Information, Privacy and Data Security Post

Hicks Morley Information and Privacy Highlights – Spring 2011

Date: March 4, 2011

Welcome to the Spring 2011 Hicks Morley Information and Privacy Highlights!

As you may have noticed, we've recently re-vamped our publication and introduced a shorter, more condensed version of our traditional Post, designed to provide you with the most relevant and leading case law.

The Highlights will now be published three times annually and will include the most significant and precedent-setting cases, ensuring that our readers remain on the leading edge of developments in information and privacy law.

Notable features in this edition include the Federal Court's judgment in *Mirza Nammo v. Transunion of Canada Inc.*, in which the Court awarded damages under the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*") for the first time, and the Ontario Superior Court of Justice's decision in *City of Ottawa v. Ontario (Information and Privacy Commissioner)*, wherein the Court found that personal e-mails stored on government e-mail servers are not subject to disclosure under provincial FOI legislation.

We hope you enjoy the Spring 2011 Information and Privacy Highlights and welcome your comments on the new design, content and anything else you'd like to write to us about.

Mireille Khoraych, Editor

NEW BRUNSWICK COURT FINDS THAT RANDOM ALCOHOL TESTING IS REASONABLE

The New Brunswick Court of Queen's Bench quashed a November 2009 alcohol testing arbitration award, which found that Irving Pulp & Paper had insufficient justification to implement random alcohol testing at its pulp mill.

The Court held that the majority of the arbitration board erred by finding that employers who operate "dangerous workplaces" (i.e. in which there is a risk of an accident with catastrophic consequences) must demonstrate a *history* of alcohol-related incidents in order to justify random alcohol testing. The Court suggested that *if a workplace is dangerous*, a program of random alcohol testing by (1) breathalyzer that (2) applies only to safety-sensitive positions is reasonable, and a history of alcohol incidents is not a necessary precondition to its implementation.

This is a significant judgment that is far more tolerant of random alcohol testing for current impairment than Arbitrator Michel

Picher's leading *Imperial Oil* case from 2007, affirmed by the Ontario Court of Appeal as reasonable in May 2009. The Court noted the *Imperial Oil* decision, but did not comment on it in its analysis.

Irving Pulp & Paper, Limited v. Communications, Energy and Paperworkers Union of Canada, Local 30, 2010 NBQB 294 (CanLII).

RECORDS PROTECTED BY SETTLEMENT PRIVILEGE EXEMPT FROM THE RIGHT OF PUBLIC ACCESS IN ONTARIO

The Ontario Court of Appeal issued a significant decision in which it held that documents protected by settlement privilege are exempt from public access under the Ontario *Freedom of Information and Protection of Privacy Act* (*"FIPPA"*).

The LCBO denied access to various records related to a mediated settlement of a number of civil proceedings between itself and a winery. It relied on the "solicitor-client privilege" exemption in section 19 of *FIPPA*. This exemption has two branches. Branch 1 exempts records that are subject to solicitor-client privilege and litigation privilege, as these privileges are recognized at common law. Branch 2 exempts records that are "prepared by or for Crown counsel for use in giving legal advice or in contemplation or for use in litigation."

The Court of Appeal affirmed the Divisional Court's decision that the records were exempt because they fit within the Branch 2 exemption. In doing so, it made the following significant findings:

- the term "litigation" in the Branch 2 exemption encompasses mandatory and consensual mediation of an Ontario civil dispute;
- the phrase "prepared for Crown counsel" should not be narrowly read to mean "prepared at the behest of Crown counsel"; and
- the "for use in litigation" requirement imports a requirement that the records be communicated to Crown counsel within a reasonably expected "zone of privacy."

Though this is a very significant decision on the *FIPPA* Branch 2 exemption, the Court declined to opine on an even more significant issue – an issue it framed as "Whether the common law settlement privilege is a free-standing exemption under *FIPPA* or whether *FIPPA* is a complete code." The Divisional Court judgment strongly suggests that privileges recognized at common law and rooted in the public interest (such as settlement privilege) can trump the *FIPPA* right of access.

Liquor Control Board of Ontario v. Magnotta Winery Corporation, 2010 ONCA 681 (CanLII).

FEDERAL COURT DISMISSES APPLICATION, ARTICULATES WHAT DAMAGES ARE COMPENSABLE UNDER *PIPEDA*

The Federal Court dismissed a *PIPEDA* application for damages for loss of employment that arguably flowed from a wrongful disclosure of personal information.

The applicant was employed selling scrap metal for his employer. He began to sell scrap metal to the respondent on the side and apparently sold some of his employer's scrap metal to his own credit. The employer spoke with the respondent after it noticed a decline in sales. The respondent disclosed the fact that the applicant had opened a supplier's account in his own name and provided the employer with the applicant's account statements. The employer terminated the applicant, who filed and then withdrew a wrongful dismissal suit in favour of a *PIPEDA* application targeted at the respondent.

