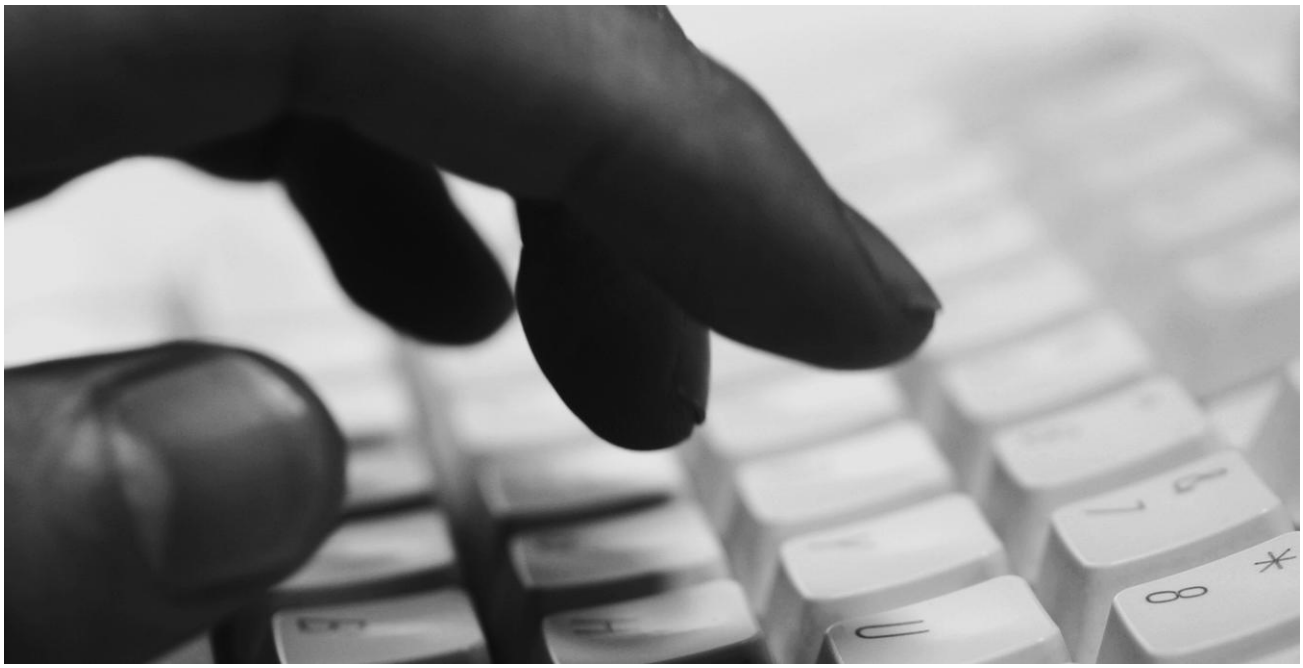
Hicks Morley

HUMAN RESOURCES
LAW AND ADVOCACY



HICKS MORLEY INFORMATION AND PRIVACY POST

2011/2012

*All dates in 2012 unless otherwise noted.

TORONTO
TD Tower, 77 King St. W.
39th Floor, Box 371
Toronto, ON M5K 1K8
Tel: 416.362.1011
Fax: 416.362.9680

WATERLOO
100 Regina St. S.
Suite 200
Waterloo, ON N2J 4P9
Tel: 519.746.0411
Fax: 519.746.4037

LONDON
148 Fullarton St.
Suite 1608
London, ON N6A 5P3
Tel: 519.433.7515
Fax: 519.433.8827

KINGSTON
366 King St. E.
Suite 310
Kingston, ON K7K 6Y3
Tel: 613.549.6353
Fax: 613.549.4068

OTTAWA
150 rue Metcalfe St.
Suite 2000
Ottawa, ON K2P 1P1
Tel/Tél: 613.234.0386
Fax/Téléc: 613.234.0418

hicksmorley.com

Hicks Morley Hamilton Stewart Storie LLP
77 King St. W., 39th Floor, Box 371, TD Centre
Toronto, ON M5K 1K8
Tel: 416.362.1011 Fax: 416.362.9680

Toronto
Waterloo
London
Kingston
Ottawa

Dear Friends:

It's late August 2012, and here's what's on our minds

Our Information and Privacy Post is back. This edition contains 61 case summaries relating to the protection of confidential business information, electronic evidence, freedom of information, privacy, privilege and production.

It has been a remarkable year. Canadian privacy law, in particular, has made a significant shift. With its decision in *Jones v Tsige* (page 12), the Court of Appeal for Ontario recognized a new common law privacy right. This new tort applies narrowly – to intentional "intrusions" into private affairs – and includes a "highly offensive" standard that defendants can rightly view as prophylactic. *Jones v Tsige*, however, opens a door. "What's next?" is the right question to ask.

Will Canadian courts, for example, recognize a cause of action for public disclosure of private facts? Will damage be presumed and, if so, what kind of damage? If liability flows from mere disclosure, will due diligence be a defence? How will the standard of care be calibrated?

Some clarity would be nice given data breach litigation in Canada is now a reality. In the *Rowlands* case (page 17), the Ontario Superior Court of Justice approved a settlement that was structured on an assumption that the compensable damages suffered by class members would be minimal to non-existent. Justice Lauwers followed a Québec decision from earlier in the year called *Mazzona* (page 16), in which the Québec Superior Court dismissed a motion for certification because a data breach class action could not be founded on "potential damage" and the petitioner failed to establish she suffered compensable psychological damage. While positive, the real prospect of data breach class action claims that, even with a reasonable defence, might expose an organization to the kind of counsel fees agreed to be paid in *Rowlands* is certainly a call to data security "behavior modification."

That kind of behavior modification certainly hasn't flown from our federal commercial sector privacy statue – the *Personal Information Protection and Electronic Documents Act*. This statute, which governs the collection, use and disclosure of personal activity in the course of commercial activity in seven out of ten provinces and the three territories, has produced a trail of cases in which applicants have established liability but received very moderate damages or no damages at all (see the cases we've indexed under "PIPEDA damages judgments"). While the Office of the Privacy Commissioner of Canada has used PIPEDA to achieve some high-profile successes in dealing with Facebook, it seems the statute is most notorious for causing the frustration of provincial superior court judges, who don't quite know what to make of it (see the cases we've indexed under "Awkward privacy cases"). With amendments that arose from a parliamentary review that commenced way back in 2006 languishing, one might question whether the statute will hold its relevance. The OPC is aware of this issue, and has begun lobbying for the power to impose administrative monetary penalties and make orders, a development for organizations to watch.

So what if privacy protection becomes the responsibility of our judges? Ontario Commissioner Anne Cavoukian made the news this year when she said she's lost faith in the inclination of judges to protect individual privacy. I don't agree. Judges are rightly conservative in making new policy. Their effective stewardship of rights under section 8 of the *Canadian Charter of Rights and Freedoms* shows they are not out of touch with privacy, though judges from Alberta deserve note for routinely trouncing upon the Office of the Information and Privacy Commissioner of Alberta. The most recent trouncing, in *United Food and Commercial Workers* (page 13), rivals *Jones v Tsige* for privacy decision of the year and raises some fundamental questions about the permissible scope of privacy legislation under the *Charter*. The Alberta OIPC has filed leave to appeal to the Supreme Court of Canada.

So these are very interesting times. The change is real and significant. We hope this document helps you get up to date and equipped for the information management and privacy issues coming your way. Of course, if we can help, please get in touch.

Dan Michaluk
Information and Privacy Practice
Group Leader

*All dates in 2012 unless otherwise noted.

TABLE OF CONTENTS

CONFIDENTIAL BUSINESS INFORMATION

Discovery questions on breach of confidence allowed

On July 24th* the Ontario Superior Court of Justice ordered a defendant to answer questions about an alleged breach of confidence over an argument that the plaintiff had no evidence of breach and was simply "fishing."

