identify any individual.

[8] Since individual users can be identified by some of the User IDs, this information could potentially qualify as "personal information" within the meaning of s. 20 of *FOIPOP*. Despite this fact, the Department neither applied the mandatory exemption under s. 20 nor provided an explanation for why s. 20 did not apply. The Department relied solely on two exemptions under section 15: s. 15(1)(e) and s. 15(1)(k).

[9] The second document at issue is a six page incident reporting form. The Department cited s. 20 (third party personal information) with respect to some of the information withheld on pages 3, 5 and 6 of the document. Names and signatures appear on every page but the Department once again did not apply this mandatory exemption to this information that, on its face, appears to qualify under s. 20. The Department cited s. 15(1)(e) for third party names, signatures and other information contained in the incident reporting form.

[10] Section 15 of *FOIPOP* provides in part:

> 15(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to
> (e) endanger the life or physical safety of a law-enforcement officer or any other person;
> (k) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

[11] Section 20(1) of *FOIPOP* provides in part:

> 20 (1) The head of a public body shall refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.[3]

Burden of proof

[12] The public body bears the burden of proving that the applicant has no right of access to a record except where the exemption applied is s. 20 - then the applicant bears the burden of proof:

> 45 (1) At a review or appeal into a decision to refuse an applicant access to all or part of a record, the burden is on the head of a public body to prove that the applicant has no right of access to the record or part.
> (2) Where the record or part that the applicant is refused access to contains personal information about a third party, the burden is on the applicant to prove that disclosure of

[2] I have avoided providing specific information about the exact make-up of the User ID in light of the s. 15 arguments discussed below.
[3] A complete copy of the *Freedom of Information and Protection of Privacy Act* is available on our website at: www.foipop.ns.ca.

the information would not be an unreasonable invasion of the third party's personal privacy.

(3) At a review or appeal into a decision to give an applicant access to all or part of a record containing information that relates to a third party,

(a) in the case of personal information, the burden is on the applicant to prove that disclosure of the information would not be an unreasonable invasion of the third party's personal privacy; and

(b) in any other case, the burden is on the third party to prove that the applicant has no right of access to the record or part.

(a) Is the Department authorized to refuse access to information under s. 15 of *FOIPOP* because disclosure of the information would harm law enforcement as set out in s. 15(1)(e) and 15(1)(k)?

User IDs and harm to the security of a system

[13] The Department withheld a column of information that lists the User IDs in the audit log report from the JEIN system. The Department argued that the disclosure of User IDs could reasonably be expected to endanger the life or physical safety of a law-enforcement officer (15(1)(e)) and harm the security of a computer system (15(1)(k)).

[14] Section 15 is a harms-based exemption. The public body bears the burden of proving that this exemption applies to the records. The Department cited a number of older British Columbia decisions as setting out the appropriate test.

[15] In 2014 the Supreme Court of Canada reviewed decisions on the "reasonable expectation of harm test" and summarized the appropriate test as follows:

> *[54] This Court in Merck Frosst adopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expected to" language is used in access to information statutes. As the Court in Merck Frosst emphasized, the statute tries to mark out a middle ground between that which is probable and that which is merely possible. An institution must provide evidence "well beyond" or "considerably above" a mere possibility of harm in order to reach that middle ground.*[4]

[16] As I have stated in a number of previous reports - what is clear from the recent cases is that evidence of speculative harm will not meet the test, certainty of harm need not be established, rather the test is a middle ground requiring evidence well beyond a mere possibility of harm but somewhat lower than harm that is more likely than not to occur.[5]

[17] The Department submits that a User ID is one of three pieces of information necessary to access the JEIN system. As with any typical database system users need a User ID, password and some means of accessing the system. The JEIN system can be accessed from computer

[4] Ontario (CSCS) v. Ontario (IPC) [2014] 1 S.C.R. 674.

[5] For a full discussion of the test and examination of the case law see NS Review Report FI-10-71 paras. 40-47.

terminals within a prison or courthouse for example. Users would of course need to be able to log into such a terminal plus know the location of the database itself unless the computer had a shortcut available. The Department states that disclosing the User IDs could jeopardize the integrity of the data or the security of the JEIN system because it is part of the information necessary to gain access to the system.

