Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Order F15-63

MINISTRY OF TECHNOLOGY, INNOVATION AND CITIZENS' SERVICES

Hamish Flanagan
Adjudicator

November 24, 2015

CanLII Cite: 2015 BCIPC 69
Quicklaw Cite: [2015] B.C.I.P.C.D. No. 69

Summary: The applicant requested a record of email activity sent to and from Ministry and other public bodies' email addresses contained in logs residing on BC Government servers. The Ministry refused to disclose the record on the basis that disclosing it would be an unreasonable invasion of third party personal privacy under s. 22. The Ministry also said that it was unreasonable, for the purpose of s. 4(2) of FIPPA to sever information to which s. 22 applies and release the remaining information. The adjudicator found that s. 22 applies to the record in issue. Further, it is unreasonable under s. 4(2) for the Ministry to sever personal information to which s. 22 applies and disclose the remaining information.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, ss. 4(2), 22.

Authorities Considered: B.C.: Order 03-06, 2003 CanLII 49170 (BC IPC); Order F14-13, 2014 BCIPC 16; Order F15-02, 2015 BCIPC 2 (CanLII); Order F08-04, 2008 CanLII 13322 (BC IPC); Order F13-13, 2013 BCIPC 16 (CanLII); Order 04-17, 2004 CanLII 7059 (BC IPC); Order F14-38, 2014 BCIPC 41 (CanLII); Order No. 63-1995, 1995 CanLII 2863 (BC IPC); Order No. 64-1995, 1995 CanLII 2240 (BC IPC); Order No. 65-1995, 1995 CanLII 549 (BC IPC); Order F07-18, 2007 CanLII 42407 (BC IPC); Order 00-53, 2000 CanLII 14418 (BC IPC); Order F15-17, 2015 BCIPC 18; Order 01-52, 2001 CanLII 21606 (BC IPC); Investigation Report IR15-01, *Use of Employee Monitoring Software by the District of Saanich,* 2015 BCIPC 15 (CanLII).

Case Considered: *R v. Cole,* 2012 SCC 53 (CanLII).

INTRODUCTION

[1] The applicant requested information about the email addresses, and date and time of emails sent and received on servers responsible for email traffic for BC Government Ministries and several other public sector entities.[1] The information is contained in message tracking logs ("Logs"), which are electronic files on servers that coordinate the delivery of emails maintained by the Ministry of Technology, Innovation and Citizens' Services ("Ministry"). The applicant is seeking information in the Logs for a period of approximately six months.

[2] The applicant says he is primarily seeking the information to obtain valuable insight into how the BC Government works by creating relationship maps that show the interactions between BC Government employees.

[3] The Ministry says that the information requested contains employee personal information, and that disclosing it would be an unreasonable invasion of the employee's personal privacy under s. 22 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The Ministry also says that it is not reasonable under s. 4(2) of FIPPA to sever s. 22 information and disclose the remainder because that would require manual review of the Logs, which, due to the large amount of information they contain, would take an unreasonably large amount of time and cost.

[4] The applicant requested the Office of the Information and Privacy Commissioner ("OIPC") review the Ministry's decision to withhold the requested information. Mediation did not resolve the dispute, and the matter proceeded to an inquiry.

ISSUES

[5] The issues in this inquiry as set out in the OIPC Fact Report are whether:

1) the Ministry is required to refuse access to information in the Logs because disclosure would be an unreasonable invasion of third party personal privacy under s. 22 of FIPPA; and
2) if the Ministry is required to refuse access to some information in the Logs under s. 22 of FIPPA, whether it is reasonable under s. 4(2) of FIPPA for the Ministry to sever that information and disclose the remaining information.

[1] Listed in the Affidavit of D. Ehle at para. 24. The entities include independent offices of the Legislature, for example Elections BC, which are not BC Government entities. For simplicity I will refer to the email addresses of employees whose work email address appears in the Logs as BC Government employees or simply employees.

[6] Under s. 57(2) of FIPPA, the applicant has the burden to prove that disclosure of information withheld under s. 22 of FIPPA would not unreasonably invade third party personal privacy. FIPPA is silent on the burden in relation to the s. 4(2) issue. The Ministry accepts that, consistent with previous orders,[2] it bears the burden in proving that the records cannot be reasonably severed. The Ministry also notes that previous orders have indicated that as a practical matter, it is in the interest of each party to provide argument and evidence to justify its position.[3]

DISCUSSION

[7] **Background—**Order F14-13[4] dealt with the Ministry's request to the OIPC under s. 43 of FIPPA for authorization to disregard the applicant's request because it was frivolous or vexatious. Order F14-13 found that the request was not frivolous and vexatious, so s. 43 of FIPPA did not apply. The Ministry therefore processed the applicant's request, which ultimately led to this inquiry.

