OIPC File F14-58135

In the matter of the application by the

Ministry of Technology, Innovation and Citizens' Services (Public Body)

for authorization under section 22

of the Freedom of Information and Privacy Act (the Act)

to refuse access to records to Paul Ramsey (Me/I).

May 4, 2015

Paul Ramsey
1684 Chandler Avenue
Victoria, BC, V8S1N6
pramsey@cleverelephant.ca

Summary

Almost two years ago, I requested the contents of the message tracking logs maintained by the provincial government's internal email servers. Such logs are maintained by mail delivery software and retain a record of who sent email, to whom, and at what date and time.

Message tracking logs are a valuable source of information about the existence of email records created by government. Unlike the emails themselves, the entries in the logs cannot be directly deleted by the sender or recipient. Given the context of incidents at the time[1], and even today[2], regarding government staff destroying electronic records that provide critical insight into government policy development, the publication of such logs would be a valuable corrective.

Message tracking logs are also an important source of information about organizational dynamics. Government reorganizes itself almost monthly (it seems), but what about the active daily information flows of government--are they reorganized at the same time? Who really reports to whom, regardless of organizational charts? Analysis and visualization of log files could illuminate the centrality and influence of particular positions and organizations within government.

---

[1] http://www.theglobeandmail.com/news/british-columbia/probe-into-boessenkool-affair-oddly-lacking-a-paper-trail/article4900224/
[2] http://thetyee.ca/News/2015/04/21/BC-Liberals-Freedom-of-Information/

Since the logs contain third-party e-mail addresses, and some specific information in the form of subject-line text, I knew that they would have to be automatically filtered to remove that information, and I met directly with representatives of the Public Body to confirm the details of that automatic filtering. The Public Body acknowledged at that meeting, and in subsequent affidavits, that automatic filtering would consume computer time, but relatively little staff time.

After that meeting, the Public Body nonetheless began proceedings under Section 43 of the Act to declare my request vexatious. When the Commissioner rejected their arguments, the Public Body instead moved to deny access under Section 22.

In my response during the Section 43 proceeding, I advanced the argument that, according to the government's own *Core Policy and Procedures Manual*[3] (12.3.1 (3) and 12.3.1 (4)), government employees were restricted from using government computers for personal purposes and were explicitly warned that any records produced using government equipment would be treated as government records.

Within a month of my advancing that argument, the manual was changed, to state that "Reasonable personal use of government IT Resources by Employees is permitted"[4]. As a result, I have some concerns about whether the government is pursuing this process in good faith.

---

[3] http://s3.cleverelephant.ca/oipc/2014_s43_hearing/citz_submission/Ehle%20Aff%20sworn%20Feb%2028-14.pdf#page=11

[4] http://www.cio.gov.bc.ca/local/cio/appropriate_use/policy.pdf#page=10

I submit that the Public Body could sever all important third party information using automatic means, and deliver the data with little staff effort, that the Public Body does not need to manually review log records to do so, and that the known value of the logs in holding the government to public scrutiny outweighs the unproven harms the Public Body asserts may occur.

1. Effective Severing of Third Party Information

1.01 As described in the Public Body in their 5.07, the only information requested is the From, To, DateTime and MessageID fields of the message tracking logs. The logs contain much more data, but the Public Body is capable of removing that data automatically, and agreed to do so in an early meeting.

1.02 Once the data have been reduced to From, To, DateTime and MessageID, there will still be records that include the email addresses of non-government persons. The Public Body is capable of anonymizing those email addresses automatically, and agreed to do so in an early meeting.

1.03 Once the third-party addresses have been anonymized, the Public Body is capable of automatically filtering any further sensitive email addresses (employment counselors, pension addresses, survey research addresses) that they feel are obvious markers of potential personal information patterns. This was not previously discussed with the Public Body, but is a straightforward application of the same technology used for 1.01 and 1.02.

