ABOVE BOARD

A QUARTERLY NEWSLETTER BY THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

VOLUME 09, ISSUE 01 JANUARY 2017

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
Tel: (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

"The Commissioner's role is to facilitate the effort of a requestor to seek access to information [...] and is effectively an ombudsman or liaison between the citizen and government in attempting to resolve the request by mediation or otherwise if documents or information known to be existing are being withheld in whole or in part for various reasons"
Justice Harrington, NL CA, NL (Information and Privacy Commissioner) v. NL (Attorney General)

FALL APSIM CONFERENCE — NOVEMBER 28-30, 2016

From November 28-30, 2016 the OIPC, with the assistance of a steering committee involving key stakeholders, hosted the annual conference for access, privacy, security and information managers without relying on an outside conference organizer. Titled "We Are Connected", the Conference focused on the overlap and common ground between these four disciplines. A full and comprehensive agenda was offered at no charge to attendees.

The conference lasted for two and a half days, with a half day workshop on day one and a full slate of speakers (including 4 sets of breakout sessions) over the next two days. The registration totaled 246 attendees and involved over 25 presenters. We had local industry leaders (for example, the CIO of Memorial University) and several speakers who travelled here from other provinces to present. The topics covered included: Cloud Computing; Genetic Information and Research; Defining Accountability for all four of our target groups; an Update on How *ATIPPA, 2015* is Working; and the One Shop Model (where IM, IT, Privacy and Access are all in the one shop) and the Advantages of this Grouping.

The feedback has been uniformly positive and our audience is anticipating another conference of this caliber next year. We would like to thank all of our presenters who donated their time so freely and our attendees for making time for this important event.

In the following pages of this Newsletter, we have highlighted some of the material covered in the 2016 conference. Please feel free to visit our conference website apsim.gov.nl.ca to learn more. We hope to have the presentations posted shortly. Summaries of other presentations will appear in future editions of our Newsletter.

RECENT OIPC REPORTS

Morneau Sheppell Ltd PH-2017-001

Personal health information collected during a medical assessment for a fitness certificate was found to have been properly collected and used by the custodian who conducted the assessment. The Report also dealt with the impact of the "circle of care" on the presumption of continued consent. Also, the personal health information was found to have been adequately protected.

City of Corner Brook P-2017-001

The complaint in this case was in relation to the City's decision to send City staff an e-mail that contained personal information about the Complainants, as well as the City's decision to post copies of this e-mail within its premises. The Commissioner determined the City breached the Complainants' privacy. This breach was exacerbated by the City's failure to ensure the accuracy of the personal information. The Commissioner recommended the City use greater caution when handling personal information in similar circumstances in the future in order to ensure that only the minimum amount of information necessary is disclosed to only those people who have a need to know. He also recommended that in future every reasonable effort be made to ensure information's accuracy before using or disclosing it.

Department of Justice and Public Safety A-2017-001

The Commissioner agreed with the use of solicitor-client privilege and the consideration of the public interest override. The record in question met all three elements of the solicitor-client exception test.

City of St. John's A-2017-002

The City properly withheld the names and addresses from a list of tax arrears as it was information gathered for the purpose of collecting a tax, which is excepted per section 39(2).

Department of Health and Community Service A-2016-030; Western Health A-2016-029; Natural Resources A-2016-028 & 027; Health and Community Services and Western Health A-2016-026

All five of these cases involved third parties who had complained, claiming section 39 should apply. In two of the cases, the Commissioner found that a clause regarding confidentiality did not permit parties to contract out of the *Act*. In four of the cases he found that contracts are negotiated and therefore information incorporated into the contract was not "supplied" and that there was no "clear and convincing evidence" presented to support reasonable expectation of significant harm. In two of the cases no argument was made at all by the third party involved.

UPDATE TO GUIDANCE ON SECTION 39

This Office issued a guidance document on the exception for Business Interests of Third Parties in section 39 of the *ATIPPA, 2015* in April of last year. In December we updated this document.

