

## DECISION NOTE

### Advice to Deputy Minister

**DATE:** April 26, 2019

**CLIFF#: 111490**

**ISSUE:** Responding to Access Requests for Records Sent or Received from Personal Email Accounts

#### **BACKGROUND:**

In June 2018, ministries received 852 related access to information requests for emails sent from or received in personal email accounts. On June 28, 2018, Legal Services Branch (LSB) requested that the Office of the Information and Privacy Commissioner (OIPC) authorize the ministries to disregard the requests under section 43 of the *Freedom of Information and Protection of Privacy Act* (the Act).

On March 7, 2019, the OIPC-facilitated mediation process concluded with the applicant confirming that they were withdrawing the 852 access to information requests at issue.

From March 7, 2019, to April 10, 2019, the applicant has submitted 576 access to information requests for emails sent from or received in the same personal email accounts. These requests differ from the original requests only in that they name specific individuals in each ministry that they would need to be canvassed for these records. Additional similar requests are continuing to be received by Information Access Operations. <sup>s.13</sup>

s.13

#### **DISCUSSION:**

The considerations and analysis relevant to the decision to proceed with a section 43 application (see Appendix A), except for the number of employees required to conduct a search for records, remain relevant to the decision required at present.

s.13; s.14

#### **OPTIONS:**

**Option 1:** Ask the Information and Privacy Commissioner to authorize the ministries to disregard these requests.

s.13; s.14

s.13

**RECOMMENDATION:**

**Option 1:** Ask the Information and Privacy Commissioner to authorize the ministries to disregard these requests.

**Option 1 – Approved**



**April 24, 2019**

**DECISION and SIGNATURE**

**DATE SIGNED**

Jill Kot

Deputy Minister

Ministry of Citizens' Services

Attachment: Appendix A - 108730 DBN Personal Email Account Requests; Appendix B – DM Memo s 43 appeal

ADM Contact: Kerry Pridmore, 250 507-1485

Prepared by: Kris Ghag, Senior Director, Access and Open Information

## 2018 Decision Note

Jill Kot, Deputy Minister

Date: June 21, 2018

Ref: 108730

Issue: Responding to Information Requests for Records Sent to, or Received from, Specified Non-Government Email Accounts

### Summary:

- Approximately 720 requests have been received from a single applicant for all emails sent to or received from 30 named email accounts that are not government-issued accounts.
- There is no established precedent as to how to respond to these requests. There are several considerations in identifying potential options for responding to these requests, including considerations related to employee privacy.
  - There is a risk of directly or indirectly disclosing personal information about the owners of the personal email accounts.
- The Appropriate Use Policy states that employees must use their government email accounts when conducting government business; however, an exception is permitted in extenuating circumstances.
  - An employee must copy the email to their government account and must delete it as soon as possible from their non-government account in this circumstance.
- It is recommended that ministries take a consistent approach to responding to these requests. There are a number of potential options for response, including:
  - 1) Ask the Information and Privacy Commissioner to authorize the ministries to disregard the requests as being systematic, repetitious, or vexatious.

s.13

- 
- It is recommended that an application should be made to the Information and Privacy Commissioner, on behalf of each of the ministries and agencies that have received these requests, for authority to disregard the requests.

## Background / Facts:

### Details of the Requests

- Freedom of Information (FOI) requests have recently been received for all emails sent to, or received from, approximately 30 specified email accounts that are not government-issued accounts.
- The requests do not specify the name of the employee, nor do they specify a subject or topic of interest.
- The FOI requests are worded as follows: *"All emails sent to, or received from, [specified non-government email address] including cc's and bcc's (Date range for records search: From 07/18/2017 to 05/15/2018)"*.
- The applicant has sent each of the FOI requests to every ministry (in other words, there are approximately 720 requests for records related to 30 named accounts).
- Interpreted broadly, this request could require any person in any ministry who may have received an email from the specified address to search for responsive records. This would include cases where the email account owner was interacting with a ministry in an individual capacity unrelated to their work.

### No Precedent

- Under normal circumstances, the principles of "duty to assist an applicant" and "conducting an adequate search" require employees to search any location where they believe responsive records may reside (including their non-government email accounts, if there is reason to believe responsive records exist there).
- However, there is no precedent for FOI requests that ask specifically for records associated with the non-work email accounts of government employees. Therefore there is no established precedent as to how to respond to these requests.

### Policy and Practice Context

- The Appropriate Use Policy requires employees to use their government email accounts when conducting government business. This includes while working outside of the workplace.
- However, the policy also permits the use of non-government email accounts for government business in extenuating circumstances, provided that the employee follows three rules:
  - Send a copy of the email to their government email account;
  - Delete the email from their personal or non-government email account as soon as possible after dealing with the extenuating circumstance; and,
  - Send or receive the least amount of confidential information necessary to deal with the extenuating circumstance.
- Any email created or received by an employee in the course of doing their work may be under the control of the public body — and therefore subject to the *Freedom of Information and Protection of Privacy Act* (the Act) — regardless of where the email is located.
- A record may be under the control of the public body even when it resides in an email account that is not government-issued.
- The Appropriate Use Policy's provision for the use of non-government email accounts in extenuating circumstances has recently been the subject of media attention and has been raised by the opposition in the House.
- At least one of the personal email aliases referenced in these requests has been captured in previous FOI requests made by this applicant and published on Open Information.