[8] **Record in Issue—**The information at issue is contained in the Logs, which reside on servers maintained by the Ministry's Office of the Chief Information Officer.[5] These servers coordinate the receipt and delivery of emails within the government email system and to and from external email systems.[6]

[9] The Logs contain more than twenty information fields about each email. Only four fields, containing the date and time of the message, an "event field", which states whether the email was sent or received, and a sender and recipient email address field, are in issue.[7]

[10] Prior to this inquiry the applicant agreed with the Ministry that all non-government email addresses that appear in the sender and recipient fields in the Logs would be anonymized. Because that information is no longer in dispute, I do not need to consider it.[8] The government email addresses in the Logs include the email addresses of employees of BC Government ministries and sixteen non-ministry organizations which are public bodies or within public bodies subject to FIPPA.[9] The Ministry states in its submission it would anonymize any government email addresses of individuals whose information is not published in the BC Government's online employee directory.[10]

---

[2] The Ministry refers to Order 03-06, 2003 CanLII 49170 (BC IPC), at para. 10 as an example.
[3] Order 03-06, 2003 CanLII 49170 (BC IPC) at para. 6.
[4] 2014 BCIPC 16.
[5] Ministry initial submission at paras. 5.05 and 5.06.
[6] Affidavit of D. Ehle at para. 12.
[7] Applicant submission at para 1.01; Ministry initial submission at para. 5.07.
[8] Applicant submission at para 1.02; Ministry initial submission at para. 3.04.
[9] Ministry initial submission at para. 5.13.
[10] Ministry initial submission at para. 5.12. The BC Government directory is located at www.dir.gov.bc.ca.

[11] The information requested is for the time period from January 1 to July 3, 2013. The Ministry estimates that if the responsive information was printed it would contain approximately 377 million lines of text. Given the size of the responsive record, the Ministry provided only a sample of the record for this inquiry.[11]

[12] I will now consider whether s. 22 applies to the information in issue in the Logs.

Section 22 of FIPPA

[13] Section 22 requires the Ministry to refuse to disclose personal information if disclosure would be an unreasonable invasion of a third party's personal privacy. Consistent with previous orders,[12] I have evaluated whether s. 22 applies by answering the following questions:

1) Is the information personal information of third parties?

2) If it is personal information, does it meet any of the criteria identified in s. 22(4)? (If so, disclosure would not be an unreasonable invasion of third-party personal privacy.)

3) If none of the s. 22(4) criteria apply, do any of the presumptions in s. 22(3) apply? (If so, disclosure is presumed to be an unreasonable invasion of third-party privacy.)

4) If any s. 22(3) presumptions apply, are they rebutted after considering all relevant circumstances including those listed in s. 22(2)?

5) If no s. 22(3) presumptions apply, after considering all relevant circumstances including those listed in s. 22(2), would disclosure be an unreasonable invasion of a third party's personal privacy?

[11] Exhibit to the Affidavit of D. Ehle in Ministry initial submission.
[12] Order F15-02, 2015 BCIPC 2 (CanLII).

Position of the Parties regarding s. 22

[14] The Ministry's submission is that the requested record contains personal information of employees that if disclosed would be an unreasonable invasion of personal privacy under s. 22 of FIPPA.

[15] The applicant's submission acknowledges that there may be some personal information in the record. He argues that the release of the personal information is outweighed by the benefits of disclosure,[13] in particular the ability to subject the BC Government to public scrutiny.[14]

Personal Information

Definition of Personal Information

[16] For s. 22 to apply, the information at issue in the Logs must be the personal information of a third party. FIPPA defines personal information as "recorded information about an identifiable individual other than contact information". Contact information is defined as "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual".[15]

Email addresses - personal information or contact information?

[17] The sender and recipient fields in the Logs contain employee email addresses. The Ministry says individual employees are identifiable from these email addresses because of the government's protocol on the format of employee email addresses. Government policy requires employee email addresses to use an employee's first and last name in the email address, typically in the format "*firstname.lastname@gov.bc.ca*".[16] The Ministry notes that there are some exceptions where, for example, there are "name collisions", which I take to refer to a situation where employees' names would result in more than one employee having the same email address. It also says there are some "positional" email addresses representing groups or functions rather than specific individuals that are contained in the Logs, for example "*helpdesk@gov.bc.ca*".

