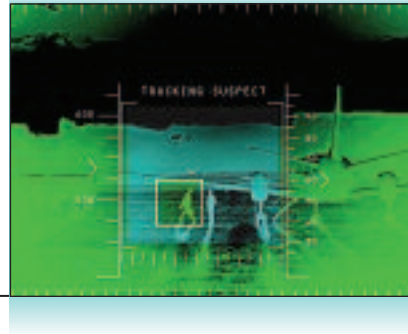


Privacy of Personal Information in Canada

By Ian Turnbull, Canadian Privacy Institute



On January 1, 2004, Canada's Federal privacy law – The Personal Information Protection and Electronic Documents Act (PIPEDA) – took general effect across the country. At the same time, the provinces of Alberta and British Columbia each introduced a Personal Information Protection Act (PIPA-Alberta and PIPA-BC, respectively), joining Quebec – which has had a similar law for many years.

These three provincial laws have all been declared as “substantially similar” to the federal legislation – that means that they take precedence over the federal law except in matters of moving personal information (PI) across provincial or federal borders for purposes of commercial activity.

OTHER DRIVERS

The U.S. Patriot Act has raised serious concerns in Canada about the intrusive nature of the Act and its use/misuse. The Province of British Columbia, in particular, is so concerned that a new law has been passed to prohibit government outsourcing to companies that are based in or operate in the U.S.

Interested in the BC privacy commissioner's report on this subject? Take a look at: http://www.oipcbc.org/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf.

The large number of companies operating in both Canada and the United States has meant that Sarbanes-Oxley (SOX) compliance reporting has become omni-present, overshadowing privacy and most other issues as administrators pull together their information.

Meanwhile almost everyone with

Internet access is painfully aware of the growing problem of spam. The failure of the U.S. CAN-SPAM Act demonstrates the international nature of the problem, and the impossibility of any one country solving it alone.

Canada is to investigate reports of serious privacy concerns posed by Google's proposed G-mail service.

All of these issues, plus continued privacy disasters, such as the Canadian Imperial Bank of Commerce (CIBC) faxing thousands of customers financial records to a West Virginia scrap yard (for over three years, despite being made aware of the problem immediately after it began – see box on right).

PRIVACY MOMENTUM SLOWS

It was generally expected that the increasing visibility of workplace-based identity theft, the growing media awareness of the issues around privacy, and the impact of the enactment of this volume of legislation, would collectively focus on the importance of the protection of PI.

This has not been the case. Since the appointment of Canadian Privacy Commissioner Stoddard, the federal office has faded from the limelight, emphasizing the ombuds-role and strongly de-emphasizing the role of privacy advocate.

Some would say that this is a positive step given former Commissioner Radwanski's difficulties with the press, but the lack of public pronouncements regarding the issues of the day has left the ship of Canadian privacy adrift.

Most distressing, extreme privacy

breaches – such as the CIBC example, have not been positive steps.

And finally, 14 European countries have been joined by Australia and actively pursued, at least not in the media, in order to raise the public's awareness level. But the awareness of the privacy commissioners across the country seems to be changing. David Loukidelis, Information and Privacy Commissioner for British Columbia in

CLASS ACTION SUIT

February 24, 2005

The Girard Law Office stating that it would be filing a class action suit against the CIBC.

The action is a result of the Bank (CIBC) faxing confidential client information RRSP investor information, names, addresses, telephone and SIN numbers as well as bank account and transit numbers, and signatures.

The CIBC was advised and aware of the situation in 2002 but continued to use an unsecured fax line and send information to the number.

The Privacy Commissioner of Canada began her investigation of the privacy breach in November 2004.

The claim seeks damages of \$9,000,000.