## Analysis:

- There is limited precedent for dealing with requests for records related to non-government email accounts.
- Occasionally, requests have been made for records related to non-government email accounts belonging to contractors providing services to government.
- However, these requests are different in that they typically identify the person or organization and the topic of the request.
- There are several considerations in identifying potential options for responding to these requests, including:

### Policy and Practice

- A public body must, by law, make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately, and completely.
- Because the Appropriate Use Policy permits limited use of non-government email accounts to carry out government business in extenuating circumstances, if any employee believes that government records responsive to any FOI request may reside only in a non-government email account under their control, the employee has an obligation to search that location when responding to the request.
- Emails originating from non-government accounts have recently been included in FOI responses. This is consistent with the legislated "Duty to Assist" FOI applicants.
- Several past orders of the Information and Privacy Commissioner have held that non-government email accounts should be searched if there is a reasonable belief that responsive records reside there.
- However, because the Appropriate Use Policy requires employees to (a) copy their government email address when sending email from a non-government account, and (b) delete the email from their non-government account as soon as possible, even those employees who have a reasonable belief that they used a non-government account in an extenuating circumstance should likely be able to locate relevant records within the government system, assuming the policy was followed.

### Privacy Protections

- The legislation provides for access to government records, but also restricts what information can be collected, used, or disclosed by ministries, to protect privacy.
- There may be privacy implications related to identifying the email account owner, and related to searching and processing emails in these accounts.
- Section 8 of the Act allows a public body to refuse to confirm or deny the existence of a record, if it could reveal personal information about a third party.
- Personal email accounts are not government-issued, and the validity of the account and the identity of the account owner, as well as use would all be considered personal information.

### Ability to apply to the Information and Privacy Commissioner for authority to disregard the requests.

- The Act provides a mechanism for dealing with requests that are clearly repetitious, systematic, made without reasonable or probable cause, or requests that show an intention to harass a public body, to "break" the system or to engage in "information warfare".
- The applicant in this circumstance has made thousands of requests to ministries over a period of months.
- The Commissioner can be asked to authorize disregarding the requests, and can also be asked to authorize relief for the public body; for example, to authorize the public body to disregard all or some of an applicant's future access requests.

#### Search

- Emails are electronic records, which can be searched for relatively easily by an employee within the public body. Emails may also exist in other locations and formats, including print copies.

#### Resources

- There is a significant workload impact associated with this request. As the wording currently stands, approximately 27,000 public servants would be required to search for records.

#### Privacy Concerns

- By providing access to records related to this request, there is a real risk of directly or indirectly disclosing personal information about the owners of the personal email accounts.
- Of the 30 specified email aliases, some contain names (e.g.: john.doe@gmail.com) that can be matched to names of current public service employees or Order in Council (OIC) appointees. Other specified email aliases do not contain names.
- In cases where the email account aliases do not contain names, there is no way to validate the authenticity of an account without collecting personal information from government employees. It is unclear whether government would be legally authorized to do so.

### **Recommendation:**

#### **Option 1 (Recommended): Ask the Information and Privacy Commissioner to authorize the ministries to disregard these requests.**

- Section 43 of the Act allows the head of a public body to ask the Commissioner to authorize the public body to disregard requests that:
  - would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the requests; or
  - are frivolous or vexatious.
- s.13; s.14
- There is an apparent lack of a meaningful cause or purpose, and cumulatively, these and other requests made by the same applicant result in a significant cost and effort to government.

s.13; s.14

s.13

s.13; s.14

s.13

**Approved**

*Final approver to specify if the recommendation has been approved or one of the other options or simply not approved.*



22 June 2018

\_\_\_\_\_  
Jill Kot, Deputy Minister

\_\_\_\_\_  
Date

**Contact:** David Curtis, ADM, 778-698-5845



## Memorandum

---

Ref: 111490

Date: April 26, 2019

To: All Deputy Ministers

Re: Application to the Information and Privacy Commissioner

---

Dear Colleagues,

I am writing to provide you with the status related to a number of access to information requests.

In June 2018, through legal counsel, government applied to the Information and Privacy Commissioner for his authorization to disregard 852 access to information requests from a single applicant, which requested records related to non-government-issued email (e.g. Gmail or Yahoo) accounts. During mediation, the applicant proposed to revise those requests by limiting the number of employees that would be required to search for records; an approach that government rejected. The applicant subsequently withdrew the 852 requests at issue.

Recently, Information Access Operations received a second set of access to information requests from the same applicant, requesting the same records, but limiting the number of employees that would be required to search for records. These requests, for over 30 identified email aliases, have each been directed to all ministries and total over 575 individual requests.

Through legal counsel, government will be applying to the Information and Privacy Commissioner for his authorization to disregard these requests under section 43 of the *Freedom of Information and Protection of Privacy Act*.

It is important that we take a unified approach to responding to these requests, and therefore the appeal will be on behalf of every ministry or office that received the requests.

I will keep you informed about the progress of this application.

Regards,

Jill Kot  
Deputy Minister