Marsh Canada Limited, David J Mew and Tom R Parsons, 2012 ONSC 3852 (CanLII).

Ontario CA comments on departing fiduciary's information-related duties

On January 16th the Court of Appeal for Ontario issued a decision in which it held that a trial judge erred in "blue penciling" a non-competition clause to render it enforceable. It also held that a departing fiduciary does not breach the duty to compete fairly by (1) merely taking confidential information without using it to compete and (2) failing to inform the former employer about an intention to compete.

Veolia ES Industrial Services Inc v Brulé, 2012 ONCA 173, application for leave to appeal to SCC filed on May 17, 2012.

ELECTRONIC EVIDENCE

Electronic parking records admissible in labour arbitration as best evidence

On March 12th Arbitrator Joseph Carrier held that electronic records of an employee's parking activity were admissible as meeting the "best evidence" requirements in the Ontario *Evidence Act*.

Lakeridge Health Corporation and OPSEU (12 March 2012, Carrier).

FREEDOM OF INFORMATION

Backup tape searches extraordinary in Ontario

The Information and Privacy Commissioner/Ontario issued a significant "e-FOI" decision on February 9th. Here is what the IPC said about retrieving e-mails from backup tapes:

> In general, an access request for emails does not require a routine search of backup tapes for deleted emails unless there is a reason to assume that such a search is required, based on evidence that responsive records may have been deleted or lost.

This sets up a presumption that institutions will appreciate, but if a requester asks or if there is an indication that responsive records may have been deleted or lost, an institution must search and retrieve responsive e-mails from backup tapes subject to its right to recover a fee.

Carleton University (Re), 2012 CanLII 5892 (ON IPC).

BC OIPC beats bold challenge to jurisdiction over privilege claims

On March 23rd the Supreme Court of British Columbia held that the British Columbia *Freedom of Information and Protection of Privacy Act* empowers the British Columbia OIPC to adjudicate questions of solicitor-client privilege for the purpose of determining whether government records are exempt from the right of public access.

In rendering this jurisdictional decision, the Court stressed that the OIPC has the power to adjudicate, including the power to "decide all questions of fact and law arising in the course of an inquiry." It also rejected an argument that the legislature could not have intended a "lay tribunal" to adjudicate privilege claims and an argument that the OIPC's power to report information about offences to the Attorney General weighed against a power to adjudicate on privilege.

In the end, the Court held that the OIPC erred in rejecting part of the institution's privilege claim because the institution had not adduced any evidence to establish that certain records were privileged. The request was for records about the expenditure of legal fees. The Court held that the responsivness of the records was sufficient to create a rebuttable presumption of privilege.

School District No 49 (Central Coast) v British Columbia (Information and Privacy Commissioner), 2012 BCSC 427 (CanLII).

Commissioner can review documents subject to privilege claim

On October 26th of last year the Supreme Court of Newfoundland and Labrador (Court of Appeal) held that the Newfoundland Information and Privacy Commissioner can require a public body to produce records claimed to be exempt from public access as subject to solicitor-client privilege.

The Newfoundland *Access to Information and Protection of Privacy Act* gives requesters a right to seek review of an access decision either through the Commissioner or the Trial Division. In the event of a review, the Commissioner may require production of records, and a public body has a corresponding duty under section 52(3) to provide responsive records "notwithstanding another Act or a privilege under the law of evidence."

The Court held that section 52(3) allows the Commissioner to compel the production of records claimed to be exempt from public access as subject to solicitor-client privilege. It relied on the provision's ordinary meaning interpreted in light of legislative purpose, which it said was "to provide for an independent review officer, as an alternative to the courts, who can undertake a timely and affordable first level review of all information request denials."

The Court also made a notable comment favoring the conservative exercise of discretion to demand review of documents subject to a privilege claim.

Newfoundland and Labrador (Information and Privacy Commissioner) v Newfoundland and Labrador (Attorney General), 2011 NLCA 69 (CanLII).

Faculty e-mails not in custody or control

The Alberta Court of Queen's Bench issued a pair of judgments about access to faculty e-mails on April 23rd, ultimately deciding that the Alberta OIPC erred in finding that faculty member e-mails relating to participation on a Social Sciences and Humanities Research Council of Canada committee were in the custody or control of the University of Alberta.

Here are the four points of significance.

First, the Court held that the standard of review for custody or control decisions is reasonableness based on the strong presumption established by the Supreme Court of Canada last December in *Alberta (Information and Privacy Commissioner) v Alberta Teachers' Association*. This is a change, albeit a predictable one in light of *Alberta Teachers' Association*. Despite the outcome in this case, custody or control decisions will generally be harder to challenge on judicial review than in the past.

Second, the Court held that the Association of Academic Staff of the University of Alberta did not have a right to notice of the OIPC's hearing as an affected party or as a matter of fairness. It held that the

AASUA interest in the precedential effect of the OIPC's finding did not give it an interest in the request under appeal sufficient to justify a right to notice and standing.

Third, the Court held that the OIPC erred in finding that the records at issue were under the university's custody or control.

In part, the Court's reasoning highlights the growing importance of assessing the purpose of access to information legislation in deciding custody or control issues. It held the OIPC erred by failing to recognize that the faculty member's e-mails related to a grant funding process in which the university had no role. They therefore shed no light on the university's own operation in furtherance of the statutory aims. Rather, the records at issue shed much more light on another public institution's operations, something the Court said the OIPC ought to have considered.

The Court's reasoning also suggests that standard technical processes used in the management of business e-mail systems will not govern whether e-mails are in the custody or control of a public institution. It held that the OIPC erred by inferring too much from the routine backup of e-mails and the right to monitor. The Court said, "It was unreasonable to focus on the general computer use policy, rather than considering the particular records in question."

Finally, the Court declined to address a bold argument by the AASUA that all records produced by faculty members in the course of participating in external committee work and in the context of their internal research and other academic work are not subject to a university's custody or control. The Court said, "Academic freedom may be one relevant factor in considering whether a university has custody or control of records, but until the Commissioner considers that question in a hearing that raises the issue at first instance, this Court need not address it here."

University of Alberta v Alberta (Information and Privacy Commissioner), 2012 ABQB 247 (CanLII) (standard of review, custody or control).

Association of Academic Staff of the University of Alberta v University of Alberta, 2012 ABQB 248 (CanLII) (notice and standing).

Ontario CA opens up the advice and recommendation exemption

On February 25th the Court of Appeal for Ontario took a significant step to clarify the scope of the "advice and recommendation exemption" in Ontario access to information legislation. It held that the Information and Privacy Commissioner/Ontario erred in applying an extremely restrictive interpretation of two 2005 Court of Appeal decisions.

The Court first affirmed the meaning of "advice" and "recommendations" it articulated in 2005. "Advice" is "material that permits the drawing of inferences with respect to a suggested course of action." A "recommendation" actually suggests a preferred course of action. Background facts that support advice and recommendations are not exempt from disclosure.

The Court then made two important clarifications.

First, the Court clarified that the entire deliberative process is protected. The IPC erred, it held, by imposing a requirement that exempt information must go to the final decision maker. In doing so, it quoted Justice Evans of the Federal Court of Appeal, who said "It would be an intolerable burden to force ministers and their advisors to disclose to public scrutiny the internal evolution of the policies ultimately adopted."

Second, the Court clarified that the presentation of a range of options may be properly withheld. The IPC erred, it held, by imposing a requirement that exempt information identify a single course of action.

The advice and recommendation exemption is a very important exemption that has always been interpreted extremely narrowly by the IPC. This decision breathes life into the exemption in a manner that will please institutions which, quite legitimately, crave a healthy zone of privacy in which to deliberate so they can make optimal decisions about policy and other matters.

Ontario (Finance) v Ontario (Information and Privacy Commissioner), 2012 ONCA 125, application for leave to appeal to SCC filed on May 15, 2012.