The Court suggested that information about the improper sales of the *employer's* scrap metal was information "about the employer's money" and not the applicant's personal information. This reasoning did not justify the whole of the disclosure,

however, as the applicant apparently sourced some of his scrap from entities other than his employer. Therefore, in the result, the Court held that the respondent had breached *PIPEDA* by disclosing the applicant's personal information without consent.

Despite finding a breach, the Court dismissed the application because the applicant had proven no compensable damages. While acknowledging that the applicant might not have been terminated had the disclosure not been made, it held that *PIPEDA* only grants a right to damages intrinsic to the breach of privacy. It explained:

"The Court must examine the real nature of the remedy claimed. Such claims as humiliation, loss of community support, diminution of standings and loss of income flowing there from (to name but a few) caused by breach of the *Act* fall within the statutory cause of action created by the *Act*. Claims for loss of income and similar loss due to termination of employment not caused by breach of the *Act*, do not.

The source of the Applicant's complaint is the loss of his employment. He even claims for loss due to loss of a second job. But all of his loss claimed is tied directly to his termination for cause. While the termination might not have occurred if there had not been disclosure, the nexus to the claimed loss is termination of employment for which Stevens had, but gave up, the right to claim was unlawful."

Stevens v. SNF Maritime Metal Inc., 2010 FC 1137 (CanLII).

SCC DEALS WITH THE DISCLOSURE OF CUSTOMER INFORMATION TO LAW ENFORCEMENT

In *R. v. Gomboc*, the Supreme Court of Canada recently held that an accused person had no reasonable expectation of privacy in detailed information about his residential power consumption. The decision contains a significant dialogue about the disclosure of customer information to law enforcement and, in such circumstances, the effect of terms governing the customer relationship.

Background

A digital recording ammeter (or "DRA") is a device that is installed on a power line to measure electrical consumption. In this case, the police asked an electrical service provider to install one at a residence they suspected of housing a marijuana grow-op. The service provider agreed, and later produced a graphical representation showing power consumption over five days. The graph showed a pattern of 18-hour cycles of high consumption, which is consistent with the presence of a marijuana grow-op. Partly on the strength of this evidence, the police obtained a warrant that led them to lay charges.

Whether the police violated the accused person's reasonable expectation of privacy by conducting a warrantless "DRA search" was the key issue in the case. It turned on (1) the effect of a regulatory provision promulgated under the Alberta *Electrical Utilities Act* that expressly permits Alberta service providers to disclose customer information to the police without consent, unless contrary to their express wishes, and (2) the nature of the electricity consumption information (and whether it went to the accused person's "biographical core of personal information"). Note that the statutory permission, in this case, was also backed by a contractual provision that warned customers that their information could be provided to law enforcement "for drug investigations."

The effect of terms governing customer information

A seven judge majority recognized the statutory permission as a relevant factor that weighed against a reasonable expectation of privacy. Four justices viewed the permission as a relevant factor while the remaining three viewed it as the dominant factor.

Not so for the two dissenting judges. Here is a passage from their jointly written dissent:

“Every day, we allow access to information about the activities taking place inside our homes by a number of people, including those who deliver our mail, or repair things when they break, or supply us with fuel and electricity, or provide television, Internet, and telephone services. Our consent to these ‘intrusions’ into our privacy, and into our homes, is both necessary and conditional: necessary, because we would otherwise deprive ourselves of services nowadays considered essential; and conditional, because we permit access to our private information for the sole, specific, and limited purpose of receiving those services.

A necessary and conditional consent of this sort does not trump our reasonable expectation of privacy in the information to which access is afforded for such a limited and well-understood purpose. When we subscribe for cable services, we do not surrender our expectation of privacy in respect of what we access on the Internet, what we watch on our television sets, what we listen to on our radios, or what we send and receive by e-mail on our computers.

Likewise, when we subscribe for public services, we do not authorize the police to conscript the utilities concerned to enter our homes, physically or electronically, for the purpose of pursuing their criminal investigations without prior judicial authorization. We authorize neither undercover officers nor utility employees acting as their proxies to do so.”

The response to this argument by the majority is remarkably subtle. Deschamps J. agreed that the reasonable expectation of privacy standard is normative, and suggested that she was not prepared to make a general pronouncement about the constitutional effect of “disclosure clauses,” but stated that terms governing a customer relationship are nonetheless one relevant factor of many in assessing the reasonableness of a privacy expectation. Significantly, however, Deschamps J. argued that a service provider’s equal interest in information about the services it provides to its customers weighs against section 8 protection.