[18] The Department made one further in camera argument with respect to the ability of this particular applicant to take advantage of the User ID information at the time of the filing of his access request. That situation no longer applies and, given the discussion below, I have not taken that information into account in my analysis.

[19] At a rudimentary level User IDs serve a number of purposes.[6] First, they are a security feature that identifies the user to the system. Only an authorized user with a valid User ID can access the system. Second, based on the User ID, system administrators can assign and authorize access privileges. Privileges usually vary according to assigned work duties. Third, User IDs form an essential part of system audit capabilities. In order to audit a system to ensure compliance with rules in *FOIPOP* for example, it is essential to know who a user is and what information he or she has accessed. Audit logs provide the raw material for evaluating whether or not a system is secure and is being properly used by authorized users.

[20] Privacy Commissioners across Canada have repeatedly recommended that effective programs for monitoring compliance with privacy laws include the creation and monitoring of audit logs for systems containing personal information.[7] For example, the Saskatchewan Information and Privacy Commissioner recently stated,

> In the past, my office has recommended that public bodies run regular random audits to ensure accesses to electronic systems are only occurring for legitimate business purposes. In addition, public bodies create policy and procedure to ensure it is conducting these types of regular random audits. Finally, where an employee has been found to be snooping, public bodies should monitor those employees for a period of years instead of 9 months. My office is currently developing guidance for public bodies on best practices for auditing.[8]

[21] In order to audit a system, the system must log activity in a manner that identifies the individual user. Best privacy practice is to ensure that all users have a unique ID and password and that individuals are granted access on a need to know basis founded on their job duties.[9] As

---

[6] The current International Standard ISO 27018 states that, "A.10.8 If more than one individual has access to stored PII (personally identifiable information), then they should each have a distinct user ID for identification, authentication and authorization purposes".

[7] See for example BC Information and Privacy Commissioner recommendation #4 in *British Columbia (Health) (Re)*; Ontario Information and Privacy Commissioner in relation to the use of video surveillance: Privacy Complaint MC13-46; Alberta Information and Privacy Commissioner Investigation Report 2013 IR-02 at para. 31.

[8] Investigation Report 131-2015.

[9] The Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioner for British Columbia and Alberta issued a security checklist that includes minimum security requirements for public bodies. The list specifies at item 13.19 that user identification must be controlled and audited. A full interactive

noted above, it is well accepted that systems must include logging of individual activity and regular auditing to ensure that access by individuals is appropriate. Put another way, User IDs are viewed as an important security feature and part of a systemic approach to ensuring that information in systems is accessed in accordance with the rules in *FOIPOP*.

[22] A series of Ontario cases discussed access to information contained on CPIC reports. CPIC is the Canadian Police Information Centre database used nationally. It is an information management system that houses information in relation to criminal charges. Reports, including audit reports from the CPIC system include various code information. Ontario adjudicators have repeatedly determined system code information including transmission access codes, format codes for accessing the CPIC database and query formats could all reasonably be expected to facilitate the commission of an unlawful act.[10] In making that determination the adjudicators determined that the code information would instruct an unauthorized person as to how information is retrieved and stored on the CPIC system[11] and would make unauthorized and illegal access to the CPIC system easier.[12] While it does not appear that the code information in these cases was specifically User ID, it does appear that the code information served a similar purpose in terms of facilitating access to a database.

[23] I could find no decisions specifically regarding the application of the equivalent to s. 15(1)(k) to User IDs. It seems this may be the case because there is general agreement that disclosing User IDs is indeed a security risk sufficient to meet the test in provisions like s. 15(1)(k) and so the matter is settled before decisions are rendered. I set out two examples below to illustrate this point.