Ontario IPC affirms fee estimate for retrieval of e-mails from backup

On July 12th the Information and Privacy Commissioner/Ontario affirmed a $5,490 fee estimate for a request that would entail retrieving e-mails from backup tapes.

Our provincial FOI legislation allows institutions to recover 100% of the "costs, including computer costs, that [an] institution incurs in locating, retrieving, processing and copying [a] record if those costs are specified in an invoice that the institution has received." In this matter, the IPC held that a quote constitutes an "invoice" for the purpose of this allowance. It upheld the institution's sizable fee estimate while noting that the nature of the request -aimed at gaining access to deleted e-mails - required the institution to use an external vendor.

Toronto Community Housing Corporation (Re), 2012 CanLII 40549 (ON IPC).

Ontario IPC orders institution to establish authenticity of record

The Information and Privacy Commissioner/Ontario issued a notable "e-FOI" order on January 19th.

The IPC ordered the Ministry of Community Safety and Correctional Services to validate the authenticity of a 911 call recording that it provided to a requester. The Ministry filed an affidavit about how the recording was extracted from the system on which it was recorded and burned to CD. However, when the requester challenged the recording's authenticity the Ministry provided the requester with a second CD that the requester successfully claimed did not match the first. The IPC ordered the Ministry to re-produce the CD and provide the requester with a sworn statement about the authenticity of the to-be-produced CD after listening to compare it with the original.

The Ministry adduced evidence of its extraction process that was very strong, but its affidavit seemingly did not capture the entire chain of custody - *i.e.*, the first-produced CD was not marked and identified in the affidavit. This can be done relatively easily by using a hash number or even physically marking the disc that's produced.

Ontario (Community Safety and Correctional Services) (Re), 2012 CanLII 2815 (ON IPC).

Principle-based framework to guide access to faculty records

On November 7th of last year the Information and Privacy Commissioner/Ontario issued a significant order for Ontario universities. It held that the IPC has exclusive jurisdiction to decide whether a record is in the custody or control of a university in the context of an access request under the *Freedom of Information and Protection of Privacy Act*. In addition, the IPC created a principle-based framework to assess whether records possessed by faculty members are in the custody or control of a university, while taking into account principles of academic freedom.

University of Ottawa (Re), 2011 CanLII 74312 (ON IPC).

SCC issues comprehensive third party information exemption decision

On February 3rd the Supreme Court of Canada issued a comprehensive decision on the third party information exemption in the federal *Access to Information Act*. Although the third party, research-based

pharmaceutical company Merck, lost its appeal, the decision establishes decent procedural and substantive protection for third parties.

Justice Cromwell wrote for the six judge majority. He endorsed the following 11 principles (our list) about the scope of the third party information exemption and the procedure for dealing with requests that engage the exemption:

1. Most generally, the duty to provide access to government information is equally important to the duty to protect third party information: "when the information at stake is third party, confidential commercial and related information, the important goal of broad disclosure must be balanced with the legitimate private interests of third parties and the public interest in promoting innovation and development."

2. The threshold for giving notice to a potentially affected third party is low: disclosure without notice "is only justified in clear cases, that is where the head, reviewing all the relevant evidence before him or her, concludes that there is no reason to believe that the record might contain material referred to in s. 20(1)."

3. A head must give notice to a third party even in the absence of a firm intention to disclose, including when "in doubt" about the application of section 20(1): "the institutional head 'intends to disclose' a record that might contain exempt information if the head concludes that he or she cannot direct either refusal or disclosure without notice."

4. A head, however, must make a "serious attempt" to apply the exemption and not simply shift the onus of review to a third party.

5. On judicial review of a decision to disclose, a third party must establish the application of section 20(1) on a balance of probabilities. It is an error of law to hold a third party to a "heavy burden."

6. Section 20(1)(a) applies to information that meets the traditional legal test for a "trade secret." It is an error of law to associate the definition with any particularly restrictive meaning.

7. Section 20(1)(b) applies to information supplied to government that is "not available from sources otherwise available to the public or obtainable by observation or independent study by a member of the public acting on his or her own." The information need not have inherent value (as a client list would, for example).

8. For the purposes of section 20(1)(b), information is not "supplied" if it is "collected by government officials' observation." In general, judgments or conclusions expressed by government officials are not "supplied."

9. The reasonable expectation of harm that triggers the application of section 20(1)(c) exists when there is "considerably more" than a "mere possibility of harm" and "somewhat less" than a likelihood of harm. It is an error of law to demand harm that is "immediate" and "clear."

10. In general, it will be hard to demonstrate that harm will flow from the disclosure of publicly available information and, as a matter of principle, difficult to establish that harm will flow from the misunderstanding of disclosed information.

11. Declining to sever and produce information from an otherwise exempt record will be justified when the non-exempt information has little meaning on its own or when a cost-benefit analysis otherwise weighs against disclosure.

These principles are likely to have at least some significance to the handling of matters under statutes other than the ATIA. Principle 9, in particular, has the potential to calibrate the handling of harms-based exemptions and promote a uniform standard for proof of harm under all Canadian access statutes.

Merck Frosst Canada Ltd. v Canada (Health), 2012 SCC 3 (CanLII).

Sex offender registry data accessible by forward sortation area

On June 4th the Court of Appeal for Ontario affirmed a 2009 Information and Privacy Commissioner/Ontario order to disclose sex offender registry data linked to the first three characters of offenders' postal codes (so called "forward sortation area" data). The IPC had rejected the Ministry of Community Safety and Correctional Services' argument that the information could not be disclosed in such a manner without causing a degree of harm to offenders contemplated by the "health and safety exemption" in section 14(1)(e) of the *Freedom of Information and Protection of Privacy Act*.

Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner), 2012 ONCA 393.

Successful candidates' employment history not accessible under ATIA

On September 27th of last year the Federal Court of Appeal held that information submitted by successful applicants in federal public service job competitions is not accessible under the *Access to Information Act*.

Records containing the personal information of others are generally not accessible to the public under the ATIA. The issue in this case was whether information about candidates' experience in other federal public service positions is accessible because such information is excluded from the definition of personal information based on section 3(j) of the *Privacy Act*.

The Court held that section 3(j) applies to information about a federal public service position and that (in the context) employment history information and educational history information submitted by candidates is more about a person than about a position. The Court described the information as being "an individual's personal assets" in the context.

Nault v Canada (Public Works and Government Services), 2011 FCA 263 (CanLII), leave to appeal to SCC refused, 2012 CanLII 11268.

PRIVACY

BCCA dismisses appeal of successful claim for privacy breach

On December 12th of last year the Court of Appeal for British Columbia dismissed an appeal of a November 2010 award of damages for defamation and breach of privacy.

The $40,000 award was based partly on a number of publications made by an ex-husband about his ex-wife that the British Columbia Supreme Court held were defamatory and unjustified. The Supreme 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 Court of Appeal dismissed the appellant's procedural grounds for appeal without comment on the merits.

Nesbitt v Neufeld, 2011 BCCA 529 (CanLII).

BC court awards nominal damages for privacy breach

The British Columbia Supreme Court awarded nominal damages for a privacy breach on November 23rd of last year.

The plaintiffs advanced the claim under the British Columbia *Privacy Act*. The Court awarded $100 to a defendant's estranged mother because the defendant read and made a copy of her will after finding it while searching for her own documents. It also awarded a company operated by the estranged mother $50 because the defendant read and made a copy of a business letter and showed it to others. (The parties agreed that a corporation could sue for breach of privacy under the statute.)

The Court also held that the defendant's brother, who had merely viewed a copy of the business letter, did not breach the Act.

Fillion v Fillion, 2011 BCSC 1593 (CanLII).

Civil action based on breach of MFIPPA tossed

On February 10th the Ontario Superior Court of Justice struck a claim that alleged a breach of the privacy part of the *Municipal Freedom of Information and Protection of Privacy Act* because an alleged breach of statute cannot found a civil cause of action.