Guidance documents are intended to be living documents that grow and change as the law changes and/or as our understanding deepens through experience with the exception. Every new guidance document (and revisions) are announced through an email to all coordinators and can be found in the "What's New" section of our website.

In this case we made several additions to the document. We clarified the exact purpose of the guidance, ensuring that it was seen as a resource to all the parties involved.

We also made our position more clear with respect to the notification process (s.19). In order for section 39 to apply, all three elements of the test must be met:

1. the information must be of a type set out in section 39(1)(a);
2. it must have been supplied in confidence; and
3. there must be a reasonable expectation that one of the outcome identified in section 39(c) will probably occur if the information is disclosed.

If either one of the elements of the test are not satisfied, the Applicant is entitled to the information without the delay associated with notification of a Third Party. While informal consultation with a Third Party is not prohibited by the *ATIPPA, 2015*, it should not delay granting access to records that are clearly not subject to an exception. While preserving the business relationship and trying to avoid surprising the Third Party with a release of their information are often cited as reasons for notifying when there is no legislated requirement to do so (i.e. when the test is not met), these reasons are clearly irrelevant in the access to information context and such notices unacceptably deny timely access to information.

The revised guidance document also provides greater detail on what should be included in a formal notice to a Third Party. Simply stating that section 39 may apply is inadequate. Sufficient detail must be provided to allow the Third Party to understand the reasoning behind that determination. At a minimum, the reasons should summarize what the Public Body's submissions to the Office of the Information and Privacy Commissioner will be if a complaint is made by the Third Party.

SUPREME COURT OF CANADA DECISION SOLICITOR-CLIENT

The Supreme Court of Canada recently dealt with Solicitor-Client privilege in *Information and Privacy Commissioner* v. *University of Calgary*, 2016 SCC 53. The Supreme Court of Canada in that case dealt with the limits on the powers of the Alberta Commissioner under their legislation (*Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25) to review records claimed to be subject to solicitor-client privilege.

The OIPC reviewed the decision and on November 27, 2016 sent a notice to all coordinators of our position regarding review of solicitor-client records by the NL OIPC following this case.

Below is the text of that Notice:

> The position of the OIPC is that records claimed by public bodies to be subject to solicitor-client privilege must continue to be produced for review by the OIPC. This is based on a number of factors, including:
>
> - *ATIPPA, 2015* contains specific provisions respecting the Commissioner's authority to review records where there has been a claim of solicitor-client privilege. These provisions are absent from the Alberta's legislation;
>
> - the 'Wells' Committee clearly and unambiguously stated that it is necessary for the Commissioner to be able to compel production of and conduct reviews of records in the course of a complaint investigation where there is a claim of solicitor-client privilege. In doing so it included additional provisions in its draft bill to fulfil and operationalize this intention. These are absent from Alberta's legislation (in particular, section 100 of *ATIPPA, 2015*);
>
> - the Province fully adopted the recommendations of the 'Wells' Committee, including the draft legislation in its report. The additional provisions in the *ATIPPA, 2015,* which are not included in the Alberta's legislation, provide clarity regarding the Commissioner's powers and authorities pursuant to *ATIPPA, 2015* and affirms the specific intent of the legislature to require public bodies to make solicitor-client privileged material available to the Commissioner for review.

Since this Notice, our position remains unchanged.

BUILDING ONE COMMUNITY

Shelley Smith, Chief Information Officer for Memorial University spoke at the Fall APSIM Conference about the model they use for their information management, a model we have colloquially referred to as the 'One Shop Model'.

This presentation was perfectly aligned with the theme of the conference—bringing the disciplines of information management, security, privacy and access to information together.

After explaining the complex environment of the University, Shelley identified their threat landscape and their top threats:

1. account hijacking –"phishes" usernames and passwords;
2. denial of service attack – aims to shut down services;
3. advanced persistent threat (often state actor) – lurks in networks to steal data and/or launch attacks; and
4. ransomware attack – encrypts and/or steals data, demands ransom.

She then shared their access to information experience — 52 access requests processed in 2015 and 65 access requests processed in the first six months of 2016. Shelley noted the complex issues related to research, custody and control, and intellectual property that the University faces as part of this process.

