CANADIAN PRIVACY LAW REVIEW

Volume 1 • Number 1 October 2003

## In This Issue:





# EDITOR'S NOTE

**Professor Michael A. Geist**

Editor-in-Chief of the *Canadian Privacy Law Review.* Professor Geist is Canada Research Chair in Internet and E-Commerce Law at the University of Ottawa and Technology Counsel at Osler, Hoskin & Harcourt LLP.

*Welcome to the inaugural issue of the* Canadian Privacy Law Review. *Privacy law and compliance has emerged as a critical issue for businesses and individuals alike. Businesses of all sizes are struggling to grapple with an uncertain legal framework at both the federal and provincial levels, while individuals have begun to test the limits of their newly established statutory privacy rights. The headlines in Canada in recent months have trumpeted controversy at the Office of the Federal Privacy Commissioner; however, less attention has been accorded to provincial implementations of private sector privacy legislation, challenges to the* Personal Information Protection and Electronic Documents Act *(PIPEDA) in federal court, and the raft of Privacy Commissioner findings on PIPEDA complaints.*

*The* Canadian Privacy Law Review *will fill that information gap by providing subscribers with a monthly look at the latest developments in the Canadian and international privacy scene. Each issue will include analysis of emerging issues, summaries of recent PIPEDA findings from the privacy team at Osler, Hoskin & Harcourt LLP, and updates on privacy law concerns from leading practitioners from around the globe. Guiding the newsletter is a stellar collection of leading privacy authorities including current and former privacy commissioners as well as representatives from private practice, industry, and academia.*

*We begin this month with the front burner issue for the fall of 2003 — Patricia Wilson of Osler, Hoskin & Harcourt examines the jurisdictional questions surrounding PIPEDA and the implementation of provincial privacy statutes in B.C. and Alberta. The monthly PIPEDA update highlights several notable findings, including analysis of the status of web site cookies and magazine lists. Christopher Kuner of the Brussels office of Hunton & Williams, an advisory board member and European privacy law correspondent, provides an update on recent developments in the E.U., while Duncan Giles of Freehills in Australia calls attention to a recent case of note from down under.*

*With a monthly print schedule, we plan to make this newsletter a "must read" for those in need of timely, relevant information on privacy law. I hope you enjoy this issue and welcome your comments and suggestions at <mgeist@uottawa.ca>.*

## Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 75 Clegg Rd., Markham, Ont., L6G 1A1, and is available by subscription only.

Web site: www.lexisnexis.ca




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

**ISBN 0-433-44418-5** (print & PDF)
**ISSN 1708-5454**

Subscription rates: $175.00 plus GST (print only)
$274.00 plus GST (print & PDF)



# THE "SUBSTANTIALLY SIMILAR" DEBATE

*The "substantially similar" declaration and exemption from PIPEDA by the federal Cabinet is intended to create consistent national privacy protection standards that apply within, as well as between and beyond Canadian provinces and territories, and represents a novel approach to national standard-setting by the federal government...*

**Patricia Wilson**

Ms. Wilson is a partner in the Litigation Department of Osler, Hoskin & Harcourt LLP specializing in privacy and information law.

## Watchpoints for Fall 2003 — The "Substantially Similar" Debate

### The Issue

Many privacy agendas in the fall of 2003 will focus on the question of whether private sector privacy legislation introduced in British Columbia (B.C.) and Alberta will be declared by Canada's federal government to be "substantially similar" to the federal privacy legislation, the *Personal Information Protection and Electronics Document Act* (or PIPEDA), by January 1, 2004, the date that PIPEDA will otherwise apply to all commercial activity involving the collection, use or disclosure of personal information within Canadian provinces.[1] PIPEDA already applies to the collection, use and disclosure of personal information about the customers and other individuals, as well as the employees of federal works, undertakings and businesses, and to the disclosure of personal information across the provincial border "for consideration", *i.e.*, as part of a commercial exchange.[2]

The "substantially similar" declaration and exemption from PIPEDA by the federal Cabinet is intended to create consistent national privacy protection standards that apply within, as well as between and beyond Canadian provinces and territories, and represents a novel approach to national standard-setting by the federal government given the extension of the federal standard to businesses and organizations typically subject to provincial jurisdiction.