[13] Applicant submission at paras. 1.07, 2.01-2.02, 2.11-2.12.
[14] Section 22(2)(a) of FIPPA.
[15] See Schedule 1 of FIPPA for these definitions.
[16] Ministry initial submission at para. 5.27 citing Chapter 12 of the BC Government Core Policy and Procedures Manual and affidavit of D. Ehle at para. 25.

[18] The Ministry says that because BC Government employee's email addresses contain employee's first and last names, the sender and recipient of emails is easily identifiable where the employee email addresses appear in the record. As a result, specific employee's activities, namely the emails sent and received by the employee, are disclosed in the record. It cites Order F08-04[17] in support of the view that information that reveals an employee's activities is personal information.

[19] The applicant suggests that employee email addresses are contact information and therefore not personal information. He says that the publically available BC Government online employee directory[18] contains more information than what he is requesting.

[20] The Ministry submits that the information is not contact information. It acknowledges that while the addresses in the Logs are business email addresses, that the addresses are not contact information in this context because they do not appear in the Logs "to enable an individual at a place of business to be contacted…". The Ministry cites three orders in support of this submission.[19]

[21] I agree with the Ministry's submission that the presence of employee email addresses in the record means the record contains personal information. Because employee email addresses contain an employee's first and last name this identifies them with the email they sent or received. The other fields (date and time of email and whether the email was sent or received) in the record reveal when the employee sent or received an email, so in the context of appearing with the employee email addresses, they disclose personal information. Therefore, the information in issue in the Logs is personal information because it is information about the activity of identifiable individuals.[20] As Order F08-04 states:[21]

> [W]here the name and position of an individual employee appear in a context such that their disclosure would reveal the employee's activities, this will constitute the employee's personal information. Of course, the fact that one's name and position are personal information does not mean the information must be withheld if requested under FIPPA. The analysis goes further than that.

---

[17] 2008 CanLII 13322 (BC IPC).
[18] At www.dir.gov.bc.ca.
[19] Order F13-13, 2013 BCIPC 16 (CanLII), Order F08-04, 2008 CanLII 13322 (BC IPC) and Order 04-17, 2004 CanLII 7059 (BC IPC).
[20] See Investigation Report IR15-01, *Use of Employee Monitoring Software by the District of Saanich,* 2015 BCIPC 15 (CanLII) at Part 4.2 for a similar finding regarding the public bodies retention of copies of emails sent and received by employees.
[21] 2008 CanLII 13322 (BC IPC) at para. 20.

[22] I find that the information in issue does not contain contact information as defined in FIPPA. The employee email addresses in the Logs are "business email addresses", an example cited in Schedule 1 of FIPPA of the type of information that can constitute contact information. However, the purpose of the definition of contact information in Schedule 1 is to capture information "to enable an individual at a place of business to be contacted". The employee's email addresses do not appear in the Logs "to enable an individual at a place of business to be contacted".[22] The information appears because employees have sent and received emails and that information has been recorded in the Logs. The information in the Logs is therefore personal information and not contact information.[23]

Other personal information in the Logs

[23] The Ministry also says the Logs include emails that, even though only revealing the sender and recipient email address, will reveal sensitive personal information about employees. Some examples the Ministry provides are emails from government employees to BC Government occupational health nurses, government labour relations specialists, or to a union representative. The Ministry submits that email addresses belonging to BC Government occupational health nurses, government labour relations specialists and union representatives would be identifiable from other publically available information such as the BC Government employee directory or union contact lists. Thus, the Ministry submits, an email between a BC government employee's email address and one of these email addresses indicates that the employee had an interaction with an individual in one of those roles. I note that union representatives are also employees, so it will depend on what other information is known as to whether it is possible to determine if a particular email is to a union representative in their capacity as a union representative or simply as an employee.

[24] The applicant's response in his submission to the Ministry's concerns is to further narrow his request to allow the Ministry to automatically filter out any BC Government email addresses the BC Government identifies as potentially disclosing sensitive personal information including the examples cited by the Ministry. The applicant says the Ministry could use the same automated technology used to remove or mask other information he had previously agreed to exclude from the scope of his request (such as non BC Government email addresses). This argument relates to severing of the records, so I will consider it when I consider the issue of reasonable severing under s. 4(2).