Abella J.’s judgment on this issue is similar. Like Deschamps J., she deflected the strong minority argument: “There can be no examination of the totality of the relevant circumstances without including the fact that the *Regulation* exists. It cannot, therefore, be seen as neutral or irrelevant.”

Biographical core and personal information

Five of the nine judges held that information about residential power consumption over a period of time reveals an individual’s “biographical core” of personal information.

Deschamps J., in the minority on this issue, held that police use of DRA technology reveals only “information about electricity use” and not about the intimate and personal choices of the occupants of a residence. She holds that DRA data can support a very strong inference that a residence is being used as a grow operation, but not much else. Though information about criminal activity is protected by section 8, Deschamps J. suggests that DRA’s focus on information about criminal activity minimizes its impact and, remarkably, favours its use as a privacy protective surveillance technique.

The minority takes great exception to Deschamps J.’s suggestion that the use of DRA can be justified by its focus on the collection of information about criminal activity: “First, the constitutionality of a search does not hinge on whether there are even more intrusive search methods the police could have improperly used.” Aside from making this rebuttal, McLachlin C.J. and Fish J. cite a *Law Review* article for the proposition that hourly electricity data can reveal “personal sleep, work, and travel habits, and likely identify the use of medical equipment and other specialized devices.”

Like the minority, Abella J. finds that DRA information reveals information of the kind protected by section 8. She doesn’t reach quite as far though, relying more on the DRA’s efficacy in revealing information about criminal activity itself and the more basic proposition that section 8 protects such information.

Conclusion

Accused persons have recently made arguments (similar to that made by the minority here) that suggest the normative rule embodied in section 8 of the *Charter* makes businesses' own interest in records of customer information and any privacy-reducing terms of contract irrelevant. Though somewhat qualified, this judgment suggests that customer information, in particular when governed by terms that permit disclosure to law enforcement, is less likely to be protected by section 8 of the *Charter*.

R. v. Gomboc, 2010 SCC 55 (CanLII).

PERSONAL E-MAILS NOT SUBJECT TO FOI LEGISLATION

The Ontario Superior Court of Justice – Divisional Court held that employee personal e-mails stored on government e-mail servers are not subject to provincial FOI legislation.

The Court read "custody or control" in the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) purposely and narrowly. It held that providing access to personal e-mails does not advance the purposively of FOI legislation – which is to advanced public participation in the democratic process.

The Court's reasoning is very broad. The only atypical fact that it relied upon was that the e-mails in question were stored in a separate folder rather than intermingled with e-mails related to governmental affairs. The Court minimized the significant of this fact as follows:

"That said, it does not follow that personal emails not filed in a separate folder (as was the case here) are necessarily subject to the operation of the *Act*. Much will depend on the individual circumstances of each case, but generally speaking, I would expect very few employee emails that are personal in nature and unrelated to government affairs to be subject to legislation merely because they were sent or received on the email server of an institution subject to the *Act*."

Importantly, the decision does not recognize a privacy right in personal e-mails or preclude institutions from auditing or inspecting personal e-mails.

The Court makes relatively clear that its decision does not rest on employees' privacy interest in the content of their e-mails.

City of Ottawa v. Ontario (Information and Privacy Commissioner), 2010 ONSC 6835 (CanLII).

FEDERAL COURT CONSIDERS ACCURACY PRINCIPLE, ORDERS DAMAGES UNDER *PIPEDA*

The Federal Court issued a *PIPEDA* judgment in which it considered an organization's duty to maintain accurate records of personal information and ordered damages under *PIPEDA*, both for the first time.

The judgment is about an inaccurate credit report given by a credit reporting agency to a bank. The agency wrongly associated negative credit information with the applicant based on the similarity between his identifiers and the identifiers of the individual to whom the negative information related. The applicant made some inquiries and diagnosed the error in early January 2008. It took the agency about 20 days to confirm the error, amend the applicant's credit record and send a notice of correction to the bank. The applicant took issue with how forthright the agency was in dealing with the matter, both in its willingness to accept responsibility for the error (as opposed to blaming the collection agency that had supplied it with the negative information) and in notifying the bank.

The Court held that the credit reporting agency:

- failed to keep the applicant's personal information "as accurate, complete and up-to-date as is necessary for the

purposes for which it is to be used" as required by *PIPEDA* principle 4.6;
- failed to keep the applicant's personal information "sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual" as required by *PIPEDA* principle 4.6.1; and
- failed to provide amended information as required by *PIPEDA* principle 4.9.5 because it simply advised the bank that the applicant's credit record had been amended without providing a copy of the amended credit record or otherwise indicating that the amendment was in the applicant's favor.

