ABOVE BOARD

A quarterly newsletter published by the Office of the Information and Privacy Commissioner

Volume 13, Issue 2 April 2021

Contact Information

Office of the Information and Privacy Commissioner

3rd Floor, 2 Canada Drive
Sir Brian Dunfield Building
P.O. Box 13004, Station A
St. John's, NL A1B 3V8

Telephone:

709-729-6309

Fax:

709-729-6500

Toll Free in Newfoundland and Labrador:

1-877-729-6309

Email:

commissioner@oipc.nl.ca

www.oipc.nl.ca

This Issue:

APSIM 2021

The Access, Privacy, Security and Information Management (APSIM) conference, originally scheduled for last year, proceeded as an online event from March 16-18 with a mix of live and pre-recorded presentations and talks. Over 250 participants registered for this event.

Conference highlights included: keynote addresses from University of Ottawa Faculty of Law professor Dr. Teresa Scassa on the future of privacy in Canada and former British Columbia Information and Privacy Commissioner David Loukidelis on developments in privacy and access laws and digital economies. There was both a Coordinator's Panel and a Regulator's Panel, providing insight into the roles played by both parties. Other conference highlights include presentations on passwords and protecting yourself online, cloud computing, online safety, managing shared drives, digital government, and data governance in healthcare.

In the coming weeks, we hope to be able to make some of the conference presentations and other resources available at https://www.gov.nl.ca/apsim/.

We continue to offer this semi-annual conference at no cost to participants, in an effort to grow our common communities. Online conferences also remove travel barriers, increasing accessibility for professionals outside of the St. John's area. If you have feedback on this conference or suggestions for future conferences, please contact commissioner@oipc.nl.ca.

This conference would not be possible without the support and involvement of the local access, privacy, security and information management communities. We'd like to thank everyone who worked collaboratively, pooled

resources and delivered an outstanding conference with quality content. This conference was presented in partnership with Memorial University and its conference services through the Signal Hill Campus. We'd like to thank all presenters, members of the steering committee and staff at the Signal Hill Campus for making APSIM possible.

OIPC is Hiring: Access and Privacy Analyst

The OIPC is currently advertising for the permanent position of Access and Privacy Analyst. For more information, please see the full job ad at the Human Resources Secretariat Online Job Portal.

April is Information Management Month!

April is Information Management Month. This is a great time to reflect on the role that solid information management plays in the access to information process. A huge thank you to the information management professionals that help keep public bodies organized!

Transferring a Request

OIPC has noticed a few situations lately involving the process of transferring a request.

Section 14 establishes the ability for a public body to transfer a request. A public body is able to transfer a request, or part of a request, not later than 5 business days after receiving it, upon notifying the applicant in writing. Transfers are authorized where it appears that the record was produced by or for the other public body; or the record or personal information is in the custody or under the control of the other public body.

Any public body that is in receipt of a transferred request must respond to the request as if it had been made directly to it by the applicant, with the timeline starting the day that the request was transferred.

Consider the following scenarios, drawn from recent access request responses on the ATIPP Office's website:

- A public body has received an access request and, while the responsive records are in its custody or control, the records were created by another public body and are also in that public body's custody or control. The initial public body could transfer the request or process the request itself; the final response should not just refer the applicant to another public body. If the request is not being transferred, the public body must respond to it, but could assist the applicant by alerting them to the other public body that also has responsive records and inform the applicant that it may be worthwhile to make another request to that public body as well.
- A public body has received an access request and has no responsive records for part of the request. Rather than transferring this part of the request or referring the applicant to another public body in their advisory response, the full 20 days was taken to respond. The applicant was left to start a new request, thus delaying access. The duty to assist means alerting applicants about such circumstances as soon as reasonably possible.

- A public body consults with another public body regarding potentially transferring a request. Any such consultation should conclude with a clear understanding regarding the status of the transfer; whether the request will be transferred or if a final decision is pending. The legislation doesn't contemplate transferring a request and then cancelling the transfer; it also doesn't contemplate a public body pulling another public body into responding to a request the first has received. Further, a public body cannot both transfer the request and continue to process a request for the same records.

The ATIPP Office's Access to Information: Policy and Procedures Manual discusses transferring requests on page 42. It states, in part, "Where a public body who receives a request knows that another public body has the records sought by the applicant, the request should be transferred rather than advising the applicant that there are no responsive records and closing the request. This is consistent with the duty to assist."