[22] See Order F14-38, 2014 BCIPC 41 (CanLII) at para. 19 for a similar finding.
[23] See Order F13-13, 2013 BCIPC 16 (CanLII) at para. 18 for a similar finding.

[25] As the applicant concedes the point, I will proceed on the basis that emails that could disclose personal information, such as emails that demonstrate contact by an employee with a union representative or an occupational health nurse, exist in the Logs.

[26] The Ministry also says that the Logs will disclose information like work hours and leave taken by employees. I accept that the date and time field and the event ID field, which indicates whether an email was sent or received will indicate when employees who sent the emails were working. I note that employees may send emails outside of work hours, for example using remote access from home, so it may not be possible to discern precisely actual hours of work from email activity. However I accept that for some employees, the pattern of email activity disclosed in the Logs will give a fairly accurate indication of their work hours.

[27] The Ministry also says the record will indicate when an employee is on leave. They say the immediate reply to emails received, indicating the operation of an automated email response advising an email sender that the recipient is out of the office, combined with a lack of other emails being sent from a particular email address for a period of time will be indicators of employee leave. I note that some employees will respond to emails even when on leave, so being on leave will not always be correlated with lack of email activity. However, I accept that for some employees, patterns of emails that indicate the operation of an "out of office assistant" tool replying to emails will reveal personal information about employee leaves.

Personal information due to personal use of email

[28] The Ministry further says that the Logs will contain personal emails between employees that disclose employee personal information. They say that these personal emails will be identifiable in the Logs where, for example, the Logs show patterns of emails being exchanged between employees who do not need to correspond for work purposes. While this information may not be obvious to everyone who reviews the emails in the Logs, it will be discernible by those familiar with the employees through professional or personal relationships. If disclosed, individuals with a particular interest in certain employees would easily be able to search the Logs for patterns of email activity.

[29] While I have already found there is personal information in the Logs, it is necessary to consider whether the Logs reveal the sending and receiving of emails whose purpose was to communicate personal matters rather than work-related matters, because this affects the extent and nature of the personal information in the Logs. Understanding the extent and nature of personal information in the Logs is a necessary precursor to assessing whether disclosure

of personal information is an unreasonable disclosure of personal privacy under s. 22.

[30] In regards to personal use of email, the Applicant argues that for the time period of his request the BC Government's *Core Policy and Procedures Manual* required that employees have their manager's permission for the personal use of IT resources and advised employees that records created or transmitted using government equipment or retained in the government network would be managed as a government record. He therefore submits that any personal information in the Logs would exist in direct contravention of this policy.

[31] I find that it is reasonable to conclude that the sending and receiving of personal emails is reflected in the Logs. The Ministry and the applicant agree that it was not until 2014 that the Government's *Appropriate Use of Government Information and Information Technology Resources ("Appropriate Use Policy")* explicitly permitted reasonable personal use of government IT resources by employees.[24] However, I accept the Ministry's submission that actual practice was that personal use occurred, and was permitted, during and outside of an employee's work time before the 2014 policy change.[25] Personal use of email, even prior to the official 2014 policy change,[26] is consistent with common practice in the workplace. Personal use by employees of employer-provided telephones was recognized as an accepted norm in some of the OIPC's earliest decisions,[27] and in regard to internet and email use has been recognized by the OIPC[28] and the Supreme Court of Canada.[29] It is therefore reasonable to conclude that the Logs will include instances of personal email use and therefore disclosing the Logs will reveal patterns of personal email use. Some of this type of information will be sensitive information, because it could, for example, reveal personal relationships between employees.

---

[24] Ministry initial submission at para. 5.16-5.17.

[25] Official BC Government policy did not become more permissive until 2014. Ministry submission at para. 5.15.

[26] I note that the applicant suggests the change in the *Appropriate Use Policy* was possibly prompted by his request and as an act of bad faith in responding to his request. The Ministry says that the change was in process before the applicant's request occurred, and that the changes to the policy were prompted not by the applicant's request but by the reality that limited personal use of email was the norm. I do not see any evidence to support the applicant's suggestion of bad faith on the part of the Ministry, which has negotiated with the applicant regarding his request, albeit without success, in an attempt to reach a solution. I prefer the Ministry's explanation for the policy change, which as I have noted above, is congruent with commonly accepted policy that incidental personal use of employer provided communication equipment is permitted.