See details at: http://www.ctv.ca/servlet/ArticleNews/story/CTVnews/1101436308027_38

his summary report, on the Patriot Act states that:

Advanced technologies have created the ability to merge isolated databases into massive banks of information about individuals. This, in turn, enables data mining — the application of database technology and techniques to uncover patterns and relationships in data and to undertake the prediction of future results or behavior. The hidden patterns and subtle relationships that data mining detects are recorded and become personal information about the individual whose characteristics or habits are being searched and analyzed. A recent audit by the U.S. Government Accountability Office has studied the extent of data mining by U.S. federal agencies. It confirmed that this practice is increasingly common and that many of the data mining efforts involve the use of personal information. The extent of data mining by governments in Canada has not been the subject of sufficient or transparent study and documentation and, in our view, since the privacy implications of data mining can be significant, this needs to be remedied.¹

Loukidelis goes on to summarize four effects that may well express today's privacy challenge in Canada and around the world:

1. *As society cannot predict with accuracy where technology will take data management in the future, it needs to institute sufficient legal privacy protections today so that public policy will guide technology, not the reverse.*

2. *Once personal information crosses borders, regulating its use is at best difficult and at worst impossible.*

3. *Increasing private and public sector reliance on digitally stored, analyzed, and accessed personal information increases the risk that inaccurate or limited snapshots of an individual will be misused, whether intentionally or not.*

4. *The distinction between business and state uses of personal information is becoming blurred and will increase the risks to privacy and to other individual rights and interests.²*

PROVINCIAL LAW

Canadian provincial laws are important because the employee/employer relationship (and the privacy protection of the employee's

personal information) is a provincial responsibility.

But the detail of which privacy commissioner is responsible to investigate which complaint is murky. For example, if the PI of a resident of BC is disclosed by the Alberta arm of a company based in Nova Scotia, which privacy commissioner has authority? As the BC Commissioner expressed (above): *once PI crosses a border, regulating its use is at best difficult and at worst impossible.*

Meanwhile, Canada's largest province – Ontario – expects to introduce its own Personal Information Protection Act by the end of 2007. Until that time, there is no law in Ontario (or in any of the other six provinces without a specific PIPA) that specifically covers PI generated by the employee/employer relationship. That is, the absence of provincial legislation does not mean that the federal legislation applies – again, unless a border is crossed.

HEALTH PRIVACY

But, Ontario does have some targeted privacy law. In November 2004, it passed the Personal Health Information Protection Act (2003) (P-HIPA, pronounced FIPA). It is focused on personal health information (PHI) and PI – as they relate to health care. Observers believe that this Act will serve as the basis for similar legislation in all provinces. P-HIPA is largely silent on the way in which health care providers (and patients) from outside of Ontario will be impacted by this legislation. This has triggered a Canada-wide inter-provincial committee that will make recommendations on how inter-provincial (and international) health care will be managed with respect to PHI and PI.

Although P-HIPA impacts employers with respect to health and benefit plans, employee assistance programs (EAP), and health management within companies, it largely ignores the role (and surrounding rules) of the employer and its commercial partners (benefits administration companies, insurers, etc.).

E-MAIL = PI?

One of the most recent decisions from the federal privacy commissioner has left observers scratching their heads. PIPEDA provides that business contact information is *not* PI.

Although the "EDA" in PIPEDA stands for Electronic Documents Act, the list of business contact information (name, title, business address, and phone) does not include e-mail. Most people assumed that this was an oversight and have been defining business contact information as that normally found on a business card, including e-mail and FAX.

Not so says the Federal Commissioners office: "As a business e-mail address is not specified in section 2 (of PIPEDA), we must conclude that it (e-mail address) is an individual's personal information for the purposes of the Act."³

The reasoning seems to be that you are allowed to collect and use publicly available information, but the use has to be directly related to the purpose for which the information appears in a directory or notice. The expectation is that any contact would have the intention of furthering the organization's interests.

For example, it could be argued that a law book publisher would have a good case for contacting a university law professor about a new publication or a pharmaceutical company might be able to e-mail doctors about a newly developed drug.