1.04 At the end of the process, the result is a set of records (some hundreds of millions) consisting, on each line, of

- An email from "someone@gov.bc.ca" and to "someoneelse@gov.bc.ca", a timestamp and message number. (In addition, emails of other known public bodies, e.g. "@bcferries.com" would appear.)

- An email from or to "someone@gov.bc.ca" and from or to "d41d8cd98f00b204e9800998ecf8427e" (where the latter is an anonymous checksum of the original email address), a timestamp and a message number.

1.05 At no point have I proposed the manual review of records to sever personal information, nor would any reasonable applicant make such a request.

1.06 The question is **not** whether the effort to manually review the data line by line would be reasonable: it would not be. Nor would a line by line manual review be particularly effective, given the low information density of the records.

1.07 The question at issue is (a) whether there are likely to be consequential personal information patterns in the records and (b) whether the downside of the release of the data that may include such patterns outweighs the upside of public access to study the other patterns of government business activity that are present in the data.

2. Disclosure in the Public Interest

2.01 I submit that the disclosure of the message tracking log files, severed in the manner described in section 1 above, would be acceptable under the Act, under section 22.2 (a) in order to "subject the activities of the government of British Columbia ... to public scrutiny".

2.02 I submit that in this case the balance of 22.2 falls in favor of public scrutiny 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.

2.03 The logs in question were generated during a period when the government *Acceptable Use Policy* for computer equipment stated **explicitly** that (12.3.1.C.3) "Employees must have their manager's permission for the personal use of IT resources." and (12.3.1.C.4) "Any content created or transmitted using government equipment or retained within the government network will be managed as a government record." Given that policy, any personal information patterns present would only be there as a direct contravention of government policy and conditions of employment.

2.04 The government changed the *Acceptable Use Policy* one month after I presented the arguments in 2.03 at the Section 43 hearing that preceded this one. The new policy states that "reasonable personal use of government IT Resources by Employees is permitted."

2.05 Notwithstanding that the new policy does not apply to the records under dispute here, it is worth discussing whether "reasonable personal use" of government email would result in patterns that could not be automatically removed by filtering as described in Section 1 above, and also whether a reasonable government employee in the current era would use their government email for such purposes.

2.06 Technology conditions have changed substantially since the decisions by the Commissioner cited by the Public Body in their 5.60-5.73. In 1995, the time of the earliest decisions, a government employee's only email access would be a government one, as would their only access to a phone. Given such conditions of access, they might reasonably be expected to freely mix personal and business uses of that equipment.

2.07 By 2004, when the later decisions by the Commissioner were made, government employees would have access to numerous free web-based email services (gmail, hotmail, yahoomail, and others) that they could access via their web browsers, leaving no records in the government email message tracking logs at all. However, personal cell-phones were not yet ubiquitous, and the personal smart phone had not been invented yet--the iPhone was introduced in 2007, and the first Samsung touch screen phone in 2008.

2.08 In the current day, not only has the number of free web-based email options expanded even further, but the ubiquity of personal smart phone technology

means that employees can access personal communications of all kinds (voice, SMS, email) without ever touching government equipment.

2.09 Given the trend of cheap and easy access to personal equipment for personal communications, the government's liberalizing of the Acceptable Use Policy on personal use of government equipment is hard to understand. There is less and less reason for employees to use government equipment for personal purposes, and such use may potentially taint government records (hence this process). If the Commissioner does in fact rule that the potential for patterns of personal information in log files outweighs the benefits of public access to the data, I hope the Commissioner would pair such a ruling with a directive to limit personal use of government equipment, or to require employees to flag personal communications at the time of creation, to remove the taint of potential personal information from future government data.

2.10 All mails generated on government equipment and delivered via the central email systems that generate the log files in dispute are from "someone@gov.bc.ca". In addition to being a valid SMTP[5] delivery address, the email address has a social signifier, namely, "this is from someone at this place of business". As e-mail has become more culturally embedded in our society, and available to users for free in non-work contexts, the meaning of

[5] https://www.ietf.org/rfc/rfc2821.txt

being "@" a particular domain has become more socially determined: an email from "someone@gov.bc.ca" is official, while an email from "someone@hotmail.com" is not. Government employees live in this social context and condition their behavior accordingly, regardless of the acceptable use policy.