[27] See Order No. 63-1995, 1995 CanLII 2863 (BC IPC) applied in Order No. 64-1995, 1995 CanLII 2240 (BC IPC), Order No. 65-1995, 1995 CanLII 549 (BC IPC) and Order 04-17, 2004 CanLII 7059 (BC IPC).

[28] Order F07-18, 2007 CanLII 42407 (BC IPC) references a University of Victoria's "incidental personal use" policy in force at the time of that inquiry. See also Investigation Report F15-01, *Use of Employee Monitoring Software by the District of Saanich,* 2015 BCIPC 15 (CanLII) at para. 1.1.

[29] *R v. Cole,* 2012 SCC 53 (CanLII).

[32] The applicant raises a related argument about whether it was reasonable for employees to use government email for personal use. In my view this argument ultimately concerns whether personal information *should be* in the Logs, not whether it is in fact. This argument is more appropriately considered when weighing the circumstances for and against whether disclosure of personal information is an unreasonable invasion of personal privacy. I will therefore address it when considering all the relevant circumstances under s. 22(2).

Summary - Personal Information

[33] In summary, the Logs contain and reveal personal information of BC Government employees. Because of the presence of employee email addresses in the Logs, the Logs reveal the work activities of identifiable BC Government employees, which is the employee's personal information. The Logs will also disclose personal information about employees based on who they emailed, for example emails to union representatives. The Logs will also reveal personal information about employee's work hours and leave. Finally, the Logs will contain personal emails. The patterns of personal (non-work) email use could disclose employee personal relationships.

Personal information of third parties

[34] Section 22 concerns personal information of third parties. The applicant argues that government employees are not third parties but are rather part of the public body – i.e., the Ministry.[30] The Ministry responds that the Commissioner has found that public body employees are third parties for the purposes of s. 22 of the Act and cites Order 00-53[31] as an example of this view. I agree with the Ministry's submission that public body employees are third parties for the purpose of s. 22.

Section 22(4) Factors

[35] Section 22(4) sets out circumstances when disclosure of personal information is not an unreasonable invasion of a third party's personal privacy. Specifically, s. 22(4)(e) relates to information about a third party's position, function or remuneration as an officer, employee or member of a public body or as a member of a Minister's staff. The Ministry accepts that a portion of the information in the Logs falls within s. 22(4)(e).[32] I agree that the Logs disclose information that relates to employee's positions and functions. For example, the email address information in the Logs reveals information related to the positions of employees. However, as I have discussed above, in context, the same information in the Logs discloses information such as employees leave activities

[30] Applicant submission at para. 3.03.
[31] 2000 CanLII 14418 (BC IPC).
[32] Ministry initial submission at para. 5.46.

or personal relationships that does not fall within s. 22(4)(e), so the issue of whether it is possible to sever and disclose information arises. I will address whether severing is reasonable when discussing s. 4(2) below.

Presumption of Invasion of Privacy – s. 22(3)

[36] Section 22(3) provides the circumstances in which disclosure is presumed to be an unreasonable invasion of a third party's personal privacy. The Ministry submits that ss. 22(3)(a) and (d) apply in this case. Section 22(3) states in part:

> A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if
>
> (a) the personal information relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation,
>
> …
>
> (d) the personal information relates to employment, occupational or educational history,
>
> …

Medical information – s. 22(3)(a)

[37] The Ministry suggests that s. 22(3)(a) is relevant because the records will contain correspondence by government employees with BC Government occupational health nurses. They say that these types of emails, combined with a lack of other emails for an employee for a particular time period during or after emails to an occupational health nurse indicates that an employee is absent from work for medical reasons. Based on the original scope of the applicant's request,[33] I accept that some information that falls within s. 22(3)(a) could be discerned from the Logs, so that s. 22(3)(a) applies.