Sampogna v Smithies, 2012 ONSC 610.

Court of Appeal for Ontario recognizes new privacy tort

On January 18th the Court of Appeal for Ontario recognized a new "intrusion upon seclusion" civil cause of action. Under Ontario law it is now clear that individuals can sue for breach of privacy based on proof of:

1. an intentional unauthorized intrusion;

2. which is an intrusion upon private affairs or concerns (*i.e.*, that breaches a reasonable expectation of privacy); and

3. that is made in circumstances that are highly offensive to the reasonable person, causing distress, humiliation or anguish.

If these elements are proven, harms that justify an award of moral damages will be presumed. Such damages will be awarded "to mark the wrong that has been done" in an amount that does not ordinarily exceed $20,000, with an amount being set based on:

1. the nature, incidence and occasion of the defendant's wrongful act;

2. the effect of the wrong on the plaintiff's health, welfare, social, business or financial position;

3. any relationship, whether domestic or otherwise, between the parties;

4. any distress, annoyance or embarrassment suffered by the plaintiff arising from the wrong; and

5. the conduct of the parties, both before and after the wrong, including any apology or offer of amends made by the defendant.

The Court stressed that valid claims for intrusion upon seclusion will only arise "for deliberate and significant invasions of privacy" and also said that the law will develop affirmative defences based on countervailing claims for the protection of freedom of expression and freedom of the press.

Jones v Tsige, 2012 ONCA 32 (CanLII).

Court decision on police access to personal health information in Ontario

On June 20th the Ontario Superior Court of Justice held that a health information custodian did not breach the Ontario *Personal Health Information Protection Act* by telling the police that it had taken a criminal defendant's blood sample at a specific time along with the name of the person who took the sample.

Section 43(1)(g) of PHIPA authorizes health information custodians to disclose personal health information, "to a person carrying out an inspection, investigation or similar procedure that is authorized by a warrant or by or under this Act or any other Act of Ontario or an Act of Canada for the purpose of complying with the warrant or for the purpose of facilitating the inspection, investigation or similar procedure." "Personal health information" is defined very broadly as information that "relates to the providing of health care," including information identifying one's health care provider.

It is questionable whether this provision is meant to authorize disclosures to police who are conducting a criminal investigation and who are not acting under some form of judicial authorization, but the Court held that the hospital's disclosure of the "relatively neutral health information" in this case was so authorized. The Court therefore dismissed the defendant's *Charter* challenge, which he brought based on the standard for protection of personal health information encapsulated in PHIPA. Note that "relatively neutral health information" is not a concept worked into PHIPA nor is the "sensitivity" concept that is part of other privacy statues recognized under the Act.

R v Rodrigues, [2012] OJ No 3013 (SCJ) (QL).

Cyber-picketing case raises questions about scope of privacy regulation

The Court of Appeal of Alberta dropped a bomb on April 30th by raising extremely broad questions about the constitutionality of Alberta's commercial sector privacy statute in disposing of a dispute about the right of a union to take images of people who cross a picket line.

Last September the Alberta Court of Queen's Bench held that the Alberta *Personal Information Protection Act* violated the right of expression guaranteed by section 2(b) of the *Canadian Charter of Rights and Freedoms* because it was disproportionate in restricting unions from engaging in "union journalism" relating to labour disputes and picket lines. The Court's focus was relatively narrow though, and its *Charter*-based order focused on the breadth of a scope provision meant to protect journalistic activity and an exclusion for publicly available information.

The Court of Appeal first re-framed the expressive interest at stake as related to labour relations and not journalism. It then held that the statute interfered with this interest in a manner that could not be justified in a free and democratic society.

The Court's proportionality analysis is remarkable in its breadth. It weighs the purpose of Alberta PIPA - protecting reasonable expectations of privacy, protecting expectations that one can control one's own image and personal information and limiting the misuse of personal information - against the right of free expression in general.

Regarding remedy, the Court issued a declaration that the restrictive order at issue was unconstitutional and invited the Alberta legislature to "decide what amendments are required to the Act in order to bring it in line with the *Charter*."

United Food and Commercial Workers, Local 401 v Alberta (Attorney General), 2012 ABCA 130 (CanLII), application for leave to appeal to SCC filed on June 28, 2012.

Improper disclosure of financial personal information warrants $4,500 in damages

On June 14th of last year the Federal Court ordered a bank to pay $4,500 in damages for disclosure of personal financial information that was subject to a subpoena directly to the requesting party's counsel. In making the award it noted that the clerk who made the disclosure denied responsibility.

Landry, 2011 FC 687 (CanLII).

Investigator's use of wife's e-mail account leads to stay for abuse of process

The use of personal e-mail accounts for work purposes is out of control. A May 23rd judgment of the Court of Appeal of Alberta illustrates.

The Court affirmed a stay of prosecution that an accounting profession tribunal ordered because an investigator used his wife's e-mail to send and receive correspondence in conducting an investigation. The Court agreed with the tribunal that the respondent did not consent.

The Court also held that the tribunal was reasonable to conclude that a stay (though an extreme remedy) was warranted, particularly given the investigation and prosecution at issue was for breaching client confidences: "...the stay was the only way to hold the CIC to the standard of conduct expected of all members of the profession."

Clark v Complaints Inquiry Committee, 2012 ABCA 152 (CanLII).

Information about business subsidies received not personal information

On June 15th the Alberta Court of Queen's Bench affirmed an Alberta OIPC finding that amounts of financial assistance received by livestock farmers under two government programs were not the farmers' personal information. The OIPC held that even if the information could be linked indirectly to individuals (*e.g.*, owners of sole proprietorships or closely held corporations) there was no proof that it had a "personal dimension" sufficient to qualify. The Court held the OIPC's order was transparent and detailed, "made sense" and was consistent with the purpose of Alberta FIPPA.

Agriculture Financial Services Corporation v Alberta (Information and Privacy Commissioner), 2012 ABQB 397 (CanLII)

Information about landlords not personal information

On September 30th of last year the Ontario Superior Court of Justice held that certain information about residential landlords was not their personal information in the circumstances.

The issue arose in an application that challenged a municipal by-law requiring landlords to obtain licences for residential rental units. The by-law required landlords to submit information in support of a licence (including name, telephone number and address information). The by-law also required a copy of an issued licence (which included similar information) to be posted. The applicants argued that the by-law conflicted with the *Municipal Freedom of Information and Protection of Privacy Act*.

The Court held that MFIPPA's privacy protection part was not engaged because the information at issue was information that identifies an individual in a business capacity rather than personal information.

London Property Management Association v City of London, 2011 ONSC 4710 (CanLII).

Law firm publication draws damages award for breach of privacy

On September 13th of last year the Federal Court ordered a law firm to pay $1,500 in damages for publishing an Office of the Privacy Commissioner of Canada decision letter and report of findings that contained an individual's personal information.

PIPEDA allows some publicly available information to be used and disclosed without consent, including:

> personal information that appears in a record or document of a judicial or quasi-judicial body, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document

The OPC arguably does not act as a judicial or quasi-judicial body in investigating privacy complaints nor are its decision letters and reports public, so the law firm could not rely on this exception.

Girao v Zarek Taylor Grossman Hanrahan LLP, 2011 FC 1070 (CanLII).

Institution faced with data breach should not have protected employee

The Information and Privacy Commissioner/Ontario issued a privacy complaint report on July 3rd that illustrates the downside of protecting an employee who has gained unauthorized access to personal information.

The IPC likes institutions and health information custodians to hold employees accountable for gaining unauthorized access to personal information by imposing discipline and (controversially) sharing the details of the disciplinary response with affected individuals. It made this position clear in 2010 in *HO-010*. In this most recent report, it even suggested that institutions should have a policy that calls for disclosing the details of its disciplinary response barring exceptional circumstances.