So far, the federal government has indicated that Québec's 1994 privacy legislation, *An Act Respecting the Protection of Personal Information in the Private Sector*, will be declared as substantially similar to PIPEDA so that the Québec legislation, rather than

PIPEDA, will apply to businesses operating within that province.[3] PIPEDA will continue to apply within Québec and in all provinces in areas of federal jurisdiction where it already applies, as well as in relation to the commercial collection, use and disclosure of personal information between, among or outside provinces or territories.

Meanwhile B.C. and Alberta have introduced virtually identical privacy laws that differ from PIPEDA in some respects.[4] These differences in turn led the former federal Privacy Commissioner to warn that he would not consider the B.C. and Alberta legislation to be "substantially similar" if enacted in their current form. Although the B.C. and Alberta bills are still before the legislatures in those provinces and remain unenacted, the former Commissioner used the report the Commissioner is required to make to Parliament each year on the extent to which provinces have enacted substantially similar legislation in order to identify the following "grave deficiencies" in the legislation as assessed against the PIPEDA standard:[5]

- provisions that grandfather personal information collected before the privacy laws are enacted;
- the absence of requirements for express consent from individuals and the emphasis on opt out forms of consent;
- the exemptions from the consent requirement for employee information and for information relevant to private investigations;
- the protection of the identity of third parties who provide information about individuals from disclosure to the individual concerned; and
- the regulation-making authority in the Alberta legislation.

## The Role of the Federal Privacy Commissioner

The standard set by the Privacy Commissioner in assessing provincial privacy legislation against PIPEDA is that the provincial legislation must be "as good or better than PIPEDA" in terms of the nature and degree of privacy protection it offers in order to be declared substantially similar. Although the federal Privacy Commissioner has identified some real differences between the B.C. and Alberta legislation and PIPEDA regarding the consent mechanisms in the legislation, there is debate on the merits of certain of the Privacy Commissioner's concerns about the B.C. and Alberta legislation, in particular those relating to employee information, which is an area where PIPEDA would not apply in any event. As well, there are questions regarding the standard the Commissioner has adopted that requires provincial legislation to be "at least as good or better" than PIPEDA.

In the criteria published by the Minister of Industry outlining the factors to be taken into consideration by the government in determining whether provincial legislation is substantially similar,[6] the Minister indicated that the Commissioner's views on provincial legislation would be sought and considered by the Minister in formulating the Minister's recommendation to Cabinet, and would be considered by Cabinet as well. This likely means that the views of the current Privacy Commissioner will also be sought by the Industry Minister when the B.C. and Alberta legislation are indeed enacted. Although the Commissioner's views will be considered, it is important to note that they do not bind the Minister or the Cabinet in the ultimate assessment of whether provincial legislation will be declared substantially similar and therefore whether a province will be exempt from the application of PIPEDA.

## The Industry Minister's "Substantially Similar" Criteria and Decision Process

The Minister of Industry has enumerated three general criteria that will be applied by the federal government to determine if provincial legislation is substantially similar. These require provincial legislation to:

- reflect the ten principles of fair information practices set out in the Canadian Standards Association Model Code (CSA Model Code) on the Protection of Personal Information (Schedule 1 of PIPEDA), with special emphasis on the consent, access and correction rights principles;
- provide for an independent and effective oversight and redress mechanism with powers to investigate; and
- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate, reflecting a similar requirement in s. 5(3) of PIPEDA.

These criteria are more general and, arguably, not the same as the Privacy Commissioner's stated criteria of "as good or better" than PIPEDA. The Minister's criteria require provincial legislation to "incorporate" the ten principles of the CSA Model Code on the Protection of Personal Information, by ensuring that all ten principles are "represented", as opposed to enumerated, in the legislation. The Privacy Commissioner's "equal or better" standard does not leave the same room for consideration of differences under the "substantially similar" rubric. As discussions between Industry Canada, the Privacy Commissioner's Office and provincial legislators continue during the fall, it will be interesting to see how Industry Canada applies these criteria in comparison to the test set by the former Privacy Commissioner.