This decision will almost certainly be addressed when PIPEDA comes up for review in 2006, but in the meantime e-mail = PI and as such, organizations using mail for commercial purposes will have to get the individual's consent. Although this case did not deal with facsimile numbers, the issue is the same. A FAX number is also not specified in PIPEDA, so logic dictates that it too is not business contact information but is PI that must be protected.

LANGUAGE

A similar surprising view has been expressed by the Office of the Privacy Commissioner regarding language. Canadian government processes nor-

mally provide that either English or French can be used (and other languages are becoming increasingly common as governments reach out to communicate to various minority groups). But since PIPEDA is silent on the subject, the Commissioner's view is that there is no requirement to communicate in the preferred language of the complainant (except in Quebec where language – usually French – is mandated provincially).

HOME TELEPHONE NUMBER

In one of the first court decisions centered on PIPEDA, the Federal Court of Canada has upheld a complaint regarding publishing home phone numbers. The court confirms that telephone companies must advise new customers that their name and number will be placed in a public directory and that there is an opportunity to ask that your home phone number remain unpublished. However, the Court also found that the phone company (Telus) could charge a fee for not publishing the information.⁴

SUMMARY

The Federal Commissioner's strategy of playing the role of privacy ombudsman, instead of being an advocate, has reduced the sense of urgency that had pervaded the business community when PIPEDA was first introduced.

PIPEDA was in force for "federal works" beginning in 2001. The volume of decisions since January 2004 when the legislation came into force for all organizations is not reflective of the increased scope of the legislation. This is not surprising since the office of the Commissioner has not grown in size, and one suspects that the office is experiencing major shock with respect to the volume of complaints.

The 2006 legislative review will hopefully clarify and then resolve many of the uncertainties around PIPEDA, while the anticipated Ontario legislation will significantly intensify the privacy focus across the country. And the ongoing security-privacy push-pull around the world will continue to apply pressures to modify and clarify the Canadian approach to privacy.

ENDNOTES

1 Gathered from http://www.oipcbc.org/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf summarizing Privacy and the USA Patriot Act Implications for British Columbia Public Sector Outsourcing that was published in October 2004.

2 Office of the Privacy Commissioner of Canada, ref: 61 00-00780

3 Dan Palavew, "Privacy chief takes aim at spammers with e-mail ruling", *Ottawa Business Journal* Staff

4 05-02-03 gathered from: <http://recueil.cmf.gc.ca/fc/src/shtml/2003/fic/v4/2003fc32864.shtml>

*Ian Turnbull is executive director of The Canadian Privacy Institute, an organization that consults about and provides information regarding privacy in Canada. He is the author of *Privacy In The Workplace – The Employment Perspective* (see: www.canadianprivacyinstitute.ca). Mr. Turnbull is a board member of the IHRIM Privacy SIG, and former chair of the IHRIM board. He can be reached at iturnbull@canadianprivacyinstitute.ca.*

IHRIM Makes House Calls!

You can bring any of IHRIM's exceptional educational courses to your company. IHRIM in-house courses present your employees with the same high quality learning experience offered at our public seminars, without the expense or inconvenience of travel. In-house courses provide a cost-effective solution to employee professional development, and each course can be tailored to fit the needs of your organization.

Choose from any of these educational offerings:

- Introduction to HR Systems Course
- Managing HRMS: Post-Implementation Issues
- Essentials for Successful Project Management
- HR Performance Measurement: Measuring the Effectiveness of the HR Function
- Managing Privacy Challenges in the Use of Employee Information
- Change Management for HRMS Projects
- Successful HR Systems Selection
- How to Build a Compelling Business Case to justify Your HRIT Initiative
- HR Outsourcing: Risks & Opportunities for Internal HR Functions
- HR Metrics for Business Partners



Learning has no limits.



IHRIM is pleased to announce that many of our courses have been approved for recertification credit hours toward PHR and SPHR recertification through the Human Resource Certification Institute (HRCI).

For more information on IHRIM educational courses visit www.ihrim.org or email moreinfo@ihrim.org to schedule your in-house course today.