The report is about an OPP clerk who gave access to an occurrence report about the complainant to an acquaintance who was the complainant's landlord. The OPP admitted the breach but also shouldered the blame. It counseled the clerk and provided remedial training to all clerks. In its representations to the IPC the OPP said "The clerk appeared to have acted alone, and made a single error on one occasion resulting in the disclosure of a single record. We believe that this mistake was due to a lack of training, rather than as a result of malice or intent."

The IPC quoted this representation twice before rejecting it and reiterating the principles from *HO-010*. It was a very problematic position to take given *HO-010* and the sensitivity of the personal information in a police occurrence report. It is also hard to frame actions like the clerk's as merely negligent.

The IPC then, as invited by the OPP's position, engaged in a detailed analysis of the OPP privacy governance framework before making a number of negative findings about the OPP's policies, procedures and training. One wonders whether the OPP's privacy governance framework would have been questioned at all if it had simply assigned fault to the clerk.

Ontario institutions and health information custodians who are faced with a privacy breach need to conduct thorough investigations with good causal analysis before the IPC gets involved. If fault lies with one or more employees, assigning fault and imposing appropriate consequences appears to be a relatively simple way to meet the IPC's expectations. Taking such steps may even dissuade the IPC from asking broader and potentially more painful questions about organizational privacy governance.

Ontario (Community Safety and Correctional Services) (Re), 2012 CanLII 37748 (ON IPC).

Majority of BCCA says accuracy duty applies broadly

On June 26th the Court of Appeal for British Columbia restored a finding that the British Columbia Ministry of Children and Family Development breached British Columbia FIPPA by failing to make every reasonable effort to ensure the accuracy of personal information before using it to answer a background check inquiry.

This is a very well-litigated dispute about a communication made by the Ministry to a social services employer who contacted the Ministry, with consent, to check into the background of a new employee. The Ministry disclosed the existence of a complaint made against the employee. It also noticed some irregularities in its file, did a full review of the file (without going behind the file to make inquires) and said to the employer, "to be on the safe side, I would prefer that he may be supervised, if you can do this."

The employee was terminated and has since been on a long campaign to seek redress. In May 2010, the British Columbia Court of Appeal dismissed the employee's $520 million action against the Ministry and others as disclosing no reasonable cause of action. About a year earlier, the Court of Appeal heard an appeal of the employee's privacy complaint and sent it back to the B.C. OIPC so the OIPC could consider whether the Ministry breached section 28 of the B.C. FIPPA. Section 28 imposes a duty to make every reasonable effort to ensure the accuracy of personal information that is used to make a "decision that directly affects [an] individual."

In the decision, a 2-1 majority of the Court held that the OIPC was reasonable to conclude that the Ministry's act of issuing a caution to the employer entailed a use of personal information in making a "decision that directly affects [an] individual." Madam Justice Bennet wrote for the majority. Most significantly, she affirmed the OIPC's broad reading of "decision" - to encompass formal and informal decisions - as reasonable. Mr. Justice Hinkson did not take issue with this finding in his dissent. He held that Ministry's highly qualified advice could not even be elevated to the status of an informal decision.

The public sector access and privacy statutes in Nova Scotia, Newfoundland, Prince Edward Island, Alberta and the three territories contain provisions with similar or identical language to section 28.

British Columbia (Ministry of Children and Family Development) v Harrison, 2012 BCCA 277.

Motion for certification dismissed in Québec data breach class action

On March 15th the Québec Superior Court dismissed a motion for authorization of a class action that claimed damages in negligence for the loss of a data tape containing the personal information (name, address, social insurance number, date of birth and some credit history information) of approximately 240,000 individuals. It held that the class action could not be founded on "potential damage" and that the petitioner failed to establish she suffered compensable psychological damage – *i.e*., a level of psychological disturbance that rises above the "ordinary annoyances, anxieties and fears that people living in society routinely, if sometimes reluctantly, accept."

Mazzona c DailmerChrysler Financial Services Canada, 2012 QCCS 958.

No damages for breach of PIPEDA - harms unclear, apology given

On May 8th the Federal Court declined to award damages under PIPEDA because the applicant had not adduced any evidence of the humiliation he suffered and the respondent had been very forthright in dealing with the breach, including by issuing an apology.

Townsend v Sun Life Financial, 2012 FC 550 (CanLII).

Ontario Court says applicant can't circumvent statutory access procedure

On July 13th the Ontario Superior Court of Justice held that it did not have jurisdiction to order a federal government institution to produce a personnel file to a deceased employee's estate.

The estate sought the file because it was trying to determine if the deceased had the mental capacity to designate an unknown third party as beneficiary under his pension plan. The Court's decision that it lacked jurisdiction to order production is very qualified. It rested to some degree on the record filed, but the Court does hint that it lacked jurisdiction because the motion was for production of information that could be accessed via the federal *Privacy Act*. In any event, the Court said that, as a matter of discretion, it would not have granted an order that allows one to circumvent the *Privacy Act*: "Finally, it is apparent to

me that even were there some sort of inherent right of this court to make the production order, I would not order it in the face of the clear process for obtaining production of private or personal information under the *Privacy Act*."

MacDonald Estate v Department of National Defence, 2012 ONSC 4155 (CanLII).

Ontario data breach class action settles

On July 3rd the Ontario Superior Court of Justice approved a settlement in a significant class action that was brought after a public health nurse lost a USB key containing the personal information of about 85,000 individuals who had been immunized during the 2009 H1N1 scare.

The settlement involved the creation of a claims period open until August 1, 2016 to allow class members to claim for economic loss but no damages payment otherwise. As Justice Lauwers explained, the defendant and its insurer agreed to accept the risk of economic harm over the six and a half year claim period, after which, he said, "the risk will be virtually eliminated."

In approving the settlement, Justice Lauwers stressed that the plaintiff faced a difficult case given, as time passed, his ability to prove compensable damages worsened.

Justice Lauwers approved an agreement to pay $500,000 in costs (including taxes and disbursements) to class counsel plus an amount equal to 25% of any claims paid. Though loss to individuals was not the basis for this amount, it equals about $5.99 per affected individual for a suspected breach involving the loss of name, address, telephone number, gender, date of birth, Ontario health number, health card expiration date, name of primary care provider and "some additional personal health information."

Rowlands v Durham Region Health, 2012 ONSC 3948 (CanLII).

PIPEDA judgment must stand until revisited by Court of Appeal for Ontario

On June 6th the Ontario Superior Court of Justice dismissed a motion by an execution creditor for an order to compel a mortgagee to provide a mortgage discharge statement so it could enforce its judgment by way of a sheriff's sale.

Justice Gray held that he was bound to apply the Court of Appeal's 2011 judgment in *Citi Cards Canada Inc v Pleasance*, in which Justice Blair held that such an order is precluded by the federal *Personal Information Protection and Electronic Documents Act*. Justice Gray confessed to being troubled by the outcome and wrote an invitation to appeal by opining on various theories in which the disclosure of personal information in a discharge statement would comply with the consent rule in PIPEDA. He questioned, for example, whether a mortgagor implicitly consents to the disclosure of information about his or her mortgage to third parties with an interest in the mortgage and whose interest is at stake.

Royal Bank v Trang, 2012 ONSC 3272 (CanLII).

Sale of business to proceed under the cover of a PIPEDA exemption order

On April 26th the Ontario Superior Court of Justice issued an order under section 7(3)(c) of the *Personal Information Protection and Electronic Documents Act* to allow credit unions to merge without gaining the express consent of members. It is not clear that such an order is actually authorized by PIPEDA (and the applicants don't appear to have given notice to members), but Justice Lauwers listed a number of Ontario commercial list matters in which such permissive orders have been made. He echoed comments made by Justice Farley in "urging that a route be provided that will permit the disclosure of the necessary personal information in such circumstances as these to avoid wasting the court's time and the parties' funds."