Information relating to a third party's employment history – s. 22(3)(d)

[38] Disclosing personal information that relates to a third party's employment history is a presumed invasion of that person's privacy under s. 22(3)(d). The Ministry says s. 22(3)(d) is relevant because the Logs will reveal information about employee leave history and hours worked. It cites Order F15-17[34] in support of this position. Order F15-17 found that information about the number of hours worked in an employee's pay statement in some instances disclosed details of the employee's leave activities, which is generally considered to be an

[33] I address the applicant's narrowed request that would mask or remove email addresses such as those for occupational health nurses in discussing severing under s. 4(2) below.
[34] 2015 BCIPC 18.

employee's work history and therefore falls within s. 22(3)(d).[35] One example it provides of how leave activities could be disclosed is because an analysis of the Logs would reveal when an employee is not using government email or has out of office automatic replies operating.[36]

[39] I have already accepted that personal information in the Logs will allow hours of work and periods of leave to be fairly accurately determined for some employees. I have noted already that some employees may access email outside of work hours and, of course, as the Ministry acknowledges, for personal emails. Also, a period without email use could be attributable to being absent for several different reasons, including work–related ones such as attending conferences or other work activities. Nonetheless, I accept that the pattern and timing of email usage will indicate information such as leave for some employees. That information could in some cases be combined with other available information to confirm an applicant was on leave. Therefore, some information in the records will reveal information that falls within s. 22(3)(d).

Section 22(2) Factors

[40] There is a presumption that disclosure of some of the information in the Logs would be unreasonable because it would disclose information that falls within ss. 22(3)(a) and (d), but it can be rebutted. Section 22(2) requires that public bodies must consider all relevant factors, including those listed in s. 22(2), in determining whether disclosure of personal information is an unreasonable invasion of privacy.

[41] The Ministry submits that there are no factors under s. 22(2) that rebut the s. 22(3) presumptions or are in favour of disclosure of the information. It suggests several factors that are in favour of withholding the information, including that disclosure may unfairly damage the reputation of any person referred to in the record (s. 22(2)(h)), that employees have a reasonable expectation of privacy and that any disclosure of the Logs must be considered to be disclosure to the world at large.

Disclosure desirable for public scrutiny- s. 22(2)(a)

[42] The applicant says s. 22(2)(a) is a factor in favour of disclosure. Section 22(2)(a) prompts considering whether disclosure is desirable for the purpose of subjecting the activities of the government of British Columbia or a public body to public scrutiny.

[35] Order F15-17, 2015 BCIPC 18 at para. 35.
[36] Out of office emails would be detected by repeated instances of a very short duration between receipt and sending of an email from an employee's email address, denoting an automated reply.

[43] In support of s. 22(2)(a), the applicant provides examples of the insight that could be gained if the requested information were made available to him to analyze. This includes the ability to compare the Logs with responses to previous freedom of information requests for email records to cast light on Government email retention habits. However, the applicant says his primary motivation for the request is to enable him to map relationship diagrams between employees in the government which would allow him to provide insight into various aspects of the organizational dynamics of the BC government.

[44] I accept that the information in issue could be used to subject the government to scrutiny by revealing patterns of interactions between its employees that could suggest patterns of influence and relationships that indicate how decisions are made and who is involved in them. This is a factor that weighs in favour of disclosure of the records.

Unfair damage to employee's reputation- s. 22(2)(h)

[45] The Ministry says the records may suggest that personal relationships exist between employees. If one or both employees has a spouse, and the Logs incorrectly suggest a personal relationship between employees other than the spouse, it says this would unfairly damage the employee's reputation. While the scenario outlined by the Ministry is somewhat speculative, given the large number of records within the request I accept it is a realistic possibility, and therefore is a factor to consider.

Other Factors

Reasonable expectation of privacy

[46] Previous orders, including those dealing with requests for logs of telephone calls, have recognized that employees have some reasonable expectation of privacy regarding their personal information, even where that information is generated in a workplace. This has been recognized, and the scope of the expectation considered, for example, in the Supreme Court of Canada decision in *R. v Cole*[37] and by the OIPC in Investigation Report F15-01. Without an extended discussion of the precise extent of employees' expectation of privacy in this particular context, it is nonetheless a factor that provides some support for the personal information in the Logs being withheld.

Disclosure is disclosure to the world

[47] As with any contemplated disclosure under FIPPA, disclosure of records must be considered to be public disclosure, with no limit on further dissemination

[37] 2012 SCC 53 (CanLII).

of the records in issue.[38] This is a factor I have considered in determining what personal information may be discerned from the Logs. Specifically, I have recognized that some individuals who review the Logs could combine the Logs information with other information and that the patterns of emails might reveal personal relationships to certain individuals not evident to others.

Reasonableness of personal use of email

[48] I have already found above that employee use of government email for personal use was accepted and was ultimately reflected in BC Government policy.