[24] In Ontario Order MO-3072 the applicant sought access to a number of records including audit log query results from a police database. The public body (a police force) withheld the querying member's security credentials (i.e. User ID) under the equivalent to s. 15(1)(k) of *FOIPOP*. By the time the request reached the adjudication stage the only outstanding issue was adequate search. The application of the equivalent to s. 15(1)(k) to the security credentials was accepted through the investigation and mediation stages and so was not at issue in the adjudication.[13] There appears to be tacit approval for the application of s. 15(1)(k) to User IDs in particular.

[25] In a recent decision in British Columbia a public body denied access to User ID and password:

> [48] BC Ferries applied s. 15(1)(l) as the sole basis for non-disclosure of three lines of information on p. 11 of the record and argues that disclosure of the lines would provide a

---

version of the checklist is available at: https://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1 A short version of the checklist is also available on this office's website at: http://foipop.ns.ca/sites/default/files/publications/Reasonable%20Security%20Checklist%20for%20Personal%20Information%20%2822%20Sept%2015%29.pdf.

[10] See for example Interim Order MO-3025-I at para. 61, Order MO-1698 at p. 4.

[11] Order MO-1293.

[12] Order M-933 and Order MO-1335.

[13] Order MO-3072 at p. 5.

> "road map" to computer hackers that could reasonably be expected to harm the security of its computer or communication systems. BC Ferries further submits that password information regarding a government email system is a "property or system" as referred to and covered by s. 15(1)(l). I note that the three lines in question consist of a website address, a User ID and a password that provide access to a report prepared by BC Ferries in 2006 regarding an illness suffered by the applicant.
>
> [49] The applicant concedes that disclosure of User ID and passwords would compromise BC Ferries' communications or computer security and thus should not be disclosed.[14]

[26] I note that the record at issue in this case contains not just one User ID but rather multiple IDs. This increases the security risk because one means of gaining access to a system is to run known common weak passwords against User IDs. Having multiple User IDs increases the chance that a weak password will work.[15]

[27] Based on the sensitivity of the data in the JEIN system, the location of available computer terminals, the number of User IDs at issue and the function of User IDs as part of the security of a system, I find that the disclosure of User IDs for the JEIN system could reasonably be expected to harm the security of a computer system within the meaning of s. 15(1)(k) of *FOIPOP*. Since I have concluded that s. 15(1)(k) applies to the User IDs I will not consider the application of s. 15(1)(e) to this information.

[28] I recommend that the Department continue to withhold the list of User IDs contained in the JEIN audit report.

Incident Reporting Form – endanger life or physical safety

[29] The Department withheld the following types of information from the incident reporting form citing s. 15(1)(e) of *FOIPOP*:

- Signature of an individual confirming that the document was a "true copy";
- Name of the complainant;
- Identity (signature) of the supervisor who received the report;
- One paragraph of the complaint narrative (a portion of which was also withheld under s. 20 discussed below).

[30] In order for s. 15(1)(e) of *FOIPOP* to apply, a public body must establish that the disclosure of the withheld information could reasonably be expected to endanger the life or physical safety of a law-enforcement officer or any other person.

---

[14] Order F14-19.

[15] This is known as "bulk guessing attacks". For a discussion of this see Michael Kasner, "User IDs and passwords: Equally important for access security" Tech Republic, July 2010 http://www.techrepublic.com/blog/it-security/user-ids-and-passwords-equally-important-for-access-security/ .

[31] *FOIPOP* does not define "endanger". However, according to the Concise Oxford English Dictionary "endanger" means to "put at risk or in danger".[16]

[32] There have been a number of decisions by my predecessors with respect to s. 15(1)(e). Generally speaking, when 15(1)(e) is successfully applied, it is difficult to tell why because the submissions on the issue are often confidential.[17]

[33] The access laws in Ontario and British Columbia have a similar provision to s. 15(1)(e). In a recent decision by an adjudicator in British Columbia, the OIPC considered the Corrections Branch's argument that disclosure of certain information, including identity information, could endanger life or physical safety of Correction's Branch staff because the applicant had a history of assaultive behaviour. In determining that the equivalent to s. 15(1)(e) of *FOIPOP* did not apply the adjudicator noted: the records were more than 20 years old, the applicant's assault record related to women with whom he had had a personal relationship and the applicant had already been provided with other records by the Corrections Branch with no evidence of endangerment created by the disclosure. On that basis the adjudicator concludes that the evidence and argument were speculative and amounted to no more than mere assertion.[18]

