



CANADIAN PRIVACY LAW REVIEW

Volume 8 • Number 7

June 2011

In This Issue:

Making Privacy Protection More Effective for Canadians: Recent and Proposed Legislative Reforms

Regan Morris.....65

Privacy Commissioner Can Now Be Choosier about Complaints She Investigates

David Elder.....71

Workplace Computer Pornography Ruling: Police Need Search Warrant; Employer Has Latitude

Maria Giagilitsis and Brian P. Smeenk.....73



MAKING PRIVACY PROTECTION MORE EFFECTIVE FOR CANADIANS: RECENT AND PROPOSED LEGISLATIVE REFORMS

By Regan Morris

Legal Counsel, Office of the Privacy Commissioner of Canada

Introduction

As anyone familiar with the mandate of the Privacy Commissioner of Canada knows, complaints from individual Canadians are an important part of her work. Complaints received from the public are one of the principal means by which investigations are initiated in relation to privacy protection in the public sector and in the private sector. The obligations of the private sector are enforced through the *Personal Information Protection and Electronic Documents Act* [*PIPEDA* or the *Act*].¹ Each year the Office of the Privacy Commissioner (“the OPC”) receives hundreds of complaints, undertakes investigations, and issues reports under *PIPEDA* setting out the Commissioner’s findings and recommendations.

The process to investigate complaints is fraught with challenges. Indeed, there have been criticisms of the complaint-process in this law review.²

On this point, Commissioner Stoddart has recently stated that one of her priorities for the next three years will be improving “service delivery”.³ In a recent speech to the University of Ottawa, she described this priority as follows:

While all of the work we do is important, at the end of the day, the priority that is most important to me on a personal level is service to individual Canadians. I want to ensure that Canadians calling my Office for help with a problem will receive the level of service they expect from us.⁴

Whether the goal of providing better service to Canadians will be met depends on a number of factors. Continued efforts to improve internal operational efficiencies will no doubt enhance the quality and effectiveness of investigations. However, upcoming and contemplated changes to *PIPEDA* — some of which have already been enacted and some of which have been proposed — also have the potential to make the OPC more efficient and effective, and thereby improve how our office serves Canadians.

Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

Design and compilation © LexisNexis Canada Inc. 2011. Unless otherwise stated, copyright in individual articles rests with the contributors.

ISBN 0-433-44417-7 ISSN 1708-5446

ISBN 0-433-44418-5 (print & PDF)

ISBN 0-433-44650-1 (PDF)

ISSN 1708-5454 (PDF)

Subscription rates: \$215.00 (print or PDF)

\$330.00 (print & PDF)

Editor-in-Chief:

Professor Michael A. Geist

Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

LexisNexis Editor:

Boris Roginsky

LexisNexis Canada Inc.
Tel.: (905) 479-2665 ext. 308
Fax: (905) 479-2826
E-mail: cplr@lexisnexis.ca

Advisory Board:

- **Ann Cavoukian**, Information and Privacy Commissioner of Ontario, Toronto
- **David Flaherty**, Privacy Consultant, Victoria
- **Elizabeth Judge**, University of Ottawa
- **Christopher Kuner**, Hunton & Williams, Brussels
- **Suzanne Morin**, Bell Canada, Ottawa
- **Bill Munson**, Information Technology Association of Canada, Toronto
- **Stephanie Perrin**, Service Canada, Integrity Risk Management and Operations, Gatineau
- **Patricia Wilson**, Osler, Hoskin & Harcourt LLP, Ottawa

Note: This Review solicits manuscripts for consideration by the Editor-in-Chief, who reserves the right to reject any manuscript or to publish it in revised form. The articles included in the *Canadian Privacy Law Review* reflect the views of the individual authors and do not necessarily reflect the views of the advisory board members. This Review is not intended to provide legal or other professional advice and readers should not act on the information contained in this Review without seeking specific independent advice on the particular matters with which they are concerned.