2.11 The message tracking logs are an important example of a government record, in that they are a huge corpus of data which should, because of their uncontroversial nature (from, to, date, id) be immediately releasable, but because of the **possibility** of personal information patterns, have become subject to this contentious process. Imagine a document warehouse full of boxes of completely uncontroversial, releasable files. Imagine that the government refuses to release the files, because an employee at the warehouse may have placed his university transcript in one of the boxes. They are not sure he did so or not, but the effort of searching all the boxes is too high, therefore none of the boxes is releasable.

2.12 The situation with email logs is fundamentally the same. The question is not whether the effort of searching the boxes is too high: that's a given, it's too high. The question is whether the potential presence of a small piece of personal information is sufficient to block the release of a huge volume of public information.

2.13 The Public Body raises numerous examples of **potential** personal information that **might** be deducible from the message tracking log files, but

can only point to two **specific** instances, of a health club email, and survey research emails (both of which could actually be removed with additional filtering). These specific instances must be held up against the several hundred million actual records of government business within the log files they are withholding on the basis of (unproven) potential personal privacy information.

2.13 The other side of the section 22.2 (a) argument, the value of the message tracking log files "to subject the activities of the government of British Columbia ... to public scrutiny" is also significant.

2.14 As the Public Body showed in having BC Stats carry out a network analysis of the records, there is substantial value to be gained through examining how information flows through the government. The implicit structure in message flows can be compared to the explicit structure of the organization. Among the large scale questions that could be examined are:

- Notwithstanding the organization chart, whom does this government department really report to?
- Are political staff directly influencing government employees outside the public service chain of responsibility?
- Does changing the Ministerial reporting relationship of a branch change the actual reporting relationship of the branch?

- Does message activity ebb and flow with policy importance? Can the priorities of government be inferred from message activity, like watching the neurons of particular sections of the brain light up in an fMRI?

2.15 Narrower questions of government policy and procedures can also be addressed with the log files. Government behaviour with respect to preservation of electronic documents has been increasingly egregious. Many of the "no documents" responses catalogued by the Commissioner[6] have involved requests for e-mail documents, and there have been several high profile examples of important e-mails being deleted[7] or allegedly never being sent[8].

2.16 The message tracking log files are a unique record of what e-mails have been sent--a record that cannot be altered or deleted by the senders or recipients. An e-mail may be deleted by the sender and/or the recipient, but the **record of its delivery** always remains in the log files.

2.17 In cases like NGD-2014-00121[9], where a Ministerial Chief of Staff rather improbably asserted that he had sent only three e-mails of a non-transitory

---

[6] https://www.oipc.bc.ca/investigation-reports/1510
[7] http://thetyee.ca/News/2015/04/21/BC-Liberals-Freedom-of-Information/
[8] http://www.theglobeandmail.com/news/british-columbia/probe-into-boessenkool-affair-oddly-lacking-a-paper-trail/article4900224/
[9] http://www.openinfo.gov.bc.ca/ibc/search/detail.page?config=ibc&P110=recorduid:6263106&title=FOI%20Request%20-%20NGD-2014-00121

nature over a the period of nine working days (and deleted the rest), a permanent record of actual e-mail transactions would be an admirable corrective. As a general rule, government assertions that decisions are made entirely "orally"[10] are not currently independently verifiable. Access to the message tracking logs would change that.

3. Specific Responses to the Submission of the Public Body

3.01 In 5.18, the Public Body states that, "if required to sever information within records, the IAO must manually review each processed record on a line by line basis to determine if the remaining information contained in the records ... may or must be withheld". While it is unlikely that manual review would result in any actionable discoveries (how many lines of information can a reviewer hold in his head at once, bearing in mind each line contains only To-From-Timestamp information), the important fact is that automatic severing can remove all definitive personal information, and all that remains is the balance of whether the public value of the 370 million records exceeds the unspecified harm the Public Body asserts will result from an analysis of a handful of those records.