[34] In Ontario Order PO 3497, the adjudicator determined that the equivalent to s. 15(1)(e) did not apply to a video despite claims from individuals seen in the video that they feared for their safety should the video be disclosed. In deciding that the exemption did not apply the adjudicator took into account the fact that the applicant had already seen the video once with no evidence of any harm resulting from that viewing. Further, the adjudicator determined that while the relationship between the applicant and the individuals in the video was "unpleasant" the submissions on the application of the exemption were unconvincing.[19]

[35] In this case the Department's arguments with respect to the application of s. 15(1)(e) are focussed on the identity of the complainant and the supervisor who signed the report – both of whom were employees of the Department. The focus of their arguments relates to the danger of identifying individuals to the applicant based in part on the applicant's criminal past which the Department says demonstrates a history of violence and a lack of respect for authority. The Department provided evidence in support of its submission and further, the records responsive to the applicant's request confirm the Department's allegations. Therefore, I am satisfied that the Department has provided sufficient evidence to establish a reasonable expectation of harm within the meaning of s. 15(1)(e) with respect specifically to the identity of the complainant and the supervisor who signed the report.

[36] The Department provided no argument or evidence as to why s. 15(1)(e) applies either to the signature of the individual who confirmed that the documents are true copies nor why s.

---

[16] Concise Oxford English Dictionary, (12th ed) p. 471.

[17] I note that on at least nine occasions my predecessors considered the application of s. 15(1)(e). None of these cases provide a detailed discussion of when and how s. 15(1)(e) might apply although there is some discussion regarding the reasonable expectation of harm test generally. See for example NS Review Reports FI-07-59, FI-99-41 and FI-98-47.

[18] Order F15-72 at paras. 11-15.

[19] Order PO 3497 at para. 36.

15(1)(e) applies to the narrative paragraph (five sentences) contained on the last two pages of the incident reporting form. In the absence of any evidence or argument to support the application of s. 15(1)(e) to this information I find that s. 15(1)(e) does not apply to the narrative paragraph (5 sentences) on pages 5 and 6 of the incident reporting form.

[37] No other exemption was applied to the first sentence of the narrative and so I recommend that it be disclosed to the applicant.

[38] With respect to the last four sentences, the Department also applied s. 20(1) to this information. I will discuss the application of s. 20(1) below.

[39] With respect to the signatures of individuals who confirmed that the document was a true copy, the Department already disclosed identical information in response to this access request. It disclosed a number of documents not at issue in this review that included the true copy stamp and the Department did not withhold the signature of the individual who signed the stamp. Presumably no harm was caused by this disclosure since the Department made no claim to this effect. Therefore, I find that s. 15(1)(e) does not apply to the true copy stamp signatures. However, as I noted above, there is a potential that s. 20 must apply to this information despite the fact that the Department did not cite s. 20(1). I will discuss the application of s. 20(1) below.

(b) Is the Department required to refuse access to information under s. 20 of *FOIPOP* because disclosure of the information would be an unreasonable invasion of a third party's personal privacy?

[40] The Department provided partial access to a six page incident reporting form. In its submission the Department says it relies on both s. 20 and s. 15(1)(e) as the basis for withholding the severed information.

[41] The Department provided no submissions on the application of s. 20 stating only that "The Department maintains this is personal information that is not the Applicant's and confirms that our position has not changed on the application of s. 20(1) to those records".