In this article, I would like to discuss these legislative changes, which can be divided into three separate phases. In the first phase are the recent changes to the powers of the Privacy Commissioner brought about by Bill C-28, or what is now being referred to informally as Canada's Anti-spam Legislation ("CASL").⁵ In the second phase are the changes contemplated in Bill C-29, in particular the changes related to data breach notification.⁶ The third phase encompasses changes that may result from the second five-year Parliamentary review of *PIPEDA*, as mandated by s. 29 of the *Act*.

Phase 1: CASL and the new investigative discretion and information sharing powers

CASL, which received royal assent on December 15, 2010, creates a regulatory regime to address spam, malware, spyware and other related online threats.⁷ However, it also introduced two new amendments to *PIPEDA* that will have broader application and that are not directly tied to spam. The first amendment empowers the Commissioner to either decline to investigate a complaint or discontinue an investigation that is already underway.⁸ A second amendment allows the Commissioner to enter into agreements or arrangements with her provincial counterparts and foreign authorities for the purposes of cooperation and information sharing.⁹ Both amendments, which were recently brought into force,¹⁰ have the potential to increase the effectiveness of the OPC in addressing contraventions of *PIPEDA*.

a. Investigative discretion powers

Formerly under *PIPEDA*, the Commissioner was required to investigate all written complaints filed with the OPC.¹¹ She did, however, have the discretion, after conducting an investigation, not to issue a report in four circumstances that were set out in s. 13(2) of the *Act*:

- where there are existing grievance or review procedures that the complainant should exhaust first (s. 13(2)(a));
- where there are other procedures that would be more appropriate for dealing with the complaint (s. 13(2)(b));

- where a report would not be useful given the amount of time between when the complainant filed his or her complaint and when the subject-matter of the complaint arose (s. 13(2)(c)); and
- where the complaint is trivial, vexatious or made in bad faith (s. 13(2)(d)).

CASL repealed s. 13(2) and instead gave the Commissioner discretion at two points in the complaint-handling process to close a complaint. First, the Commissioner can decide not to investigate a complaint, essentially for the same reasons as existed under s. 13(2)(a) to (c) of *PIPEDA*.¹² In effect, the Commissioner's discretion has been moved up earlier in the complaint-handling process on the premise that, at least in some cases, the existence of one of the three situations in the former s. 13(2)(a) to (c) obviates the need for an investigation, let alone a report.

Second, the amendment provides that the Commissioner can decide to discontinue an investigation already underway. Her discretion may be exercised for essentially the same reasons formerly outlined in s. 13(2) for not issuing a report. However, her discretion is also broadened to include additional reasons such as where there is insufficient evidence to pursue the investigation, the organization has provided a fair and reasonable response, the matter is already the object of an ongoing investigation, and the matter has already been the subject of a report by the Commissioner.¹³

It should be noted that under amendments that have yet to be declared in force the Commissioner will also have the discretion not to conduct or to discontinue an investigation where the complaint relates to a contravention of a provision of CASL that is the responsibility of the Canadian Radio-television

and Telecommunications Commission ("CRTC") or of new prohibitions in the *Competition Act*, R.S.C. 1985, c. C-34, relating to false or misleading representations in electronic messages.¹⁴

In all cases the Commissioner is required to notify the complainant and the organization concerned and give reasons.¹⁵

The Commissioner may reconsider her decision not to investigate if the complainant provides a compelling reason to do so.¹⁶ There is no equivalent provision for reconsidering a decision to discontinue an ongoing investigation. However, in the case of a discontinued investigation, a complainant is entitled to apply to the Federal Court under s. 14 of the *Act* for relief.¹⁷

Having considered these new discretionary powers, it might be asked how a broader discretion to decline or discontinue investigations will improve service delivery to Canadians. After all, if these new powers are exercised the upshot will be that some complaints are not investigated.