If the scenarios above resulted in complaints to OIPC, the Duty to Assist would be part of the investigations. Further, in the first scenario, the authority on which its final response was based would be sought, along with discussions of how the final response was in compliance with the expectations established in section 17. In the second scenario, details on why Coordinators from both public bodies did not discuss the records in their custody or control and refer the applicant to the second public body earlier in the process would be part of the investigation.

Inadvertent Consequences: Attaching a Personal Device to a Work Asset

Do you have any policies or guidance on staff connecting personal devices to work assets? OIPC Saskatchewan recently issued a report that serves as a cautionary tale of unintended consequences stemming from a seemingly innocent activity.

An employee of the Saskatchewan Health Authority (SHA) connected their personal device to their SHA workstation using a USB cord to charge the device. While connected, they opened an infected MS Word document from their personal email account using their personal device. This triggered the execution of ransomware on the workstation that led to a ransomware attack that impacted fileshares with eHealth, the SHA and the Ministry of Health due to the shared infrastructure on which the fileshares reside. This resulted in the disclosure of approximately 40 gigabytes (GB) of data to three IP addresses – two in Germany and one in the Netherlands.

While the report includes valuable discussion on safeguards and appropriate responses to cyber-attacks, OIPC NL wants public bodies to reflect on the root cause – one individual used a work asset to charge a device.

Anyone interested in reading the full report can access it online here: Investigation Report 009-2020, 053-2020, 224-2020.

Intentional Leak of Applicant's Identity

In February, the Nunavut Information and Privacy Commissioner issued Report 21-189. This report examined a situation where a public body employee whose duties include being able to view access requests intentionally "leaked" the name of a person who had filed an access request, along with

the subject-matter of the request, to a third party. The Report contains a number of interesting comments:

On revealing the identity of the leaker:

> *[17] I agree that revealing a leaker's identity will, in most cases, serve no useful purpose. But I do not lay this down as a general rule: there may be cases in which the name, position or methodology of the leaker is essential to an understanding of what happened, and revealing those details will reveal the leaker's identity.*

On the intent of legislative requirements that protect the identity of applicants:

> *[28] If I were to summarize these rules in plain language, I would say: a requester's identity must be known by as few people as possible within a public body, and usually no further than the designated ATIPP Coordinator; and even when further disclosure is required, it must still be limited to a need-to-know basis.*

On the implications of an intentional leak like this on the access to information process:

> *[37] I think Nunavummiut would be surprised at how much the ATIPPA process depends on all of the participants acting in good faith. Keeping and managing proper records, assisting applicants, performing diligent searches, cooperating with ATIPP coordinators, obeying statutory timelines, claiming only necessary and limited exemptions, producing all responsive documents, and assisting the Commissioner to perform the oversight role: all depend on a commitment by GN staff to the public-policy objectives of the ATIPPA. In the absence of good faith, the access system quickly crumbles.*

One of the Report's recommendations questioned if the entity was prepared for such a leak and recommended that a conflict of interest policy be developed as part of the ATIPP policy manual, stating, in part, "There should be an established procedure for identifying, disclosing, and handling ATIPP requests for which departmental staff may be in a conflict of interest."

As a reminder, section 12 of *ATIPPA, 2015* addresses anonymity of the applicant. Even once an access request has been processed, the identity of the applicant is still personal information within the custody or control of the public body and *ATIPPA, 2015* still applies. For further information on this topic, OIPC has produced guidance titled Anonymity of Applicants and the ATIPP Office has produced a handout titled Anonymizing Identity of Applicants.

ATIPPA, 2015 Privacy Breach Statistics January 1 – March 31, 2021

During the first quarter of 2021 (January 1 to March 31, 2021), the OIPC received 47 privacy breach reports from 21 public bodies under *ATIPPA, 2015*; 31 of the breaches involved e-mail. Public bodies are reminded of some tips to avoid e-mail breaches:

- confirm the full email address before you hit send;
- delete pre-populated addresses;
- add a disclaimer signature line informing the recipient to notify and destroy if not the intended recipient;
- send a test email first to ensure you have the right person; and
- use the bcc field for mass electronic mailouts.

The Royal Newfoundland Constabulary reported one intentional breach this quarter. While the information accessed in the MRD system was the individual's own, this incident still meets the definition of an intentional privacy breach because it was an unauthorized use.