[42] To be clear, the fact that the applicant bears the burden of proving that the disclosure of information would not be an unreasonable invasion of a third party's personal privacy does not relieve the public body from its responsibility to properly apply *FOIPOP* and to provide reasons for the exemptions it has chosen.[20]

[43] Further, s. 20 is a mandatory exemption. This means that if the requirements of s. 20 apply, the information must be exempted from disclosure. The Department may feel confident that since s. 15 has been applied to the same information it is protected. But s. 15 is a discretionary exemption that requires evidence of harm. If the test for s. 15 is not satisfied, third

[20] Section 7(2)(a)(ii) of *FOIPOP* requires that public bodies provide reasons for any refusal and state the provision upon which the refusal is based. Further, the courts have consistently applied a four step analysis to the application of s. 20 and it is only in the last step that the burden on the applicant is considered.

party personal information may be unprotected and a disclosure could potentially result in a privacy breach by the Department.

[44] Since the Department has provided no submission on the application of and in some cases on its failure to apply the mandatory exemption in s. 20, I have conducted an evaluation of all the information to which s. 20 could potentially apply.

[45] *FOIPOP* permits the disclosure of third party personal information if such a disclosure would not be an "unreasonable invasion" of a third party's personal privacy. In order to determine whether or not a disclosure would result in an unreasonable invasion of personal privacy, public bodies must take a four step approach to their analysis:[21]

1. Is the requested information "personal information" within s. 3(1)(i)? If not, that is the end. Otherwise, the public body must go on.
2. Are any of the conditions of s. 20(4) satisfied? Is so, that is the end.
3. Is the personal information presumed to be an unreasonable invasion of privacy pursuant to s. 20(3)?
4. In light of any s. 20(3) presumption, and in light of the burden upon the appellant established by s. 45(2), does the balancing of all relevant circumstances, including those listed in s. 20(2), lead to the conclusion that disclosure would constitute an unreasonable invasion of privacy or not?

1. Is the requested information personal information?

[46] "Personal information" is a term defined in *FOIPOP* in s. 3(i) and it includes names (s. 3(i)(i)), and opinions about third parties (s. 3(i)(viii)).

[47] I have identified six types of information in the record that qualify as "personal information" within the definition.

[48] The Department did not apply s. 20 to three pieces of information that, in my view, contain personal information. However, in all three cases I have already determined that s. 15 applies to the information and so I will not further evaluate whether or not s. 20 applies to this information:

i. Name of the complainant on the incident reporting form;
ii. Signature of the supervisor/investigator on the incident reporting form;
iii. User IDs that reveal individual identities on the JEIN audit report.

[21] See for example *House (Re)*, 2000 CanLII 20401 (NS SC), and *Sutherland v. Dept. of Community Services*, 2013 NSSC 1. This approach has been consistently followed by former Review Officers. See for examples: NS Review Reports FI-08-107 and FI-09-29(M).

[49] There remains three types of information that qualify as "personal information" on the incident reporting form:

i. Signature of the person confirming that the document is a true copy (pp. 1, 2, 3, 4, 5 and 6) (s. 20 not applied by Department);
ii. Name of a third party and information that could identify this third party (pp. 3 and 5) (s. 20 applied by the Department);
iii. The complainant's opinions about a third party which qualify as the third party's personal information (eight lines in first paragraph on page 5 and last four sentences of the narrative on page 6) (s. 20 applied by the Department).

2. Are any of the conditions of s. 20(4) satisfied?

[50] Section 20(4) states that a disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if any of the listed circumstances apply. Section 20(4) states, in part:

> 20(4) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if:
>
> (a) the third party has, in writing, consented to or requested the disclosure;
> (b) there are compelling circumstances affecting anyone's health or safety;
> (c) an enactment authorizes the disclosure;
> (e) the information is about the third party's position, functions or remuneration as an officer, employee or member of a public body

[51] In my opinion these are the only provisions in s. 20(4) that might apply to the three remaining types of information I have identified as qualifying as "personal information" within the meaning of *FOIPOP*. No evidence was provided to support the application of s. 20(4)(a), (b) or (c). As noted above, the Department did not apply s. 20 to the true copy signatures. I can only assume this was because the Department was of the view that the true copy signatures fell within s. 20(4) and so, s. 20 did not apply. The most likely provision to apply to the information is s. 20(4)(e).