A practical consideration that will affect the timing of a decision by the federal government is the fact that the Alberta and British Columbia legislation, at this point, remain unenacted, which means that the federal government cannot begin the process of making a decision to exempt the province from the application of PIPEDA until the legislation is passed.[7] In addition, the Minister of Industry must publish any requests for an exemption from PIPEDA by a province in the *Canada Gazette* and provide a period of public comment, likely in this case to be 30 days. Those comments will be considered in the preparation of the Industry Minister's recommendation to the Governor-in-Council. Following preparation of the Minister's recommendation, time for the consideration by Cabinet and publication of an Order in the *Canada Gazette* must be scheduled. All of this needs to take place before December 31, 2003 in order to clarify whether or not businesses or other organizations operating in B.C. and Alberta are to comply with the provincial or the federal legislation. Privacy buffs will therefore be watching the federal-provincial discussions with great interest as December 2003 approaches.

## What Happens if the Federal Government Does or Does Not Exempt a Province from the Application of PIPEDA?

Constitutional gymnastics are needed to answer this question, and there is considerable debate, even amongst the country's Privacy Commissioners, on this issue. These factors aside, the following is a schematic attempt at describing how federal and provincial privacy regimes would apply after January 1, 2004.

If the federal government does declare provincial privacy legislation to be "substantially similar" to PIPEDA:

- PIPEDA will continue to apply where it now applies, to federal works, undertakings or businesses with respect to customers and others and with respect to employees;
- provincial legislation will apply to organizations in the province that are not covered by PIPEDA in respect of customers and others, and in respect of employees of the organization;
- PIPEDA will apply to the interprovincial collection, use and disclosure of personal information in the course of commercial activities;
- provincial legislation may also apply to interprovincial collection and disclosure taking place in the province (B.C.'s legislation does say that it will not apply if PIPEDA applies, but the Alberta legislation does not contain a similar provision. The Québec and Alberta Commissioners have stated publicly that they would assert jurisdiction in such situations); and
- use of personal information within the province will be covered by provincial legislation.

If the federal government does not declare provincial legislation to be substantially similar to PIPEDA:

- PIPEDA will continue to apply where it now applies (see above);
- PIPEDA will also apply to collection, use and disclosure of personal information about customers and others in the course of commercial activity within the province;
- PIPEDA will not apply to employers in relation to their employees unless the employer is a federal work or undertaking;
- provincial legislation will apply to employers with respect to employees except for federal works or undertakings;
- Alberta legislation will also apply within the province to the extent of its terms; and

- the B.C. legislation currently states that it will not apply where PIPEDA applies.

Businesses with operations in B.C. and Alberta should be in a position to make a realistic assessment of whether PIPEDA or provincial privacy legislation will apply to them in these provinces sooner, rather than later, this fall. As businesses prefer a more or less consistent set of privacy protection standards across the jurisdictions in which they operate, with no one jurisdiction imposing significantly higher or more difficult standards than the rest, a sensible approach for many organizations will be to choose a privacy standard likely to comply in most jurisdictions, with the prospect of adjustments in various provincial jurisdictions being minor or minimized. The closer time draws towards January 1, 2004, the more likely it is that the PIPEDA standard, based on the CSA Model Code, will be chosen by organizations implementing privacy compliance across their Canadian operations.

---

1 PIPEDA, S.C. 2000, c. 5, s. 30(2) and s. 26(2)(*b*).

2 It is important to note that PIPEDA will **not** apply to organizations with respect to their employees unless the organization is a federal work, undertaking or business (such as banks, telecommunications carriers, radio or television broadcasters, interprovincial transportation companies and, although there is room for debate on this issue, ISPs). Employee privacy in non-federal sectors and industries will be subject to provincial privacy legislation where so enacted.

3 See Privacy Commissioner of Canada, Report to Parliament on Substantially Similar Legislation, May 2002.

4 *Personal Information Protection Act*, Bill 38, April 30, 2003 (British Columbia).

5 Privacy Commissioner of Canada, Report to Parliament on Substantially Similar Legislation, June 2003.

6 *Canada Gazette, Part I*, Saturday, September 22, 2001, p. 3618.

7 PIPEDA, s. 26(2)(*b*) requires the Governor-in-Council to be satisfied that "...legislation of a province that is substantially similar to this Part *applies* to … organizations" within the province, meaning that enacted bills cannot be considered.

# INTERNATIONAL DEVELOPMENTS

*The Treaty, if adopted, will give binding legal status to the Charter of Fundamental Rights of the Union, which recognizes the right to data protection as a fundamental right.*

**Christopher Kuner**

Mr. Kuner is a Partner in the Brussels office of the international law firm Hunton & Williams.