In upholding the accuracy complaint, the Court rejected the agency's argument that its use of industry standard matching practices (which contemplate some margin of identification error) and its correction effort rendered it in compliance. The Court was very clear that neither compliance with industry standards nor complying with the duty to correct are valid defences to an accuracy complaint, but did suggest that liability for keeping inaccurate personal information is not absolute. It stated:

"*PIPEDA* does not require that personal information be completely accurate, complete, and up-to-date; rather, it requires that personal information be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. Thus, it is the use that the information is put to that dictates the degree of accuracy, completeness, and currency the information must have."

The Court then suggested that the agency failed to take the reasonable precaution of conducting a manual check prior to issuing its credit report.

The Court awarded the applicant $5,000 in damages for humiliation suffered. While it recognized its recent statement in *Randall v. Nubodys Fitness Centres* that damages ought to be awarded in "egregious situations" only, it held that damages should be ordered to "uphold the general objects of *PIPEDA* and uphold the values it embodies," including by deterring future breaches. In awarding damages in the circumstances, the Court noted the evidence of humiliation, the credit reporting agency's profit motive and the credit reporting agency's "failure to take prompt, reasonable steps to correct the record and reverse the situation it had caused."

There are other aspects of the Court's judgment of significance, including with regards to the scope of the Federal Court's jurisdiction under section 14 and its jurisdiction to make compliance orders under section 16(a).

Mirza Nammo v. Transunion of Canada Inc., 2010 FC 1284 (CanLII).

COURT COMMENTS ON LEGALITY OF SURREPTITIOUS VIDEO SURVEILLANCE

Ramsey J. of the Ontario Superior Court of Justice made the following comment on the legality of surreptitious video surveillance in striking a Statement of Claim that alleged an "unlawful investigation scheme":

"As I have noted, the only conduct about which facts are alleged with any particularity consists of the insurance company hiring an investigator to investigate the plaintiff, and the investigator's approach to a neighbour, during which he made himself known to the neighbour, who immediately told the plaintiff that the plaintiff was being investigated. That cannot possibly sustain a claim of wrongdoing or improper motivation.

Insurance companies are entitled to conduct surveillance of plaintiffs if they do so within the confines of the law. They cannot trespass on private property and they cannot intercept communications electronically. They cannot threaten witnesses or litigants. They cannot commit the tort of defamation. The plaintiff does not claim that they did. The fact that a private investigator is conducting an investigation is not defamatory. Anyone who is involved in a car accident or a divorce might be investigated by a private investigator.

Insurance companies do not need grounds to believe that the plaintiff is making a fraudulent claim before they conduct an investigation. They can conduct surveillance to refute a claim, to confirm a claim, or to see whether a claim is valid or not.

They can photograph a plaintiff in places open to public view. They can identify themselves to the neighbours, and ask them for information about the case. Stripped of bald assertions and fanciful conclusions, the statement of claim alleges no wrongful acts and nothing from which improper motivation could be inferred."

This certainly highlights the significance of the Federal Court's recent *State Farm* decision, which suggests that the collection of evidence in defence of a civil action is not *PIPEDA*-regulated notwithstanding the involvement of "commercial" actors such as insurers, lawyers and private investigators.

Pontillo v. Zinger et al., 2010 ONSC 5537 (CanLII).

BCSC AWARDS DAMAGES FOR BREACH OF PRIVACY

In *Nesbitt v. Neufeld*, the British Columbia Supreme Court awarded $40,000 in damages for defamation and breach of privacy. The award was based partly on a number of publications made by an ex-husband about his ex-wife that the Court held were defamatory and unjustified. The Court also upheld a privacy claim based on the ex-husband's use of e-mail communications he obtained from an old home computer and distributed for the purpose of scandalizing his ex-wife. The breach of privacy claim was brought under British Columbia's *Privacy Act*, which codifies the tort of invasion of privacy.

Nesbitt v. Neufeld, 2010 BCSC 1605 (CanLII).

The Quicklaw cases linked to in this Post have been reprinted with the permission of LexisNexis Canada Inc. LexisNexis is a registered trademark of Reed Elsevier Properties Inc, used under licence. Quicklaw is a trademark of LexisNexis Canada Inc. No part of the cases may be copied, photocopied, reproduced or translated or reduced to any electronic medium or machine-readable form, in whole or in part, without written consent from LNC. Any other reproduction in any form without permission of LNC is prohibited.

The articles in this Client Update provide general information and should not be relied on as legal advice or opinion. This publication is copyrighted by Hicks Morley Hamilton Stewart Storie LLP and may not be photocopied or reproduced in any form, in whole or in part, without the express permission of Hicks Morley Hamilton Stewart Storie LLP. ©