However, this neglects the potential benefits of these new powers in terms of more effective complaint handling. As noted above, the amendments allow for discretionary powers that already existed to be exercised earlier in the complaint-handling process. As such, a complainant can now be informed earlier in the process that, for instance, there are other procedures that they should pursue first in order to resolve their complaint. Furthermore, while the Commissioner is given new grounds to discontinue an investigation, these are focused on making the best use of the OPC's resources and preventing the risk of recurring backlogs. For instance, if the organization has already adequately responded to the complainant or the Commissioner has already addressed the matter,

there may be little value in pursuing the investigation and producing a report, which are both time-consuming and resource-intensive activities. In other words, the new discretion should allow the OPC to focus its resources on those complaints which raise serious privacy issues meriting investigation and broader systemic issues of significant importance for all Canadians.¹⁸ If exercised properly, they have the potential to result in increased, not diminished, privacy protection for Canadians.

b. Cooperation and information sharing powers

As noted above, the Commissioner has also been granted the power to sign agreements or arrangements to cooperate and share information with provincial counterparts and foreign authorities.

The OPC already had the ability to coordinate activities with provincial privacy commissioners.¹⁹ However, this amendment extends this ability to foreign data protection authorities, and, importantly, allows the Commissioner to share information — including information that is considered confidential as a result of s. 20(1) of *PIPEDA* — with both provincial counterparts and foreign authorities.²⁰ The information can only be used for the purpose for which it was shared and it must be treated confidentially.²¹

The new powers to coordinate and share information are crucially important in light of the increasingly inter-connected world we live in. Privacy issues are extending beyond domestic borders. Foreign organizations based in other countries can have a significant impact on the privacy of Canadians, and Canadian organizations can have a similar impact on individuals in other countries. In addition, even where an organization operating in Canada is dealing with Canadians' personal infor-

mation, there may be international implications. For example, the collection by Google Street View cars of personal information from unsecured WiFi networks concerned a number of privacy regulators around the world.²²

In order to effectively address many complaints it will be necessary for the Commissioner to coordinate her investigations and to share information with her provincial counterparts and foreign authorities. This may involve conducting joint or parallel investigations, obtaining information from foreign authorities or sharing information with foreign authorities so that they may take on the matter. The new powers allow for this and, as such, they should enable the OPC to deal with complaints that involve cross-border data flows or have international implications in a more effective manner. They should also allow for greater consistency in standards and findings across jurisdictions, which can facilitate compliance, and provide a better way of tackling global challenges.

Phase 2:

Bill C-29 and data breach notification

Data breach notification refers to organizations proactively disclosing when there has been a breach affecting the security of the personal information held by the organization. The OPC, in consultation with provincial privacy commissioners and other stakeholders, have developed guidelines for when organizations should notify the relevant authorities and individuals in case of a data breach.²³ In practice, some businesses do notify affected individuals when a data breach has happened, but there are currently no legally binding standards as to when and how such notifications should occur.

Bill C-29, which died on the order paper when the most recent federal election was called, had as its purpose to implement many of the recommenda-

tions from the first Parliamentary review of the *Act* and would have, among other things, addressed the gap in legally binding standards. The Bill required an organization to report to the Commissioner regarding “any material breach of security safeguards involving personal information under its control.”²⁴ An organization was also required to notify an individual of a breach where the breach creates “a real risk of significant harm to the individual.”²⁵ Both reports to the Commissioner and notifications to individuals had to include prescribed information and be in a prescribed form.²⁶ An organization also had to notify another organization or government institution about the breach if the organization or institution could assist in mitigating the risk of harm from the breach.²⁷

These new requirements would have made the OPC more effective at addressing the important issue of how organizations protect the personal information under their care. One of the central principles of *PIPEDA* is, of course, that personal information must be protected by appropriate safeguards.²⁸ However, when a data breach occurs, the affected individuals may not be aware of it or the circumstances surrounding the breach. As such, they cannot take steps to mitigate any harm that might result or lodge a complaint with the OPC to have the safeguards improved. Similarly, it is difficult for the OPC to be aware of a data breach unless the organization makes a proactive disclosure. By requiring notification to the Commissioner, Bill C-29 would have allowed the OPC to ensure that steps were taken to correct or mitigate the damage and that organizations were held accountable for data breaches. The OPC would also have been able to verify that there were no systemic problems that require attention.