## European Data Protection Developments

### Right to Data Protection Anchored in Draft Treaty Establishing a Constitution for Europe

On June 20, 2003, the project drafting a new constitution for Europe (the so-called "Convention") submitted its draft of a "Treaty Establishing a Constitution for Europe" to the European Council. The Treaty, if adopted, will give binding legal status to the Charter of Fundamental Rights of the Union, which recognizes the right to data protection as a fundamental right. For further information, visit the Convention's web site: <http://european-convention.eu.int/bienvenue.asp?lang=EN&Content>=>.

### Controversy Surrounding Transfer of Airline Passenger Data to US Heats Up

While US government officials are still negotiating with their European counterparts over the transmission of transatlantic flight passenger information from Europe to US law enforcement authorities, the Amadeus computer reservation system has recently confirmed that 40 data fields of passenger information are currently being transferred to US authorities (see news report in German at: <http://futurezone.orf.at/futurezone.orf?read=detail&id=168229>).

On July 9, 2003, a hearing was held by the European Parliament (EP) Committee on Citizens' Rights, Justice and Home Affairs, at which the airline passenger data issue was discussed. At the hearing, various Members of the EP criticized the European Commission for allowing the transfers to go ahead in contravention of European law, and threatened to sue the Commission under Article 232 of the Treaty of Amsterdam if a legally-binding agreement with the US government to ensure that the data is subject to an adequate level of data protection is not reached by September (agenda of the meeting is available at: <http://www.europarl.eu.int/meetdocs/committees/libe/20030709/486237en.pdf>).

### Commission Finds Argentina to Have an Adequate Level of Data Protection

On June 30, 2003, the EU Commission recognized the adequacy of Argentina's data protection regime. As a result personal data may now flow freely between Argentina and the EU member states in compliance with the Directive's requirements. Commission Decision C(2003) 1731 can be downloaded from DG Internal Market web site: <http://www.europa.eu.int/comm/internal_market/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf>.

### EU Citizens are Still Denied Access to Documents

Earlier this year, the Council of the European Union and the European Commission released their first annual reports on public access to documents. Both reports reveal that many legal requirements, as prescribed by Regulation 1049/2001, are not met, in particular: (1) the obligation for each institution to keep a public register of documents and to update it; and (2) to give EU citizens access to such register. On June 12, 2003, a public hearing on access to documents was held at the European Parliament, at which speakers were highly critical of the lack of transparency of EU institutions. The Commission's report of April 29, 2003 is available at: <http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0216en01.pdf>.

### CEN/ISSS Data Protection Standardization Initiative Moves Forward

At a meeting held in Brussels on July 3, 2003, the decision was taken to proceed with work on the ISSS data protection standardization work under the umbrella of the European standardization body CEN. While many prominent IT companies did not attend the meeting out of protest, a majority of those present supported going ahead with the work in some form. Diana Alonso Blas of the European Commission indicated that if industry is not able to agree on voluntary data protection standards to help increase the level of compliance in Europe within the next few years, the Commission might have to propose a legislative instrument to do so during its next review of the Data Protection Directive 95/46/EC in 2005. Among the areas being considered for work are the development of a standard data processing contract ("Article 17 contract"), and a set of "common European voluntary best practices for data protection". More information on the meeting is available at <http://www.cenorm.be/isss/Workshop/DPP/default.htm>.

### Belgium: Data Protection Authorities Publish Results of Spam Consultation

In October 2002, the Belgian Data Protection Authority opened a "spam box", to which Internet users were invited to redirect all unsolicited commercial messages they received. The objective of this anti-spam campaign was to get a clear view of the phenomenon in Belgium. On July 7, 2003, the Commission published the results on its web site — see <http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf>. The study revealed that: (1) over 50,000 unsolicited commercial messages reached the spam box in two and a half months; (2) most of them originated from the USA, and to a lesser extent from Canada, while only 2.8 per cent were sent from within Belgium; (3) spam messages can be classified in four categories according to contents (financial offers, health products, pornographic messages and offers for miscellaneous electronic products). The Commission outlines the measures taken to fight spamming in Belgium, in France, and the US. It also published a guidebook on the rights and obligations of Internet users sending and receiving spam.