3.02 In 5.24, the Public Body submits that the information in the message tracking logs is not contact information, even though the data consist of nothing but

---

[10] https://fipa.bc.ca/oral-culture-at-top-levels-of-government-grows-under-open-government-premier-4/

lines of text containing two emails, a date, and a message number. The data are in fact almost nothing but contact information. The publicly available government directory[11] contains more information than the message tracking logs files, holding, as it does, names, emails, phone numbers, job titles, and complete organizational structures.

3.03 In 5.29, the Public Body submits that the information in the message tracking logs is about "third party employees", which is an awkward construction. Information about "third parties", that is, persons not employed by the Government of BC, is to be severed using the automatic means as already agreed upon by the Public Body. What remains is information about "employees", who are members of the government of British Columbia and are generating government records on their government equipment and transmitting them to government servers for storage and delivery over the government network.

3.04 In 5.31, the Public Body argues rather broadly that "disclosure of the [government] employee's activities will constitute the employee's personal information". As a general principle applied to government employees carrying out the business of the public, this seems to foreclose numerous avenues of inquiry about the business of government, since most government business does involve the activity of it's employees.

---

[11] http://www.dir.gov.bc.ca

3.05 In 5.31, the Public Body further notes that "a portion of emails will be made by employees for personal reasons, rather than work related reasons" and it is worth reminding the reader here that what is at issue is not content of emails, but rather, for each email sent in government between government employees, the record of who it was sent **from**, who is was sent **to**, and **when**. Nothing more.

3.06 In 5.33, the Public Body notes that message tracking logs contain the record of who it was sent **from**, who is was sent **to**, and **when.** They note that "it is information about an identifiable individual". More specifically, it is about an identifiable government employee, using government equipment and a government email of the form "@gov.bc.ca", indicating the business-oriented nature of the communication.

3.07 In 5.36, the Public Body ignores the important public policy implications of access to this data, since the data cannot be said to only produce a "robust picture of an employee's interactions", they **also** produce a robust picture of the operations of government that is otherwise not available. And of course the picture of employee interactions the data produces is almost entirely a picture of their professional interactions in the course of pursuing public business.

3.08 In 5.38 to 5.40, the Public Body makes the case that analysis can reveal a great deal about the operations of government, which is one of the points of this access request.

3.09 In 5.41, the Public Body enumerates a number of specific cases where point-to-point delivery information might allow non-employment-related information to be inferred. They do not then enumerate the ways in which automatic filtering might remove references to the particular addresses of concern (pension corporation, health nurses, union officials, fitness centre), but instead jump to the conclusion that manual inspection of millions of records is required. Removing particular addresses from a corpus of millions is work for computers, not IAO staff, and suggesting that millions of dollars are required to remove those references is not working within the spirit of open data access.

3.10 In 5.42, the Public Body admits that, despite all previous assertions, they are not actually sure any personal information exists in the message tracking logs, only that they are pretty sure there might be, and that the only instance they managed to find involved an email to a fitness center (which could be easily purged from the list by adding the fitness center contact email to the list of emails to be removed from the corpus of data).

3.11 In 5.54, the Public Body enumerates the individual work time information that **might** be deduced from log file information (bearing in mind that it cuts against their implication that work emails are used extensively for personal purposes) but does not mention the public policy benefit of being able to independently verify the extent to which the government relies on out-of-hours and overtime labour. Further, investigation of the individual work

habits of particular employees does not require access to email log files, only the occasional monitoring of a few government parking lots.

3.12 In 5.57, the Public Body states that "employees do not check their privacy rights at the door", and indeed they do not in an absolute sense; but they do accept that their employment makes their rights contingent, particularly with respect to storing their own information on their employers systems. As the Public Body's own (current) Acceptable Use Policy[12] states in Section E.25, "Any collection, access, use, transmission, or disposal of Government Information or use of government IT Resources, **whether for personal reasons or not**, may be audited, inspected, monitored and/or investigated" and proceeds to enumerate a very liberal list of reasons for such investigations. So, the **actual content** (not just the transmission logs) of employee's personal emails may be accessed by their employer, for reasons as critical as "improving business processes and managing productivity". With respect to their employer, BC government employees do in fact check their privacy rights at the door.