The meaning of "positions, functions or remuneration" (s. 20(4)(e))

[52] Does any of the personal information listed above qualify as information about a third party's "position, functions or remuneration" of an employee of a public body?

[53] Section 20(4)(e) has two requirements: first the information must be about the third party's position, functions or remuneration and secondly, it must be about the third party's position, functions or remunerations as an employee of a public body.[22]

[54] In each of the three instances listed, is the information about an employee's position or functions as an employee, or is it more accurately about his or her work history? The distinction

[22] This is consistent with the approach taken in B.C. to an identically worded provision. See for example Order F09-15 at paras. 15-16 and Order F14-21 at para. 24.

is important because if the information is simply about the employee's position or functions, s. 20 cannot apply. However, if the information is more accurately characterized as being about his or her work history then, by virtue of s. 20(3)(d) (discussed below) s. 20 is presumed to apply unless something outweighs that presumption.

[55] "Functions" is listed alongside other words which together describe what the employee is hired to do, his or her position within the public body and what the employee receives for fulfilling his or her assigned duties. It appears then that s. 20(4)(e) is intended to apply to information about the job occupied by the individual more so then information about the individual.

[56] The leading case on this exemption is *Dagg v. Canada (Minister of Finance*) [1997] 2 SCR 403. In that case the Supreme Court of Canada was considering the provision in the federal *Privacy Act* that is similar to s. 20(4)(e). The Court notes that the intention of the provision is:

> . . . to exempt only information attaching to positions and not that which relates to specific individuals. Information relating to the position is thus not "personal information", even though it may incidentally reveal something about named persons. Conversely, information relating primarily to individuals themselves or to the manner in which they choose to perform the tasks assigned to them is "personal information".
>
> I agree. Moreover, I agree with La Forest J. that "[g]enerally speaking, information relating to the position . . . will consist of the kind of information disclosed in a job description", such as "the terms and conditions associated with a particular position, including . . . qualifications, duties, responsibilities, hours of work and salary range" (para. 95).[23]

[57] The majority of the Court went on to decide that the building sign-in logs containing the name, dates and times individuals went to their work places constituted information about the position and so did not fall within the personal information exemption. The majority made this finding despite the fact that the logs included weekend and evening work hours because they were of the view that the information reflected the work demands of the position. The Court noted that there is neither a subjective aspect nor an element of evaluation contained in the report on the individual's presence at the workplace beyond normal working hours.[24]

[58] It appears that the "true copy" stamp was applied to the responsive records and signed because the applicant in this matter had requested a "true copy" of documents in response to his access to information request.[25] The sole purpose for the signature then was to attest to the accuracy of the document. The employee signed the document in that context as one of his or

---

[23] *Dagg v. Canada (Minister of Finance*) [1997] 2 SCR 403 at paras. 3 – 4 [*Dagg*].
[24] *Dagg* at para. 12.
[25] The date stamps throughout the response package are dated and signed in November, 2011. The applicant's request for access to "true copies" of various records was received by the Department on November 9, 2011 and they sent their initial response on January 5, 2012. The timing therefore suggests that the true copy stamps were in direct response to the access requests particular demand for "true copies".

her work duties. I find therefore that s. 20(4) applies to this information and so s. 20 cannot apply. Since I earlier determined that s. 15(1)(e) does not apply to this information I recommend that the signature of the individual who signed the true copy stamp be disclosed.[26]

[59] The name of a third party and other information that could identify the third party on pages 3 and 5 of the incident reporting form was withheld by the Department under s. 20. The third party is identified as the focus of the workplace occupational health and safety complaint. I find that this information does not fit within the definition of "functions" of an employee and so I find that s. 20(4) does not apply to this information. Likewise, the complainant's opinions about a third party (pp. 5 and 6) do not fit within the definition of "functions" of an employee and so I find that s. 20(4) does not apply to this information.

3. Is the personal information presumed to be an unreasonable invasion of privacy pursuant to s. 20(3)?

[60] Since s. 20(4) does not apply to the identity of the third party (pp. 3 and 5) nor to the opinions contained on pages 5 and 6, I must now consider whether any provision in s. 20(3) applies to the information. In this case, based on the content of the withheld information, two presumptions might apply: s. 20(3)(d) and s. 20(3)(g).