### France: the CNIL Takes Position on the Use of Credit Card Data

On June 26, 2003, the French Data Protection Authority (CNIL) published a recommendation on the storage and use of credit card numbers collected in connection with the distance purchase of products or services. The purpose is to remind businesses about their obligations when processing credit card data. It follows an online consultation conducted by the CNIL. In particular, the CNIL makes the following points: (1) credit cards, which are meant primarily as means of payment, are now used for identification and fighting fraud; (2) data subjects are seldom aware of such practice; (3) use of a credit card number for identification purposes or retention beyond completion of a transaction require the data subject's consent; and (4) the processor of such sensitive data must apply all appropriate protective measures.

The recommendation is available at: <http://www.cnil.fr/frame.htm?http://www.cnil.fr/textes/recomand/d03-

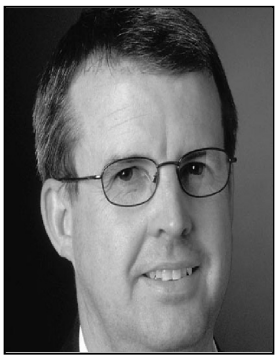
034.htm>, and an analysis at: <http://www.cnil.fr/thematic/banque/index.htm>.

### German Government Comments on TCPA

On March 17, 2003, the Christian Democratic (opposition) fraction of the German Parliament (Bundestag) asked the German government to comment on the competition, copyright, and data protection aspects of the "Trusted Computing Platform" currently being developed by Microsoft, IBM, Intel, Compaq, HP, and other companies. On April 7, 2003, the government responded, stating that 1) the government has established a task force of technical experts to study the initiative, 2) the government shares many of the concerns expressed about the data protection implications of the initiative, but that 3) it is currently too soon to reach any conclusions. The questions are available at <http://dip.bundestag.de/btd/15/006/1500660.pdf>, and the government's responses at <http://dip.bundestag.de/btd/15/007/1500795.pdf> (both in German only). See <https://www.trustedcomputinggroup.org/home> for more information on the TCPA.

### Italian Government Approves New Data Processing Code

On June 27, 2003, the Italian government approved a new "privacy code" that unifies the requirements of the Italian *Data Protection Act*, the new EU Directive on Privacy and Electronic Communications 2002/58, certain legislative decrees, and various sectoral codes of conduct already approved by the Italian Data Protection Authority (the Garante). In particular, the code contains simplifications of notifying data processing to the Garante; new rules on the use of consent; modifications of informational requirements in certain sectors; new rules covering the processing of medical, employee, telecommunications, judicial, and electoral data; and confirms the application of the Garante's sectoral codes in the areas of Internet, video surveillance, and direct marketing. More information is available in the Garante's newsletter of June 23-July 6, at <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Newsletter%2F2003>; the text of the code is available at <http://www.infogiur.com/news/privacy_tu_dlgs.asp> (all materials only in Italian).



**Duncan Giles**

Mr. Giles is Special Counsel with the law firm Freehills in Sydney.

*Editor's note: Gayle Hill is co-author of this article. Ms. Hill is Special Counsel at the law firm Freehills in Melbourne.*

## New Australian Right to Protection from 'Highly Offensive' Invasions of Privacy

In a very significant shift in Australian privacy law, the Queensland District Court has recently[1] found that a new common law right to compensation exists where a person's conduct intrudes on another's "privacy or seclusion ... in a manner which would be highly offensive to a reasonable person of ordinary sensibilities". On June 16, in the case of *Grosse v Purvis*,[2] Senior Judge Tony Skoien of the Queensland District Court awarded the Mayor of Maroochydore $178,000 to compensate her, not for inappropriate dealing with her personal information, but for invasions of her privacy generally.

The decision in *Grosse* is particularly significant because it does not rely on any legislative privacy obligation, instead it seeks to develop the independent tort hinted at by the High Court in its 2001 decision in *ABC v. Lenah Game Meats*.[3]

In *Lenah*, Justice Michael Kirby noted that courts in a number of other jurisdictions have recently looked at the availability of such a common law actionable wrong of invasion of privacy. Justice Kirby's view was that this trend was stimulated in part by invasions (including by the media) deemed unacceptable to society and, in part, by the influence of modern human rights jurisprudence that recognizes a right to individual privacy. He went on to say (at 278):

> *[W]hether…it would be appropriate for this Court to declare the existence of an actionable wrong of invasion of privacy is a difficult question. I would prefer to postpone an answer to the question. Upon my analysis, no answer is now required.*

The potential for the development of the *Grosse* right was therefore clearly signposted.