All of this would make the OPC more effective at addressing the issue of safeguards for personal information. While it is not clear whether a similar bill would be re-introduced after the election, breach notification is an important reform that should be implemented sooner rather than later.

Phase 3: The second Parliamentary review of PIPEDA

The amendments to *PIPEDA* in CASL and Bill C-29 discussed above arose from the first Parliamentary review of the *Act*. While Bill C-29 has died on the order paper, it is not too early to begin thinking about what further reforms are needed to make *PIPEDA* more effective as part of the second Parliamentary review.

To begin the discussion, the OPC commissioned Professor France Houle and Dean Lorne Sossin to conduct an analysis of the effectiveness of *PIPEDA*. Their report, which was recently posted on the OPC’s website, is a wide-ranging and detailed look at whether the ombudsman model is effective in regulating the personal information protection practices of the private sector.²⁹

Of note, Professor Houle and Dean Sossin found that the current ombudsman model has achieved mixed success. They noted that the current model will likely need to be strengthened in the future, particularly, in their view, for small and medium-sized enterprises. Specifically, they recommend that the Commissioner be given a limited and targeted order-making power, including the power to impose financial penalties. Based on the experience of provincial counterparts who already have an order-making power, they noted that even though such a power would not likely be used often, its presence alone would serve as a significant deterrent. The report also recommended that creative new regulatory strategies to increase accountability

— such as the development of a privacy certification programme — be explored.

In addition to the work by Professor Houle and Dean Sossin, the OPC has held consultations on two consumer privacy issues that have the potential to test the effectiveness of *PIPEDA* in the future, namely, online tracking, profiling and targeting, and cloud computing. The consultations were intended, in part, to inform the second Parliamentary review of *PIPEDA*. While participants were generally of the view that *PIPEDA* was capable of addressing online tracking, profiling and targeting and cloud computing, they did point to challenges these issues might create for *PIPEDA*. Among other things, participants highlighted the definition of personal information, consent, limiting use and retention of personal information, jurisdiction, safeguards and access as issues needing further exploration. A final report summarizing the results of the consultation was published last month.³⁰

This work is, of course, the beginning and not the end of the discussion. No doubt there will be many more opportunities for bringing forward ideas to make *PIPEDA* and the OPC more effective in the coming months.

Conclusion

The common theme of the legislative developments canvassed in this article is that they all have the potential to make the OPC more effective for Canadians. As the Commissioner looks forward to the next three years of her mandate and to focusing on the priorities she has identified, she can be hopeful that the amendments made by CASL, data breach notification and the potential changes resulting from the second Parliamentary review of *PIPEDA* will go some way towards meeting the goal of improved service delivery to Canadians.

¹ S.C. 2000, c. 5.

² See e.g. C. Berzins, "Complaining under *PIPEDA*: An Exercise in Futility" (2010) vol. 7, no. 9 Canadian Privacy Law Review 104.

³ Appearance before the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the 2009-2010 Annual Report to Parliament on the Nomination for Reappointment, December 2, 2010: <http://www.priv.gc.ca/parl/2010/parl_20101202_e.cfm>.

⁴ "Making Privacy Protection More Effective for Canadians", Remarks at the Centre for Law, Technology and Society of the University of Ottawa, Address by Jennifer Stoddart, Privacy Commissioner of Canada, January 19, 2011: <http://www.priv.gc.ca/speech/2011/sp-d_20110119_e.cfm>.