In the Matter of an Application Under Rules 14.05(3)(d), 2012 ONSC 2530 (CanLII).

PRIVILEGE

BCCA splits on privilege given to lawyers' trust account ledgers

On March 27th the Court of Appeal for British Columbia split on whether lawyers' trust account ledgers are presumptively subject to solicitor-client privilege.

Mr. Justice Smith dissented. He noted that, in *Maranda v Richer*, the Supreme Court of Canada held that "all information arising out of solicitor-client relationships whatever may be their legal context" is presumptively privileged. Facts are not privileged, but Smith J. A. explained that the Supreme Court adopted a broad and protective rule for a record related to the solicitor-client relationship because solicitor-client privilege is so important and because "it is difficult to segregate single professional acts from the complex of facts, events, and communications that characterizes ongoing solicitor-client relationship."

Mr. Justice Chiasson (Madam Justice Newbury concurring) held that *Maranda* was about a search for lawyer fee accounts in the course of a law enforcement investigation and could not be applied directly to a dispute about the production of trust account ledgers in the civil context. Trust accounts, according to the majority, "generally record facts." Therefore, the party claiming privilege over trust account ledgers must establish that the entries claimed "arise out of the solicitor-client relationship and what transpired within it" to establish a rebuttable claim. In applying this test, the majority held that some entries met this test and others which related strictly to a real estate transaction did not.

The Court also unanimously rejected application of the crime and fraud exception to solicitor-client privilege in the circumstances and made a comment on the procedure for hearing privilege claims in a manner that protects privilege but is also fair and transparent.

Donell v GJB Enterprises Inc, 2012 BCCA 135.

E-mails sent to in-house counsel for "simultaneous review" not privileged

Master Short of the Ontario Superior Court of Justice issued a decision on December 21st of last year in which he held that e-mails merely copied to in-house counsel were not subject to solicitor-client privilege.

Humberplex v TransCanada Pipelines, 2011 ONSC 4815 (CanLII).

Federal Court protects CJC's "fact finder" report as privileged

On December 13th of last year the Federal Court held that a report prepared by Professor Martin Friedland to the chair of a judicial conduct committee was subject to solicitor-client privilege and therefore not to be filed in a judicial review of the chair's decision to dismiss a complaint.

Although Professor Friedland was retained under Canadian Judicial Council policy to make "further inquires" into a judicial conduct complaint - a fact-finding role in its essence - the Court held that his communication to the chair was best considered to be legal advice given Friedland's status as a lawyer and the legal context for his communication.

The Court also held that privilege applied to the entire report, making clear that the common law generally does not contemplate the severance and partial disclosure of a privileged communication. Finally, the Court stated that Professor Friedland's report was subject to public interest privilege given the special need to encourage full and frank participation in the investigation process.

Slansky v Canada (Attorney General), 2011 FC 1467 (CanLII).

Lawyers' notes taken before third party privileged

On May 7th the Ontario Superior Court of Justice held that notes taken by lawyers who represented individuals at audit committee interviews were privileged. The Court accepted that the notes were taken for the dominant purpose of reasonably anticipated litigation and that they were worthy of protection given they reflected the lawyers' thinking and were more than mere transcriptions. The Court also ordered the lawyers, who were called as witnesses to the interviews, to refresh their memories by reading their notes.

R v Dunn, 2012 ONSC 2748 (CanLII).

Justice Perell carves out broad exception to settlement privilege for ongoing actions

On June 4th Justice Perell of the Ontario Superior Court of Justice issued a decision that establishes a relatively broad exception to settlement privilege for signed settlement agreements that change the adversarial orientation of an ongoing lawsuit. He held that the exception applies regardless of the technical form of the settlement and held that settling parties have an obligation to promptly (and in advance of trial) disclose agreements to their opponents and to court. Justice Perell also held that settlement privilege is a class privilege and need not be established on a case-by-case basis.

Moore v Bertuzzi, 2012 ONSC 3248 (CanLII).

Notes privileged, facts discoverable says court

On April 7th of last year the Ontario Superior Court of Justice issued a decision in which it explained the degree to which a valid privilege claim protects information from discovery.

The Court held that notes taken by a non-lawyer at the direction of a lawyer for the purpose of receiving legal advice about a human rights complaint and defending the complaint were privileged. It specified however, that the privilege did not preclude the discovery of relevant information learned through the non-lawyer's fact gathering process, including the names of persons interviewed and the substance of their evidence.

Reis v CIBC Mortgages Inc, 2011 ONSC 2309 (CanLII).

"Stolen" solicitor-client communications to be returned

On January 11th the Ontario Superior Court of Justice ordered solicitor-client communications to be returned to the exclusive possession of a defendant to a constructive dismissal action and denied the plaintiff a declaration that privilege had been waived based on an alleged "reckless" disclosure.

Pottruff v Don Berry Holdings Inc, 2012 ONSC 311 (CanLII).

PRODUCTION

ABCA modifies spoliation remedy, preserves sanction

On May 7th the Court of Appeal of Alberta varied a sanction for spoliation because it was not well-proportioned. It explained:

> As a remedy for the contempt, the chambers judge ordered that the individual appellant pay the cost of the application on a full indemnity basis. While acknowledging that "in the present case no information has been lost", he nevertheless ordered a full computer forensic investigation. The chambers judge speculated that "it is unclear what else may have been deleted". The contempt application was based entirely on the efforts to delete

> the HSE Manual. No allegation was made of the destruction of any other document, nor is there any evidence of any other destruction. Embarking on an expensive fishing expedition at this stage of the litigation is unwarranted. Should the discovery process produce evidence of other problems, further applications for relief can be brought.

Despite allowing the appeal in part, the Court ordered the appellant to pay the full costs of the appeal "to ensure an effective sanction."

Fuller Western Rubber Linings Ltd v Spence Corrosion Services Ltd, 2012 ABCA 137 (CanLII).

Arbitrator denies production to challenge youth's credibility

On October 15th of last year Arbitrator Joseph Carrier denied a production request that sought a variety of records relating to a resident of a facility for young offenders.

The request was made before a hearing of a discharge grievance. The employer terminated the grievor based on evidence provided by a resident. The union intended to dispute the resident's evidence. His credibility would be an issue.

Arbitrator Carrier's decision requires reasonable particulars to be provided in support of a request for production. It also stands for the proposition that production will not be ordered for the sole purpose of challenging the credibility of a witness.

OPSEU, Local 601 and Northern Youth Services (15 October 2011, Carrier).

Case shows when sending a preservation letter to opposing counsel matters

Sending preservation letters to opposing counsel can be quite a useless exercise when done as a matter of routine. A March 20th decision of the British Columbia Supreme Court illustrates when a hold letter can serve a critical purpose. It also illustrates how a party's duty to preserve evidence that is likely to be relevant in foreseeable litigation can weigh heavily in favor of allowing an adversary to inspect evidence where no direct duty to allow for such an inspection exists.

The facts are simple. A fire started on the defendant's premises and spread to the plaintiff's premises. The defendant denied the plaintiff's insurer access to its premises, which led the plaintiff's insurer to write. The insurer said that it would likely bring a subrogated claim and that the plaintiff should preserve all physical and other evidence. This left the defendant with an option to allow the requested inspection or stop cleaning the damaged property and debris. It did neither.

The plaintiff raised a spoliation claim in the context of a production dispute. It claimed that privilege in certain communications should be waived in the interests of justice on account of the defendant's spoliation. Master Baker of the BCSC agreed.

Brown v Wilkinson, 2012 BCSC 398 (CanLII).

Court sanctions departed employee for intentional spoliation

On March 7th, the Alberta Court of Queen's Bench found a departed employee in contempt for counseling a contact to destroy evidence for the purpose of interfering with the administration of justice. The Court ordered the employee:

- to produce any and all computers and electronic media in his possession, power or control, for a forensic review to be conducted by a computer expert retained by the plaintiffs;

- to pay for the review and post $30,000 in security for costs; and
- to pay the costs of the contempt motion on a full indemnity basis.