## Characteristics

The Australian *Privacy Act 1988*, and all other Australian state and territory privacy statutes, regulate the way in which 'personal information' can be collected, stored, used and disclosed. These laws therefore focus solely on regulating the appropriate processing of information about individuals (or from which their identity can reasonably be ascertained). The right formulated in *Grosse* provides a very different means of redress for those disturbed by conduct amounting to an 'invasion of privacy'.

In the judgment, which he admitted was a bold first step in Australia, and is subject to an appeal likely to be heard later this year, Judge Skoien declared that Australian law allows the recovery of damages for harm (including mental, psychological or emotional suffering), embarrassment, hurt, distress and post-traumatic stress disorder, where a deliberate act intrudes on the private affairs or seclusion of another in a way which would be reasonably regarded as highly offensive. He also held that damages could be awarded for any enforced changes of lifestyle caused by such an intrusion.

Although Skoien J. recognized his judgment was at the leading edge of Australian privacy law, he considered it to be both logical and desirable. He found that:

- following, watching, approaching or loitering near a person;
- contacting a person in any way, including by telephone, mail, fax, e-mail or any other technology;
- loitering near, watching, approaching or entering a place where a person lives, works or visits;
- giving offensive material to a person or leaving it where it can be found by the person;
- an intimidating, harassing or threatening act against a person, whether or not involving a threat of violence; and
- an act of violence, or a threat of violence, against any property,

may justify an action for invasion of privacy if such conduct intruded on an individual's privacy or seclusion in a highly offensive way and caused harm or hindered them in doing an act they were lawfully entitled to do.

## Consequences

A non-statutory, common law right to the protection of private matters opens a large and unexplored new area for Australian privacy law. If the right survives the appeal process, or other similar actions are successful, it can be expected that a considerable body of new jurisprudence will evolve which will be very different for the statutory rights available under existing legislation.

The new right to take action at common law also has significant implications in a number of specific areas including the media and employment.

It is likely, for example, that if journalists and media organizations engage in highly offensive intrusions into people's personal affairs, they may be exposed to new actions for damages for any emotional harm and distress caused. As the new law is unrelated to the *Privacy Act*, the defences and exemptions in that Act do not apply, although a defence of public interest may be available.

Also, under Australia's current employment laws, the types of conduct that Skoien J. found to constitute invasion of privacy, are dealt with under equal opportunity legislation (harassment and discrimination) and occupational health and safety legislation (bullying).

It is unlikely that an employer would be found vicariously liable for the tort of invasion of privacy, as such behaviour is unlikely to be in the ordinary course of conduct as an employee. However, Australian employers should consider their general duty under the law of negligence to prevent reasonably foreseeable harm. An employer who had reason to suspect that an employee was engaged in a highly offensive invasion of privacy that related to the workplace in some way, and took no steps to prevent it would risk incurring liability in negligence, as well as under equal opportunity and occupational health and safety legislation.

---

1 June 16, 2003.
2 [2003] QDC 151.
3 (2001), 208 CLR 199.

## PIPEDA FINDINGS

**Privacy Law Group**
**Osler, Hoskin & Harcourt LLP**

*Decision #176*

*Bank Call Recording Practices Breach Consent Principle and Staff Training Requirements*

**Date of Decision: June 3, 2003**

**Disposition: Well Founded**

An individual claimed that his bank had recorded his customer service call without his consent, and subsequently refused to destroy the recording after he expressly withheld his consent to the collection.

The complainant called the bank to activate a credit card. Upon learning that his call was being recorded, he objected, however the telephone agent and supervisor said that the recording could not be stopped. The bank further advised the complainant that the tape could not be erased since it was made for the purpose of record-keeping, and was likened to a signature. The bank claimed that the complainant had implicitly consented to the recording since he had been informed of this practice via documentation that accompanied his accounts.

In a previous decision the bank had promised the Commissioner that it was recording customer calls according to the "best practices" he had recommended, namely informing a customer of call-taping, requesting their permission, and offering alternatives to call-taping. A few months after the bank claimed to have instituted the improved policy, the complainant called the bank and learned that these best practices had not been implemented. This situation also did not improve ten months after the purported implementation.