⁵ *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23. The legislation was enacted, somewhat inconveniently, without a short title. Although the legislation deals with more than just spam, referring to it as Canada's Anti-Spam Legislation at least provides the convenience of a workable shorthand.

⁶ Bill C-29, *Safeguarding Canadians' Personal Information Act*, 3rd Sess., 40th Parl., 2010 ("Bill C-29"). The bill died on the order paper when the most recent federal election was called.

⁷ For an overview see, A. Davies and T. Thomas, Library of Parliament, "Legislative Summary of Bill C-28:

An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities", May 28, 2010 revised February 4, 2011:

<<http://www2.parl.gc.ca/sites/lop/legisinfo/index.asp?Language=E&query=7019&Session=23&List=Is>>.

⁸ *PIPEDA*, *supra* note 1, ss. 12(1), 12.2(1), as amended by CASL, *supra* note 5, s. 83.

⁹ *PIPEDA*, *supra* note 1, ss. 23, 23.1, as amended by CASL, *supra* note 5, s. 87.

¹⁰ The amendments made to *PIPEDA* by CASL relating to the new discretionary powers and information sharing, with the exception of ss. 12(2) and 12.2(2), were brought into force on April 1, 2011: see S.I. 2011-0022. The amendments to *PIPEDA* relating specifically to the anti-spam regime as well as the other provisions of CASL are, however, not yet in force.

¹¹ *PIPEDA*, *supra* note 1, s. 12(1), as it read prior to being amended by CASL, *supra* note 5.

¹² *PIPEDA*, *supra* note 1, s. 12(1)(a) to (c), as amended by CASL, *supra* note 5, s. 83. Paragraphs 13(2)(a) and (b) are reproduced exactly, whereas s. 13(2)(c) is recast to put the focus on the reasonableness of the amount of time taken to file the complaint rather than on the usefulness of a report.

¹³ *PIPEDA*, *supra* note 1, s. 12.2(1)(a), (c) to (e), as amended by CASL, *supra* note 5, s. 83.

¹⁴ CASL, *supra* note 5, s. 83, which would amend ss. 12(2) and 12.2(2) of *PIPEDA*. While the remainder of s. 83 has been declared in force, these subsections have not been

since they are directly tied to the anti-spam regime: see S.I. 2011-0022.

- ¹⁵ *PIPEDA*, *supra* note 1, s. 12(3), as amended by CASL, *supra* note 5, s. 83.
- ¹⁶ *PIPEDA*, *supra* note 1, s. 12(4), as amended by CASL, *supra* note 5, s. 83.
- ¹⁷ *PIPEDA*, *supra* note 1, s. 14, as amended by CASL, *supra* note 5, s. 85.
- ¹⁸ See Statement by Elizabeth Denham, Assistant Privacy Commissioner of Canada, Appearance before the House of Commons Standing Committee on Industry, Science and Technology on Bill C-27, the *Electronic Commerce Protection Act*, June 18, 2009: <http://www.priv.gc.ca/parl/2009/parl_20090618_ed_e.cfm>.
- ¹⁹ *PIPEDA*, *supra* note 1, s. 23, as it read prior to being amended by CASL, *supra* note 5.
- ²⁰ There are also new information-sharing powers under CASL itself, which permit the Commissioner to share information with the CRTC, the Competition Bureau and with foreign authorities with respect to spam and related conduct (CASL, *supra*, note 5, ss. 58, 60.). Unlike the new information-sharing powers in *PIPEDA*, there is no express carve-out from s. 20(1) of *PIPEDA*, which requires the OPC to keep information confidential. However, in case of conflict, CASL is deemed to take precedence over *PIPEDA* (CASL, *supra* note 5, s. 2).
- ²¹ *PIPEDA*, *supra* note 1, ss. 23(4) and 23.1(3), as amended by CASL, *supra* note 5, s. 87.
- ²² See e.g. BBC News, "Privacy body to re-examine Google", October 24, 2010: <<http://www.bbc.co.uk/news/technology-11614970>>.
- ²³ See OPC, *Key Steps for Organizations in Responding to Privacy Breaches*: <http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.cfm>.
- ²⁴ Bill C-29, *Safeguarding Canadians' Personal Information Act*, cl. 11 (s. 10.1(1)).
- ²⁵ *Ibid.* cl. 11 (s. 10.2(1)).
- ²⁶ *Ibid.* cl. 11 (ss. 10.1(3) and 10.2(5),(6)).
- ²⁷ *Ibid.* cl. 11 (s. 10.3(1)).
- ²⁷ *PIPEDA*, *supra* note 1, Sch. 1, cl. 4.7.
- ²⁸ See F. Houle and L. Sossin, "Powers and Functions of the Ombudsman in the Personal Information Protection and Electronic Documents Act: An Effectiveness Study", August 2010: http://www.priv.gc.ca/information/pub/pipeda_h_s_e.cfm.
- ²⁹ The Commissioner herself has raised the possibility of increased enforcement powers in a recent speech: see "Making Privacy Protection More Effective for Canadians", Remarks at the Centre for Law, Technology and Society of the University of Ottawa, Address by Jennifer Stoddart, Privacy Commissioner of Canada, January 19, 2011: <http://www.priv.gc.ca/speech/2011/sp-d_20110119_e.cfm>.
- ³⁰ OPC, Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing: <http://www.priv.gc.ca/resource/consultations/report_2011_05_e.cfm>.