Fuller Western Rubber Linings Ltd v Spence Corrosion Services Ltd, 2012 ABQB 163 (CanLII).

Non-party privacy tips the balance in favor of *Anton Piller*

On November 23rd of last year the Alberta Court of Queen's Bench issued an *Anton Piller* order based significantly on a concern for the privacy interest of customers whose information the plaintiff alleged had been stolen.

The plaintiff is a BMW dealership that was confronted with a regrettable breach of its sales and customer relationship management system when it failed to remove system privileges from a terminated manager. It alleged the manager gained unauthorized access to the system and downloaded the names, e-mail addresses and "other personal details" of about 5000 customers.

The Court noted that it contained gaps, but seemed to be swayed by the customer privacy interest at stake and stated that a public interest supported making the order.

Bavaria Autohaus (1997) Ltd v Beck, 2011 ABQB 727 (CanLII).,

Master MacLeod gives a boost to role of particulars under new Ontario rules

In a decision issued June 6th, Master MacLeod of the Ontario Superior Court of Justice asked whether particulars should be more readily ordered under the Ontario rules given the relationship between pleading, discovery and expense. He concluded:

> All of this is to say that the requirement of particulars for the purpose of pleading should not be construed too narrowly. A request for particulars should be upheld if it appears that it will result in a more focused and intelligent pleading and it should be refused if it simply adds another unnecessary step or delays the progress of the action.

Ottawa (City) v Cole & Associates Architects Inc, 2012 CarswellOnt 7204.

Plaintiff ordered to disclose information on social media sites

On December 12th of last year, the Ontario Superior Court of Justice ordered a plaintiff in a motor vehicle accident case to re-attend at discovery to answer questions about photographs of himself that he posted on his Facebook or MySpace pages and to produce such photos if they exist. The defendant did not establish the relevance of status updates and messages posted by others.

Morabito v DiLorenzo, 2011 ONSC 7379 (CanLII).

POA defendants get *McNeil* disclosure despite inspector privacy claim

On May 3rd, the Divisional Court held that defendants to regulatory prosecutions under the *Provincial Offences Act* receive the benefit of "*McNeil* disclosure" notwithstanding a claim made by OPSEU on behalf of provincial regulatory inspectors.

"*McNeil* disclosure" is a form of Crown disclosure facilitated by a 2009 Supreme Court of Canada decision. The Court held that the Crown has a positive duty to build-out the Crown brief by making "reasonable inquiries" of other Crown agencies and departments. This duty, said the Court, includes a

duty to collect and disclose records of police misconduct, at least where an officer is likely to be a witness at trial and has a record with some arguably relevant blemishes.

After *McNeil* was issued, the Ontario Ministry of Labour initiated a procedure for conducting CPIC checks on Ontario *Occupational Health and Safety Act* inspectors to support its disclosure duties. OPSEU grieved, and in March 2011 the Grievance Settlement Board held that the Ministry's procedure did "not accord with an appropriate exercise of management rights under the [OPSEU/OPS] Collective Agreement." The Toronto Star headline read, "Province slammed for secret criminal checks on labour inspectors."

The Divisional Court has now held that the GSB erred in finding that an inspector's criminal record should not be the subject of first party disclosure pursuant to *McNeil*. This is good news for POA defendants.

OPSEU v Ontario, 2012 CarswellOnt 6293, 2012 ONSC 207.

Party can assert a duty to ensure relevant evidence held by another is preserved

On June 7th the Ontario Superior Court of Justice dismissed a partial summary judgment motion, thereby allowing a defendant to plead that the plaintiff had committed spoliation by failing to obtain a piece of plastic she had ingested after it was surgically removed. The plaintiff argued that the pleading should be struck because there was no claim that she ever had power, possession or control of the piece of plastic (which was lost by the hospital at which she was treated). Justice Quigley held that summary judgment is not a means to strike part of a defence and that the defence pleaded was novel yet "legally tenable."

Melissa Topp v Costco Wholesale Canada Ltd, 2012 ONSC 3354 (CanLII).

SEARCH AND SEIZURE

Ontario CA on computer searches - broad access and targeted searches endorsed

On October 12th of last year the Court of Appeal for Ontario issued a judgment in which it held the police violated section 8 of the *Canadian Charter of Rights and Freedoms* by proceeding with a lawfully authorized search of a personal computer after finding evidence of a crime that was not within the scope of authorization. This important decision recognizes a police duty to search carefully (as opposed to indiscriminately) for evidence of crime and stop upon finding incriminating evidence that is beyond the scope of a warrant.

R v Jones, 2011 ONCA 632 (CanLII).

WORKPLACE PRIVACY

Alberta arbitrator awards $1,250 per unauthorized credit check

On April 5th, Arbitrator Andrew Sims awarded $1,250 to each member of a group of 26 government of Alberta employees because the government checked each employee's credit without authorization or sufficient justification.

An internal investigator conducted the checks to see if any of the employees were in financial difficulty, which he thought might indicate a motive to engage in the fraud he was investigating. The government admitted a breach and apologized, but its employees' union grieved to seek damages. Arbitrator Sims heard the grievance based on an agreed statement of facts that stipulated the employees had "suffered emotional stress in their personal lives and in the workplace."

Arbitrator Sims relied on the Court of Appeal for Ontario's decision in *Jones v Tsige* and the Federal Court's decision in *Nammo v Trans Union of Canada* in crafting a damages award.

Alberta v Alberta Union of Provincial Employees (Privacy Rights Grievance), [2012] AGAA No 23 (Sims) (QL).

Arbitrator okays recording of investigation interview

On July 18th of last year Arbitrator Colin Taylor dismissed a grievance about recording an interview with an employee who was the subject of investigation. He held that recording an interview (openly) did not violate the employee's right to representation or any other collective agreement right.

There are mixed views about the wisdom of recording interviews, with some believing that recording has a negative effect on candor that outweighs its benefit.

Teck Coal (Fording River) and USW, Local 7884 (18 July 2011, Taylor).

Arbitrator says demand for personal cell phone records not justified

On November 22nd of last year Arbitrator Michel Picher held that an employer was not justified in demanding production of an employee's personal cell phone records.

The employee - an apprentice diesel mechanic who worked in a safety sensitive environment - was observed holding his Blackberry device contrary to company policy. He said his shift was almost over and he was just checking the time. In its investigation, the employer asked for copies of his cell phone records.

Arbitrator Picher inferred that the request was made for the purpose of checking whether the employee had used his phone earlier in the shift, an improper purpose (not supported by reasonable grounds, I note) and a significantly different purpose than following up on a significant accident or near miss. Arbitrator Picher has previously endorsed limited requests for personal cell phone records for the latter purpose.

The Canadian Pacific Railway and CAW-Canada, Local 101 (22 November 2011, M. Picher).

Arbitrator says *Jones v Tsige* doesn't matter in workplace medical management

On February 22nd Arbitrator George Surdykowki held that the Court of Appeal for Ontario's recognition of an "intrusion upon seclusion" tort does not change rights and obligations related to the use of employee medical information for employment purposes. It's nice to have a clear and strong statement like this so soon after the Court of Appeal's landmark judgment. The medical information management arbitral jurisprudence that deals with justification for collection is well-settled and well-calibrated. *Jones v Tsige* doesn't and shouldn't make a difference.

Complex Services Inc and OPSEU, Local 278 (22 February 2012, Surdykowki).

Case demonstrates need for internal controls on IT searches

Employers who are regulated by privacy legislation need to reckon with privacy commissioner oversight in conducting searches of their work systems for evidence of misconduct. This is the clear lesson from the recent and much-discussed Calgary Police Service order of the Alberta OIPC that dealt with the service's unauthorized access to an employee's personal e-mail account.