[49] Regardless of the policy or practice, the applicant questions whether a reasonable government employee would *in practice* use their government email for personal use. He accepts that previous orders found that employees can be expected to mix personal and work use of government IT equipment, but he suggests that this was because at that point in time employees only email and phone access may have been via their government-issued email and phone. He says the technological setting of his request sets it apart from these earlier orders that deal with telephone logs, and he points to the prevalence of free web-based email services, as well as personal cell phones and smartphones. He says that there is no longer a reason for employees to use government IT infrastructure for personal use because employees have access to personal communication devices which they can use for any personal needs they may have.

[50] The Ministry agrees that the availability of technology has changed. It submits that, nonetheless, for reasons of ease of access and convenience employees still make personal use of government email. It further notes that this is particularly the case for employees who have access to their government email from mobile devices. It also explains that for security reasons the government restricts access to web-based email providers. This leaves employees who want to send emails from their government-issued computer or other communications device with little choice but to use their government email address.

[51] While accepting that technology has changed substantially since the cases involving telephone logs were decided, for the reasons outlined above, I accept that mixed personal and business use of government technology remains the reality. The fact that patterns of personal email use will appear in the records as a result of reasonable personal use of Government IT resources is a circumstance that weighs against disclosure of the information.

[38] See Order 01-52, 2001 CanLII 21606 (BC IPC) at para. 73.

Section 22(1)

[52] The applicant argues that the balance of factors relevant to the s. 22 issue weighs in favour of disclosure because of "the weak nature of the personal information that might be discoverable within the patterns of the log files and the strong nature of the information about government operations that will be available in the logs."[39]

[53] The Ministry accepts that some of the personal information in the Logs discloses only employee's positions and functions, and falls within s. 22(4)(e), and therefore would not be an unreasonable invasion of personal privacy to disclose.

[54] However, the Ministry's evidence demonstrates that the Logs reveal personal information, including information that is subject to a presumption that disclosure would be an unreasonable invasion of personal privacy. Against that, I recognize the valuable insights into the practical workings of government that could be gained from the applicant having access to the information.

[55] However, this is insufficient to rebut the presumptions that apply to some of the information or to overcome the invasion of personal privacy that would result from disclosure of the Logs. Disclosure of some information in the requested information in the Logs would be an unreasonable invasion of personal privacy under s. 22.

[56] This conclusion is consistent with other previous cases involving requests for logs of telephone calls, which found that disclosure of the logs was an unreasonable invasion of personal privacy under s. 22.[40]

[57] To be clear, my conclusion does not mean that metadata in the Logs can never be disclosed under FIPPA. The breadth of the applicant's request means that the volume of responsive information allows patterns to be discerned that make disclosure in this particular case an unreasonable invasion of personal privacy. In a smaller subset of the same type of information, such patterns may not be so easily discerned so the personal privacy issues may be different.

[58] In conclusion regarding s. 22(1), I find that it would be an unreasonable invasion of third party personal privacy to disclose the information requested in the Logs. I will now consider whether it is reasonable under s. 4(2) of FIPPA for

[39] Applicant submission at para. 2.02.
[40] Order No. 63-1995, 1995 CanLII 2863 (BC IPC) applied in Order No. 64-1995, 1995 CanLII 2240 (BC IPC), Order No. 65-1995, 1995 CanLII 549 (BC IPC) and Order 04-17, 2004 CanLII 7059 (BC IPC). See also Order F13-13, 2013 BCIPC 16 regarding a request for cellphone bills which included a log of calls.

the Ministry to sever information that can be withheld under s. 22 from the Logs and disclose the remaining information.

Section 4(2) severing

[59] As the Ministry acknowledges, the Logs contain some information the disclosure of which would not constitute an unreasonable invasion of personal privacy to disclose under s. 22(4)(e).

[60] The applicant concedes that a manual review of the information in the Logs in order to sever personal information in them would not be reasonable.[41] I agree and note, as the applicant does, that a manual review of the information would likely not even be effective in identifying instances of sensitive personal information in the Logs. The sheer volume of the information alone would make it virtually impossible for a manual review to identify all of the patterns in the information that disclose personal information. In some instances, personal information in the Logs, such as personal relationships between employees, may only be revealed by automated analysis that discerns patterns across the many millions of lines of text in the record.

[61] The applicant queries whether personal information such as instances of reasonable personal email use could be removed from the Logs using automated filtering. There is no evidence before me that suggests that there is a way to automatically filter out this kind of personal information of BC Government employees contained in the Logs. This is because context is required to discern that emails between BC government employees reveal personal rather than simply professional relationships. Such context might only reveal itself by asking the employee or employees about the nature of their interactions. Some personal information might also be revealed when the information in the Logs is combined with other available information to which the public may have access. In both cases, automated severing would not prevent such disclosures. There is no evidence before me that any automated review of the Logs could accurately discern, and therefore mask or remove, this type of personal information.