> 20 (3) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if
>
> (d) the personal information relates to employment or educational history;
>
> (g) the personal information consists of personal recommendations or evaluations, character references or personnel evaluations.

[61] The document at issue is a workplace incident reporting form. The withheld information identifies an individual who is the focus of the complaint and includes comments and opinions about that person including what can be characterized as an evaluation.

[62] I find that both s. 20(3)(d) and s. 20(3)(g) apply to the withheld information on pages 3, 5 and 6 of the incident reporting form.

4. In light of any s. 20(3) presumption, and in light of the burden upon the appellant established by s. 45(2), does the balancing of all relevant circumstances, including those listed in s. 20(2), lead to the conclusion that disclosure would constitute an unreasonable invasion of privacy or not?

[63] The applicant's submissions focussed on the JEIN audit report and the identity of the individuals accessing the records. He made no submission on or response to the Department's claim that either s. 15 or s. 20 applied to the incident reporting form. Section 20(2) sets out a

[26] I note that unlike the situation in NS Review Report FI-12-01(M), the signature in this case is not accompanied with a type written name so that the individual employee cannot, in this case, be identified without disclosing the signature. In addition, the sole purpose of the true copy signature is to confirm the accuracy of the document, in other words, the signature is the work product in this situation.

non-exhaustive list of considerations in making the final determination as to whether or not disclosure of third party personal information would be an unreasonable invasion of a third party's personal privacy. In this case the applicant may believe that because he is mentioned in the incident reporting form the record is about him. Section 20(2)(c) states that one consideration is whether the disclosure is relevant to a fair determination of the applicant's rights. In my opinion, the incident reporting form is about two correctional officers and the applicant is only incidentally mentioned in the report. Two other potential considerations are that the information in the report was supplied in confidence by the complainant (s. 20(2)(f)) and that the disclosure might unfairly harm the reputation of any person referred to in the record (s. 20(2)(h)). I am satisfied that both considerations apply to the withheld information and weigh against disclosure.

[64] I find that the applicant has failed to satisfy the burden of proof and has not provided any evidence to outweigh the presumption in s. 20(3)(d) and s. 20(3)(g). I recommend that the Department continue to withhold third party personal information on pages 3, 5 and 6 of the incident reporting form.

[65] For clarity I will provide the Department with recommended severing of the incident reporting form with its copy of this report.

FINDINGS & RECOMMENDATIONS:

[66] I find that:

1. Section 15(1)(k) of *FOIPOP* applies to the User IDs listed in the JEIN audit report.
2. Section 15(1)(e) of *FOIPOP* applies to the complainant's and supervisor's name in the incident reporting form.
3. Section 15(1)(e) of *FOIPOP* does not apply to the identity of the individual who signed the true copy stamp on the incident reporting form.
4. Section 15(1)(e) of *FOIPOP* does not apply to the narrative (final paragraph) of the incident reporting form.
5. Section 20 of *FOIPOP* applies to the information withheld on pages 3 and 5 and the last four sentences on page 6 of the incident reporting form.

[67] I recommend that:

1. The Department continue to withhold User IDs from the JEIN audit report pursuant to s. 15(1)(k) of *FOIPOP*.
2. The Department continue to withhold the identity of the complainant in the incident reporting form pursuant to s. 15(1)(e) of *FOIPOP*.
3. The Department continue to withhold the identity and identifying information of a third party on pages 3 and 5 of the incident reporting form.
4. The Department disclose the signature of the individual who signed the true copy stamp on each page of the incident reporting form.

5. The Department disclose one sentence from the incident reporting form (the first sentence of the last paragraph on page 5).
6. The Department continue to withhold the eight lines from page 5 and the final four sentences of the incident reporting form (page 6) pursuant to s. 20(1) of *FOIPOP*.

March 14, 2016

Catherine Tully
Information and Privacy Commissioner for Nova Scotia