The facts are simple. The service embarked on an internal sexual misconduct investigation that included a review of an employee's work e-mail account. It conducted a search for the word "password" as a matter of protocol because the sending and receiving of passwords through e-mail is indicative of a number of common IT security problems. The service found a message to an outsider containing the employee's password to her personal e-mail account, a communication the service said "seemed odd." Given the employee had also sent "snippets" of confidential service records to others internally, the service accessed the personal account on a theory that the employee was leaking confidential

information through the personal e-mail account. It happened to find evidence of work-related sexual misconduct and used it to discipline the employee. The employee later complained to the OIPC under Alberta's public sector privacy legislation.

The OIPC was not impressed with the service's professed basis for using the password to access the employee's personal account, particularly given the investigator had no mandate to determine whether the employee had committed a breach of confidence. It upheld the employee's complaint.

The result is no surprise. Taking a step in an investigation as intrusive as gaining unauthorized access to a personal e-mail account based significantly on the discovery of a communication that "seemed odd" is problematic. The record shows that the service was clearly on a fishing expedition, and despite the OIPC's finding, its approach still signals respect for management's right to investigate. The OIPC says, for example, "It might be policy for IT to check for data leakage whenever a Public Body employee is being investigated for inappropriate email or computer use, but this cannot extend, without cause, to an employee's personal email account."

Order F2012-07 (April 30, 2012).

Discipline undermines grounds for referral to psychiatric assessment

On April 3rd Arbitrator Nimal Dissanyake held that an employer did not have grounds to order an employee to attend a psychiatric assessment. He was driven by a number of factors:

- the employee had demonstrated a pattern of angry behavior, but had not made an express or implied threat;
- the employer did not base its assessment direction on input from a company physician/advisor;
- the employer's decision maker admitted that he (simply) had doubts about the employee's mental health; and
- the employer disciplined the employee for the same behavior that caused it to issue its assessment direction.

While Arbitrator Dissanyake rejects "a technical rule that conduct that had been the subject of discipline in the past may not be relied upon in requiring an IME," his reasoning suggests that basing a discipline charge and an order to attend an IME on the same behavior is problematic. While employers should be careful about picking their means of managing aggressive or angry behavior in the workplace, question whether an employee can have the mental capacity to commit a workplace offence and, at the same time, have a mental condition that (on reasonable grounds) requires assessment.

IBEW, Local 636 and Niagara Peninsula Energy Inc (3 April 2012, Dissanyake).,

Employer has duty to protect employee's reputation in some circumstances

On May 29th the Federal Court of Appeal held that an employer breached a duty to protect its employee's reputation, but also made clear that the duty arose only out of the well-established duty to exercise good faith in terminating employment - the "*Wallace* duty."

The facts are worth a close read and detailed analysis, but we will simplify here and say that employers who terminate an employee who is embroiled in public controversy without asserting cause for reasons related to the controversy ought to beware of a positive duty to protect the employee's reputation.

Tipple v Canada (Attorney General), 2012 FCA 158 (CanLII).

"Meaningful on call duties" mean position has safety sensitive status

In a March 30th decision, Arbitrator Michel Picher said, "An employee who is trained and remains meaningfully on call to perform safety sensitive functions must be recognized as having safety sensitive status, regardless of the frequency of the functions." In applying this principle, he held that qualified diesel mechanics at a railyard were in a safety sensitive position even though they only were required to operate locomotives on a very occasional basis - some as little as a few times a year. Arbitrator Picher's finding means that the mechanics are subject to special medical assessment and drug and alcohol testing requirements.

Canadian Pacific Railway Company and CAW-Canada, Local 101 (30 March 2012, M Picher).

Ontario arbitrator treats the occupational health file as a locked box

On August 31st of last year Arbitrator Russell Goodfellow issued an order relating to the production of a grievor's occupational health file before a pending arbitration hearing. In doing so, he suggested that an employer requires consent or an arbitrator's order to use information in an occupational health file in preparing for arbitration, a suggestion many employers will find problematic.

Telus Inc v Telecommunications Workers Union, 2011 CanLII 57030 (ON LA).

Outburst does not justify direction to attend psychiatric assessment

On June 29th of last year Arbitrator Michel Picher held that an employer was not justified in directing an employee who had made a concerning outburst to a psychiatric assessment.

The employee was a 26-year mechanic who became frustrated about the theft of his tools. The company alleged he told a manager that he, "was bringing in a knife, and that the next time someone touches anything of his he will cut their hand or head off." He later said he would pray that the manager and his family would answer to God. The company referred the employee to its OHS physician, who recommended that the employee attend an IME. This led to a lengthy dispute that came before Arbitrator Picher five years later, after the parties agreed the employee would be reinstated; they argued only about the terms of reinstatement, including whether an IME would be a condition of return.

Employers faced with concerning behavior are in a dilemma, and should never be too confident in their own ability to assess an employee's disposition to commit an act of violence. This case is notable as highlighting the requirement to have a reasonable basis for requiring a psychiatric assessment, but the finding is very qualified. Arbitrator Picher noted that the employee had supported his rejection of the IME direction by submitting medical evidence from his own physician, evidence that the company appeared not to address effectively in the arbitration. He also noted that the precise statement made by the employee was in dispute, and the employer did not bring the manager to the hearing. Finally, Arbitrator Picher ordered the employee to be reinstated without compensation. In a way, the employer got what it wanted: an independent review of the circumstances prior to reinstatement.

The Canadian Pacific Railway and CAW-Canada, Local 101 (29 June 2011, M. Picher).

Significant public sector criminal background check decision

On July 25th the Information and Privacy Commissioner for British Columbia issued a significant report on public sector criminal background checks, pushing the government of British Columbia to further tailor the scope of its program.

The report was about the province's screening program and not vulnerable sector checks governed expressly by British Columbia criminal record check legislation. The program seems to be a top notch program. For example, it applies based on a job classification scheme developed based on a risk assessment, it limits police checks in favor of CPIC checks and it features adjudication of positive results by a body at arms length from the hiring department.

Nonetheless, the Commissioner conducted a very close review and took issue with a number of aspects of the program, especially its breadth. For example:

- She held that four out of the ten job classifications to which a background check requirement applies are redundant or drafted too broadly. According to the Commissioner, for example, a mere responsibility for handling personal information should not attract a background check requirement given there are other means of controlling for misuse of personal information (like access control and access logging, she mentioned).

- She held that requiring a check when dictated by third parties was "fundamentally flawed": "Government should determine when it will conduct criminal record checks on its employees and it should ensure that it only conducts record checks when it is authorized by FIPPA to do so."

- She held that post-employment checks should not be a routine requirement except for "particularly sensitive functions" and when someone is hired into a new position with a significantly different risk profile.

The third party finding is aggressive, but might have been conceived by the Commissioner as a means of giving the British Columbia government bargaining power over the third parties with whom it deals. The post-employment check limitation is also a significant constraint. In making this finding the Commissioner drew from Arbitrator Michel Picher's finding in a case involving firefighters at the City of Ottawa. The Commissioner's finding in this report and her adoption of Mr. Picher's principled statements are likely to be taken together as quite authoritative.

The Commissioner also addresses issues related to the identification of candidates, notification and record retention.

Investigation Report F12-03 (25 July 2012, Information and Privacy Commissioner for British Columbia).

SUBJECT MATTER INDEX

HICKS MORLEY'S INFORMATION AND PRIVACY PRACTICE GROUP

Toronto Office

Michelle Alton

Brenda Bowlby

Joseph Cohen-Lyons

Ian Dick

Mireille Khoraych

Craig Lawrence

Daniel Michaluk

Simon Mortimer

Craig Rix

David Ross

Amy Tibble

Scott Williams

Andrew Zabrovsky

Nadine Zacks

London Office

Paul Broad

Waterloo Office

Seann McAleese

Kingston Office

Vince Panetta

Ottawa Office

George Vuicic