PRIVACY COMMISSIONER CAN NOW BE CHOOSIER ABOUT COMPLAINTS SHE INVESTIGATES



David Elder
Counsel
Stikeman Elliott LLP

Legislative amendments that came into force on April 1, 2011 mean that the Privacy Commissioner of Canada may now be more selective about the complaints her office decides to investigate.

The amendments in question, made to the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*], were actually contained in Bill C-28, Canada's Anti-Spam Legislation, which received Royal Assent last December. Although most of that statute is not yet in force (and may be delayed in coming into force by the federal election call and the appointment of a new Minister of Industry), by Order-in-Council P.C. 2011-479, dated March 25, 2011, the Governor in Council proclaimed in force some of the consequential amendments in that bill that affect *PIPEDA*, leaving for proclamation at a later date those *PIPEDA* amendments that coordinate with new obligations in the Anti-Spam law itself.

Previously, *PIPEDA* required the Privacy Commissioner to investigate all complaints submitted to her office, regardless of their nature or seriousness, although she had some discretion in not having to prepare a report in all cases.

With these new amendments, the Commissioner is no longer required in all circumstances to conduct an investigation in respect of a complaint received. Complaints need not be investigated if the complainant has not exhausted other grievance or re-

view procedures that may be available, if the complaint could be more appropriately dealt with under another Federal or Provincial law, or if the complaint was not filed within a reasonable time after subject matter of the complaint arose.

In all cases, complainants must be notified that their complaint will not be investigated. The Commissioner retains the right to reconsider a decision not to investigate a particular complaint, if the complainant is able to provide compelling reasons to investigate; however, the law provides no guidance as to what might be found to be compelling in such circumstances.

The new powers have long been sought by the Commissioner as a way to better manage the workload of the Office of the Privacy Commissioner, by weeding out complaints whose resolution would be of little public interest or significance, thereby allowing for the focus of resources on issues of a broader systemic nature. While the Privacy Commissioner seems to have addressed the significant backlog of complaints that once challenged the resources of her office, workload challenges remain as public awareness of privacy issues increases and privacy-impacting technologies are developed and implemented.

The authority to manage the processing of complaints in this way is already afforded to some degree to other tribunals, including the Canadian Human Rights Commission and the Information and Privacy Commissioner for Alberta.