Memorial has a relatively new Director of Information Management and Protection. This person and their 5 staff have been tasked with: Information Management policy; records classification plan and retention schedule; information risk assessments and information protection program; reorganization to create separation of duties between operational IT security and information protection and compliance; and, integration of Information Management and Information Protection considerations into Information Technology decisions.

The convergence that is happening at Memorial is happening in all organizations. As Shelley stated now we're all information professionals as there is information in many more places and formats than ever. We as information professionals need a comprehensive view and integrated information services to promote convergence of data governance, privacy, security and access by design.

Therefore, at Memorial, the Office of the CIO is responsible for:

1. IT Services (Network management and security, telecommunications, data centre

continued over...

BUILDING ONE COMMUNITY

services, project management, solution delivery, client services, application services, disaster recovery, and business continuity);
2. Information Management and Protection (Information Management Advisory Services, education and awareness, risk assessments, process definition and improvement, and compliance monitoring); and
3. Information Access and Privacy (Access to Information requests, privacy breach management, advisory services (including Privacy Checklists and PIA), education and awareness.

Although these three areas involve individual roles and a separation of duties, the work is conducted in a collaborative environment. This has allowed for "APSIM by Design" which has allowed for solutions developed or acquired to consider:

1. security classification (determine security controls and access rules, privacy checklist and, if required, full PIA);
2. risk assessment (determine level of security testing and system architecture, may include Cloud assessment, vulnerability assessment and/or security review); and
3. Information Management assessment (determine requirement/ability to implement retention schedule, determine whether data may have long term value and therefore data archiving requirements).

At Memorial this process has also involved ongoing partnerships with Legal Counsel, Office of Internal Audit, Office of Chief Risk Officer and has resulted in the best solution to meet client needs, while also considering Information Management, Access and Privacy compliance, and Information Protection and Security.

Shelley closed her presentation with the idea that the information professional of the future will need to be

Part policy expert	Part IT expert	Part IM expert
Part access and privacy expert	Part lawyer	Part evangelist
Understands the business	Keeps up with advances in technology	
Manages vendors (Cloud, etc.)	Walks on water!	

The OIPC and all the Steering Committee members would like to thank Shelley Smith for her very valuable contribution to our conference and for allowing us to have a look at the way things are organized at Memorial University.

ATIPPA PRIVACY BREACH STATISTICS OCT 1—DEC 31, 2016

In our most recent reporting period (October 1 to December 31, 2016), the OIPC received 52 privacy breach reports from 21 public bodies under the *ATIPPA, 2015*. This is up from the 41 reports from 15 public bodies received in the second quarter of 2016-2017.

Privacy breach reports to the Commissioner are used primarily to allow the OIPC to advise public bodies about the breach response process, to discuss ways to avoid similar breaches and also to target specific issues or public bodies for privacy training.

If you want the OIPC to deliver training regarding privacy breaches, or any other topic relating to access or privacy, contact our Office to arrange a time.

Summary by Public Body	
Advanced Education, Skills and Labour	5
Central Health Integrated Health Authority	1
City of Corner Brook	1
City of St. John's	1
College of the North Atlantic	5
Department of Children, Seniors and Social Development	2
Department of Finance	2
Department of Justice and Public Safety	2
Department of Municipal and Intergovernmental Affairs	1
Eastern Health	4
House of Assembly	1
Memorial University of Newfoundland	3
Multi-Materials Stewardship Board	1
Newfoundland and Labrador English School District	3
Newfoundland and Labrador Housing Corporation	3
Office of the Public Trustee	1
Public Service Commission	1
Royal Newfoundland Constabulary	1
Service NL	10
Western Integrated Health Authority	1
Workplace NL	3

Summary by Breach Type	
Email	16
Fax	3
In Person	5
Intentional (i.e. willful breach)	2
Mail Out	20
Other	6

The OIPC issued a tip sheet on Avoiding Inadvertent Privacy Breaches (it can be found on our website oipc.nl.ca)