[62] The applicant argues that email addresses whose disclosure would be an unreasonable invasion of privacy could be automatically severed by the Ministry.

[63] The Ministry's reply submission argues there are practical difficulties with this suggestion. The Ministry says that it is not possible to reliably identify all the email addresses whose disclosure could be an unreasonable invasion of privacy because of what they might reveal about personal relationships or matters related to health or employment history. It says it does not have an exhaustive list of such email addresses and that any such list would change with time, for

[41] Applicant submission at paras. 1.05 and 1.06.

example with changes to an employee's personal circumstances such as their relationship status with regard to another employee.[42]

[64] The Ministry further responds by saying that even if it could successfully remove some email addresses from the Logs, personal information whose disclosure would be an unreasonable invasion of privacy could still remain in the Logs. This is because it cannot anticipate and remove all information in the Logs that if disclosed would reveal personal relationships between employees, when an employee is on leave, or work and overtime hours.[43]

[65] I accept that, even if the Ministry was to use its best endeavours to identify and remove some email addresses, the responsive information in the Logs will still contain personal information of employees because of the range of personal information revealed by the records. Given the nature of the personal information in the requested information, there is no evidence that there is an automated method to selectively remove only the personal information from the Logs whose disclosure would be an unreasonable invasion of privacy under s. 22.

Possible severing

[66] In my view, it may have been reasonable under s. 4(2) to sever all the email addresses. The remaining fields in the Logs (date/time stamp and whether an email was sent or received) ("Remaining Information") would, it appeared to me, no longer be information about identifiable individuals and, therefore, not personal information for the purposes of FIPPA and s. 22. Based on the evidence of the Ministry,[44] it appeared that an automated process could have been used to prepare a record containing only the Remaining Information. It therefore would not be unreasonable from a practical standpoint to sever the sender and recipient email address fields and disclose the Remaining Information to the applicant.

[67] Neither the applicant nor the Ministry addressed this option for severing the records in its submission so I sought simultaneously the applicant's interest in receiving the Remaining Information, and the Ministry's position on disclosure of the Remaining Information if the applicant indicated he wanted it. The applicant's

[42] The Ministry also says that as the applicant's request to remove sensitive email addresses is essentially a new request, it would want to make a submission on the application of s. 6(2) of FIPPA to it. Section 6(2) relates to whether it is possible for the Ministry to create a record and whether it is unreasonable to require it to do so. The Ministry says its argument under s. 6(2) would be that producing the Logs with sensitive email addresses severed would be unreasonable.[42] It is not necessary to make a decision about the Ministry's request to make submissions on s. 6(2) given my conclusion regarding s. 22 and s. 4(2).

[43] Ministry reply submission at para. 4.

[44] The affidavit of D. Ehle at para. 22 estimates that it would take 35 hours to prepare the Logs requested, including anonymizing non-government email addresses. Presumably creating the Remaining Information, which contains less fields of information and requires no anonymization at all, would take less than 35 hours.

response that he did not want the Remaining Information meant I did not consider this option for severing and disclosing the information further.

Applicant's request for direction regarding personal use of government equipment

[68] The applicant suggests that if this inquiry finds that harm from disclosure of personal information in the Logs outweighs the benefits of public access, the Commissioner should direct that government employees limit their personal use of government equipment or flag personal communications at the time of creation to avoid contaminating government data. The Ministry's reply states that such an order would be outside the Commissioner's powers.

[69] In my view, the applicant's request, whether within the Commissioner's powers or not, would be ineffective in facilitating the access to, and public scrutiny of, the requested records. The Logs disclose patterns and information about employee's leave and other personal information that it is typically an unreasonable invasion of personal privacy to disclose. It will appear in the records even if no personal use of emails by government employees were to occur so I do not see that removing personal emails from the Logs will facilitate access to the Logs.

CONCLUSION

[70] For the reasons given, under s. 58 of FIPPA, the Ministry must continue to refuse to disclose the requested information in the Logs under s. 22 of FIPPA.

November 24, 2015

ORIGINAL SIGNED BY

Hamish Flanagan, Adjudicator

OIPC File No.: F14-58135