Once the investigation of a complaint commences, the new amendments also give the Privacy Commissioner the power to discontinue investigation in certain circumstances. Investigations may be discontinued where:

- there is insufficient evidence to pursue the complaint;
- the complaint is trivial, frivolous or vexatious or is made in bad faith;
- the organization that was the subject of the complaint has provided a fair and reasonable response;
- the subject matter is already the subject of a report by the Commissioner;
- the complainant has not exhausted other grievance or review procedures that may be available;
- the complaint could be more appropriately dealt with under another Federal or Provincial law;
- the complaint was not filed within a reasonable time after subject matter of the complaint arose;
- the matter is being or has already been addressed via another grievance or review process, or pursuant to a procedure under another Canadian law;

As with a case of declining to investigate, the Commissioner must notify a complainant and organization of the discontinuance of a complaint, giving reasons for the discontinuance.

With other tribunals that have the power to decline to investigate complaints, there has understandably been a reluctance to exercise this authority, since doing so denies a complainant a full consideration on the merits of the complaint. As a result, the bar for refusing a complaint has tended to have been set fairly high, with complaints being declined or dis-

continued only in the clearest and most egregious of circumstances.

One suspects that this will also be the approach of the Privacy Commissioner; however, the new powers should nevertheless afford her office a great deal more control in managing its caseload, focusing strained resources on matters of the greatest public interest and systemic benefit.

WORKPLACE COMPUTER PORNOGRAPHY RULING: POLICE NEED SEARCH WARRANT; EMPLOYER HAS LATITUDE



Maria Giagilitsis
Associate
Fasken Martineau DuMoulin LLP



Brian P. Smeenk
Partner
Fasken Martineau DuMoulin LLP

In a decision released on March 22, 2011, the Ontario Court of Appeal issued a surprising ruling affecting privacy rights in the workplace. The case, *R. v. Cole*, [2011] O.J. No. 1213, involved criminal charges against a teacher involving possession of child pornography. The court said the employee has a reasonable expectation of privacy regarding the contents of his workplace computer. This meant that he was protected against computer searches by the police absent a search warrant. The employer was given more latitude, but not free reign. While this decision certainly muddies the waters, it may not be as damaging as first appears for employers' ability to control how their computer equipment is used.

Until now, the general rule was that personal information stored by employees on workplace computers would be treated as the employer's property,

with full access by the employer. Employers could clearly investigate suspected mis-use of equipment, and take action against employees who violated their policies. It was assumed that this might include handing over to the police material that might lead to criminal charges. But in this decision, the employee's reasonable expectation of privacy meant that prosecutors would be unable to use many of the images police obtained from the workplace computer, at the teacher's criminal trial. However, the Court said that different considerations apply to employers. This raises new questions about what employers can do to ensure their equipment is not mis-used by employees.

The Basic Facts

A Sudbury high school teacher was provided with a laptop by his school. He used the laptop to teach communication technology. He was also responsible for supervising a laptop program for students.

The teacher had the authority to remotely access data stored on the students' laptops. He did this regularly. While reviewing one student's computer files, he discovered nude photos of another student. The teacher copied the nude photos onto the hard drive of his (school-issued) laptop, rather than reporting the incident.

The school's computer technician discovered the nude photos in a "hidden" folder on the teacher's computer. He found them while doing a routine data scan. Upon identifying the girl as a student, the technician notified the principal. The principal instructed him to copy the images, along with the teacher's internet surfing history, onto a disc. That surfing history included a large number of pornographic sites. The employer gave that, along with the nude photos, to the police. The police viewed both the disc and the laptop without a warrant.

The teacher was charged with possession of child pornography and criminal use of computer systems. In court, the teacher's lawyer argued that the teacher had a reasonable expectation of privacy in the contents of his laptop. The issue was appealed to Ontario's highest court.

Interesting Twists

The Court of Appeal emphasized that the teacher had exclusive use of the laptop and that the laptop was protected by a personal password. The Court also noted that teachers were generally permitted personal use of school computers.