3.13 In 5.59 and 5.60, the Public Body again describes a case of potential personal information in the logs without being able to guarantee the actual existence of such information. Laid against clear public policy benefits of access to the data, and the extensive access employees have to non-government

---

[12] http://www.cio.gov.bc.ca/local/cio/appropriate_use/policy.pdf

communications channels, the **possible** existence of edge cases such as this is not a reasonable objection to release.

3.14 In 5.69, the Public Body notes the decision of the Commissioner in 1995, which appears similar to this case, but in its technical fundamentals is not. In 1995, the City of Vancouver could not **automatically** sever all records relating to non-government business. The Public Body, on the other hand, can use automatic filtering to only retain government-to-government records, while anonymizing government-to-outside records, to meet this request without undue effort. Further, in 1995 City of Vancouver employees would have had access **exclusively** to government equipment for communications: there were no cell phones or alternate non-governmental means to carry out their personal communications, so the Commissioner was correct in inferring that a large volume of the records would be related to personal communication. In 2015, this circumstance no longer applies.

3.15 In 5.70 and 5.71, the Public Body points to decisions in which the volume of effort required to sever outweighed the public benefit to be obtained. I would submit that, given the automatic severing already agreed to and demonstrated by the Public Body (in providing data to BC Stats), the effort of severing is not an issue in this case. The only issue is the relative public benefit of access to the data weighed against the potential personal information the Public Body asserts exists within the data.

3.16 In 5.74, the Public Body refers to the cost of developing software to automatically sever records, in relation to a previous decision, but does not note that the Public Body has already developed the computer scripts needed to sever data to the standards in this request and has applied them to the log files in providing example data to BC Stats.

3.17 In 5.79, the Public Body states that "message tracking logs reveal a picture of who an individual is interacting with, how frequently they are interacting, and when", but that is an overbroad description, since the requested logs only describe what government employees a government employee is interacting with, and further only when that interaction is via their "@gov.bc.ca" email accounts. The question is not whether interaction is occurring, since it is their job to interact, it is whether the patterns of those interactions includes personal information so consequential that it outweighs the release of the rest of the data to the public.

3.18 In 5.81, the Public Body provides a perfect example of an additional filtering rule that can be easily added to their automatic processing: if there is concern that the presence of web survey emails show who is receiving surveys, simply add the indicated email address to the filter of addresses to be removed. The answer is not to manually review all addresses, the answer is to identify reasonable improvements to the log filtering process that balance the public interest against personal information protection and apply those rules automatically.

3.19 In 5.82, the Public Body asserts that "while some lines will require no severing, others will require investigation and severing of information by the IAO". Before accepting that manual investigation is required (or useful), the Commissioner should ascertain what, on the basis of "From", "To" and "Date" fields, would prompt an IAO staffer to conclude that one record required investigation while another would not? In particular, what conditions that could not be trivially added to a computer filter.

3.20 In 5.84, the Public Body again asserts that manual review is both required and useful, and proceeds to calculate some numbers, which is an amusing intellectual exercise, but not relevant to the actual request. If there is personal information embodied in the patterns of the data, manual inspection of the data will not reveal them (as the Public Body tacitly admits in 5.37).

4. Relief Sought

4.01 I seek an Order from the Commissioner that the Public Body release the requested records after automatic severing as described in Section 1 here and in the affidavits filed by the Public Body.

4.02 In the event the Commissioner rules that the records cannot be effectively severed using the automatic process or using an enhanced automatic process, I request that the Commissioner also Order the Public Body to enact

acceptable use policies such that future electronic records will not be tainted by potential patterns of personal information.

Respectfully Submitted,

May 4, 2015

Victoria, British Columbia

Paul Ramsey