The Commissioner found that it was not reasonable that the bank had not brought the practice of recording telephone calls to the complainant's attention in the instructions on activating a new credit card. This was the one place the complainant was most likely to learn of this practice. Further, the Commissioner believed that it was a reasonable expectation of the individual that the fact and purposes of a collection of personal information should be brought to the individual's attention at the time of collection. While the bank did inform the complainant that the call was being recorded for specific purposes, he should have nonetheless been given the opportunity to consent or reject.

Accordingly, in the Commissioner's view the complainant had every reason to expect: (1) that the bank would stop taping his conversation once he refused to give consent; (2) that he would be told of any alternative means for achieving this purpose; (3) that his message would have been readily accessible since it was collected for record-keeping purposes; and (4) that the bank would honour his request for the deletion of his personal information. The bank did not meet any of these reasonable expectations. The Commissioner therefore found that the complainant did not consent to the tape-recording of his credit card activation, and did not respond in a reasonable manner to his refusal of consent, contrary to Principles 4.3 and 4.3.5 (in obtaining consent, the reasonable expectations of the individual are relevant). Because the bank had obviously failed to teach its staff about the best practices regarding the tape-recording of customer calls, the bank had also acted contrary to Principle 4.1.4 (requiring organizations to implement policies and practices training staff and communicating to staff information about the organization's privacy practices).

The Commissioner recommended that:

- the bank should try to find the tape-recording of the complainant's call for the purpose of providing him with a transcript of the conversation and to erase the call from its records;
- the bank should erase the recordings of the complainant's calls;
- the bank's call-recording system should be changed to permit telephone agents to initiate the recording only if customers consent;
- in instructions accompanying new credit cards, customers should be informed that their phone calls to the bank may be recorded;
- agents should notify customers from the outset that their call is being recorded;
- the bank should establish alternatives to the recording of card activation calls;
- the bank should revise its policy concerning the recording of customer calls, and consider the Commissioner's recommendations; and

- the bank should commence a formal training program to ensure that all of its agents adhere to the Commissioner's recommendations.

*Decision #172*

*Phone Company Breaches Consent Principle by Failing to Automatically Provide Call-Blocking of Non-Published Numbers*

**Date: April 28, 2003**

**Disposition: Well Founded**

A telephone company customer who has an unpublished telephone number complained that her name and number appeared on call display screens of other customers. The call display service allows subscribers to identify callers by name and number on their own telephone display screen. The telephone company responded to the complaint by asserting that non-published number subscribers could not have a reasonable expectation that their number would not be displayed on a call display screen given the pamphlets sent to subscribers in 1992 and 1994 upon implementation of the call display service; the welcome package sent to new subscribers, the information found in the telephone directory white pages, under sections pertaining to the call display service; and privacy and instructions to customer service staff to direct customers to this information. Those sources of information direct non-published number subscribers to a free blocking option whereby the subscriber's name and number would not display to recipients of outgoing calls from the unpublished number. The company also drew the Commissioner's attention to a decision of the CRTC approving the tariff amendment introducing the call display service in 1994. In this decision, the CRTC concluded that the introduction of call display with appropriate built-in safeguards would provide subscribers with the ability to select the most appropriate means of protecting their own privacy concerns, and that providing call-blocking to all non-published number subscribers automatically would significantly erode both the value of the call display service and the effectiveness in reducing annoying and offensive calls. The CRTC concluded that a benefit would be achieved by the call display service and that it was in the public's interest to approve the service.

The Commissioner assessed the publication of unpublished subscriber information on call display against the requirement in Principle 4.3.5 of the CSA Model Code on the Protection of Information (CSA Model Code), which states that the reasonable expectations of the individual are relevant in obtaining consent. The Commissioner found that new subscribers were being reasonably informed of the privacy implications associated with call display and that by going forward with non-published service, new subscribers had consented to the possible disclosure of their number on call display screens. There was no special effort made, however, to alert long-time non-published number subscribers to the blocking options available with respect to call display in the 1992 and 1994 pamphlets, nor would a long-time subscriber likely look in the telephone directory under call display or privacy issues to find out if their listing information would be disclosed. The Commissioner found that, when an individual pays for a non-published number, the individual's reasonable expectation is that the number will remain protected and not appear on call display screens. The onus, therefore, should not be on the individual to take steps to block the number from appearing, but rather should be on the company to automatically provide call-blocking as part of its non-published service. Without adequate notification to long-time subscribers having been made, the company contravened the Principle 4.3 Consent requirement in the CSA Model Code. The Commissioner recommended that the telephone company return to the CRTC given the prior tariff decision and take steps to ensure that automatic blocking of non-published telephone number subscriber information from appearing on call display screens be implemented.

