Social Media and Transparency

Frank DeVries

Manager, Adjudication

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

COGEL

December 4, 2017

Outline

Ontario context

- Definition of record
- Legislation only applies to records in the custody or control of an institution
    - has more to do with the purpose/use of the record, as opposed to how it was created and where it is stored
    - Staff records vs. political records

Select decisions dealing with electronic records in various formats (including access decisions and evidence of retention)

Unique issues/challenges for different types of records

Recent amendments to the legislation relating to preserving records

About the IPC

The Information and Privacy Commissioner (IPC) provides an independent review of **government decisions** and practices concerning **access** and privacy

The IPC oversees compliance with *(FIPPA), (MFIPPA)* and *(PHIPA)*

The purpose of FIPPA and MFIPPA include:

- to provide a right of access to information under the control of institutions, and
- to protect the privacy of individuals with respect to personal information about themselves which is held by institutions

Record – broadly defined

- "record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes,
- (a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, *a machine readable record*, any other documentary material, regardless of physical form or characteristics, and any copy thereof, and
- (b) subject to the regulations, *any record that is capable of being produced from a machine readable record* under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution;

Instant messages and emails

Instant messages and emails are forms of electronic correspondence and are considered records under the acts, regardless of the tool or service used to create them.

- Instant messaging tools allow electronic, written messages to be shared in real-time. They include: Short Message Service (SMS), Multimedia Message Service (MMS) text messages, BlackBerry Messenger, internal instant messaging systems, online instant messaging applications like WhatsApp, Facebook Messenger or Google, and any similar application that allows for real-time, written communication

Issues regarding access to these records primarily focus on whether the record is in the custody or control of an institution, rather than where the record is stored or in what format.

Section 10(1) - custody or control

Section 10(1) reads, in part:

> Every person has a right of access to a record or a part of a record in the custody or under the control of an institution unless …

Under section 10(1), the *Act* applies only to records that are in the custody or under the control of an institution.

A record will be subject to the *Act* if it is in the custody OR under the control of an institution; it need not be both.

The courts and this office have applied a broad and liberal approach to the custody or control question.

Custody or control

- The IPC has set criteria that are used to decide if a record is in the custody or control of an institution. These go beyond the physical location of a record and involve factors such as the purpose of the record, who created it, and whether or not it relates to the institution's mandate or functions.

- A record does not need to be both in the custody and control of an institution, but rather one or the other. Therefore, in those cases where a record is not in the custody of the institution, the question is whether it is under the institution's control. In deciding this, the IPC considers the following:

    1. Do the contents of the record relate to the institution's business?

    2. Could the institution reasonably expect to obtain a copy of the record on request? (*Supreme Court of Canada decision*)

Are instant messages and emails sent from or received in personal email accounts subject to the Acts?

They can be. It depends on whether they are in the institution's custody or control.

Generally, records held by ***officers or employees*** relating to institution matters are in the custody or control of the institution.

Records held by ***politicians*** may not be in the custody or control of the institution, unless the politician is an officer of the institution or in certain "unusual circumstances."

Emails on a city server found not to be in the city's custody or control

Court decision: *City of Ottawa*

Records held by staff on institution server found ***not*** to be in the custody or control of the institution – not subject to the Act

- City solicitor was doing volunteer work for a local children's organization
- He sent emails from his city account on the city server

Court applied purposive approach.

- No real difference between email and paper records
- Only significant difference was that electronic records could be accessed and audited by the city. This limited role did not affect the Court's finding.

Records relating to a *politician's* twitter account – not in the institution's custody or control

"The records, if they exist, were not created in furtherance of any city business. They are related to the councillor's own Twitter account, which is not an official city account. I have not been provided with any authority to suggest that the city has a statutory power or duty to maintain a Twitter account for city councillors. I accept the councillor's statement that he uses his account to share thoughts and ideas he has as an individual member of society and political representative, and that communications he has with his staff about the account are for the purpose of representing his constituents."

Decision referenced the fact that the city has its own Twitter accounts that it uses to communicate about city business.

Emails sent from or received in personal email accounts have been found to be under an institution's control

City of Oshawa case #1

- The record was an email located on councillor's personal device
- The record was found to be in the institution's custody and control, because the councillor was found to be acting on behalf of municipality when she sent it
- The city was ordered to issue an access decision to the appellant in accordance with the provisions of the Act.

Emails sent from or received in personal email accounts – search issues

City of Oshawa #2

- A subsequent issue was raised regarding other records which were also sent using the councillor's personal device
- The councillor stated that these emails were only stored on her personal email account, and that they had been deleted and couldn't be retrieved.
- The adjudicator received affidavit evidence from the councillor's IT provider, confirming that the emails could not be retrieved based on their deletion date, the particular system, etc.
- However, there was some evidence that the councillor may have copied the email to her city email account, and the city was ordered to search for those records on its city server.

A police officer's use of their personal email account

An appellant provided evidence that a police officer had used his personal email account for police business, on at least one occasion.

The adjudicator found that, although this may have been a "one-off", it begs the question of whether other responsive emails exist in the police officer's personal email account.

Absent any technical supporting evidence, the adjudicator did not accept the police officer's assertion that migration from one application to another would delete emails on the police officer's personal email account.

The adjudicator ordered that a further search for any responsive records that may exist in the police officer's personal email account be conducted.

BBM decisions

A request was made to a school board for all email and BBM communications between two individuals. The issue was whether the search was reasonable.

- The board provided an affidavit of its Chief Technology Officer, confirming that all emails and texts (BBMs), whether generated by laptop, Blackberry phone, desktop computer, would flow through this server. It also confirmed that the search was conducted on the emails and Blackberries for all the listed individuals who had a board-issued Blackberry.

A government institution responded to a request for “all communications (emails, memos, SMS, BBM, PIN) between any current or former Premier’s Office staff and a named individual.” Records were located and an access decision was issued.

PRIVACY COMPLAINT PI16-3

- During a traffic stop, a police officer recorded the requester's voice on his personal electronic device (due to concerns that the requester might initiate legal action, and due to his abusive and enraged behavior).
- The policy in place at the time of the incident (which has since changed) read: "A uniform member should not routinely use his/her personal cell phone for OPP business related matters. If utilized, his/her personal phone records could be subject to judicial disclosure."
- The IPC recommended that the ministry ensure that the police amend its Personal Electronic Device Policy to include a requirement that if a personal electronic device is used to record, send or receive police operational information, the information must immediately, or within a reasonable time, be copied to an authorized police system or device.

Recent amendment to the Act re: preservation of records

Section 10.1 of the *Act* reads:

Measures to ensure preservation of records

Every head of an institution shall ensure that reasonable measures respecting the records in the custody or under the control of the institution are developed, documented and put into place to preserve the records in accordance with any recordkeeping or records retention requirements, rules or policies, whether established under an *Act* or otherwise, that apply to the institution.

Photograph of a screenshot taken from a cellphone

- This decision involved a different Act and context (PHIPA)
- It addressed the actions of an individual, not an institution
- An individual in a doctor's office took a photograph of a computer screen containing the personal health information of others
- The decision found that the individual improperly retained the image
- The individual was ordered to delete image (and any copies in any format) and to provide an affidavit confirming that this was done

HOW TO CONTACT US

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada M4W 1A8
Phone: (416) 326-3333 / 1-800-387-0073
TDD/TTY: 416-325-7539
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965