But the evidence also was that the school's Policy and Procedures Manual prohibited having sexually explicit content on school computers. The Manual also said that all data and messages are considered the property of the school board. The Manual further advised teachers that the school would access private emails if inappropriate use is suspected. And users were advised that they should not assume that files stored on the network or harddrives were private.

The Court of Appeal Decision

The Court found that the teacher did have a reasonable expectation of privacy in the contents of his laptop, at least vis-a-vis the police. The police therefore violated the teacher's right against unreasonable search and seizure under the *Charter of Rights and Freedoms* when they seized the laptop and searched it without a warrant.

The Court looked beyond the strict wording of the school's computer use policies. It focused instead on the actual practice and customs of the workplace. While the policy was that computers were meant to be used for business purposes, staff routinely used computers to store intimately personal information, such as financial and banking data. All

the circumstances satisfied the Court that the teacher had a reasonable expectation of privacy in the contents of his laptop. This gave him protection against police seizures and searches.

The Court, however, gave the employer more leeway than it gave the police. Although the Court assumed that the *Charter* could apply to the school board [note that this is contentious — the *Charter* does not apply to most employers], it found that the employer did not violate the teacher's *Charter* rights. The employer did not act improperly when it accessed the teacher's laptop and copied the photos to disc. The employer found these photos while performing normal computer maintenance — an activity that the Court acknowledged was within the employer's right to carry out on its own equipment.

Similarly, the teacher's principal acted properly in viewing some of the images found by the technician, directing him to copy the photographs onto a disc, and requiring the teacher to hand over the laptop. Even though this was a "search and seizure", it was consistent with the principal's duty to ensure the health and safety of students. The principal could not be held to the same standard as the police.

As for the employer itself, the school board, it did not violate the teacher's *Charter* rights either. This, even though it searched the laptop and secured further evidence regarding the teacher's computer and internet use before handing it over to the police. The search and the preservation of evidence for internal discipline procedure were in accordance with the employer's obligation to ensure a safe and secure environment for its students.

Quick Assessment

This case will be analyzed and commented upon by many. An early assessment is that it may not be as bad for employers as first appears.

First, it must be emphasized that the expectation of privacy only operated against the police's search and seizure in this case. Secondly, note that this decision was based on *Charter* rights. Those rights do not apply to most employment relationships. Certainly not those in the private sector.

One might argue that the Court's decision places individual privacy rights over other rights. This might be true with respect to police searches and seizures. However, the decision supports employers who maintain well-drafted policies that make it clear the employee has no privacy rights on the employer's computers. It also favours employers who actively maintain, monitor and enforce their own computer use policies.

The decision acknowledges that employers may access data stored by employees on workplace

computers in appropriate circumstances. It also acknowledges that such data can be used in internal investigations and later disciplinary proceedings. This is clearly the case with respect to situations that are found as a result of regular monitoring and maintenance.

The decision highlights the importance of well-written computer use policies. It also highlights the importance of ensuring that workplace practices are consistent with those policies.

[*Editor's note:* This article was re-published with the permission of the law firm *Fasken Martineau DuMoulin, LLP*, as well as the publishers of *Northern Exposure*, a blog written by the law firm's lawyers. *Northern Exposure* is produced in conjunction with *HRHero.com*. You can read more *Northern Exposure* blog posts at <http://blogs.hrhero.com/northernexposure>.]

ELECTRONIC VERSION AVAILABLE

A PDF version of your print subscription is available for an additional charge.

**A PDF file of each issue will be e-mailed directly to you 12 times per year,
for internal distribution only.**

INVITATION TO OUR READERS

**Do you have an article that you think would be appropriate for
Canadian Privacy Law Review and that you would like to submit?**

AND/OR

**Do you have any suggestions for topics you would like to see featured in future issues of
Canadian Privacy Law Review?**

If so, please feel free to contact Michael A. Geist

@mgeist@uottawa.ca

OR

cplr@lexisnexis.ca