**Note:** *This decision contrasts with the approach of the Commissioner in an earlier case involving a prior CRTC decision. In the earlier case, the Commissioner found a complaint by an unpublished telephone number subscriber that a telephone company charged fees for the unlisted service to be not well-founded, based on a prior decision of the CRTC authorizing the telephone company's charges for non-published telephone service (see* PIPED Act Case Summary *#8, August 14, 2001 and* Englander v. TELUS Communications Inc.*, [2003] F.C.J. No. 975 (QL), 2003 FCT 705 (T.D.)).*

*Decision #162*

*Airline Website Breaches Tied Consent Prohibition by denying Access to Cookie Disabled Users*

**Date of Decision: April 16, 2003**

**Disposition: Well Founded**

In this complaint, an individual claimed that an airline company: (1) denied him access to its web site because his browser was configured to disable "cookies"; and (2) the company inappropriately collects personal information of all visitors to the web site by placing a cookie on their computer hard drives.

The airline web site used both permanent and temporary cookies. The permanent cookies were used to collect the user's language and country of choice, so that the user is greeted in his/her preferred language and sees the version (either Canadian or US) of the site previously selected. The temporary cookie stores information from fields in the customer's profile which is created when the customer signs in. The collected information includes the customer's name, mileage balance, residing country code and language preference. The information collected by the temporary cookie is deleted when the customer logs off.

The web site in question was coded in a manner that prevented customers from proceeding until a cookie had been stored. As a result, the complainant was unable to proceed to the home page of the site.

The company acknowledged that this was caused by an application glitch and took steps to ensure that visitors with disabled permanent cookies could use the site. The company also acknowledged that it did not include information about the cookies it uses in its privacy policy nor on its web site.

The Commissioner found that the information stored by the temporary and permanent cookies qualified as personal information under PIPEDA. Although the company did not intentionally deny access to its web site to individuals who had disabled permanent cookies, the denial of access to the complainant was in contravention of Principle 4.3.3 of the CSA Model Code, which prohibits an organization from, as a condition of the supply of a product or service, requiring an individual to consent to the collection, use or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes. In addition, the airline had failed to meet the requirement for knowledge and consent in Principle 4.3 of the CSA Model Code by failing to advise individuals about its use of cookies on its web site.

*Decision #167*

*Magazine Breaches Consent Requirement with Inadequate Opt Out Mechanism*

**Date of Decision: April 11, 2003**

**Disposition: Well Founded**

A magazine subscriber complained that the magazine had been selling or renting his name and address to third parties without his consent. When the complainant wrote to the magazine requesting they stop this practice, the magazine replied by confirming the removal of the complainant's name from its list rental database, and by requesting that its list-rental companies do so as well. The magazine pointed out that the masthead of its issues contained notification of its disclosure of subscriber information to third parties and of the opt out procedure.

During the investigation, the magazine expressed concerns to the Commissioner that it would be put at a competitive disadvantage if it were to provide notification at a level of disclosure different from that of the rest of the industry and that it would take any recommendation made by the Commissioner to the Canadian Marketing Association for discussion.

The Commissioner noted in his findings that his conclusions in any given case were never meant to be subject to industry approval, and that he expected compliance with the Act from an industry as a whole no less than from particular organizations within it. The Commissioner fully approved of the magazine's intention to take the Commissioner's recommendations to the CMA for discussion, but stated he wished to make clear that the recommendations were issued for compliance, and not for negotiation.

The Privacy Commissioner found that the magazine's masthead did contain a notification that subscribers' names were sometimes made available to other companies and of the opt out mechanism, but that this notification appeared in very small print and was buried in a dense paragraph of miscellany at the bottom of a column. The Commissioner also noted that the notification did not identify the companies or types of

companies to which subscribers' names were made available, did not explicitly state that subscribers' addresses were made available as well, and mentioned only one method of opting out — request by mail. In addition, the Commissioner found that no opt out or notification appeared on the magazine's subscription card.

The Commissioner determined that the complainant had a reasonable expectation that the magazine should have brought its secondary marketing purposes for the use and disclosure of subscriber information to the complainant's attention on the occasion when the Complainant was making the decision to subscribe and thereby entrust his personal information to the organization. The Commissioner noted that an individual whose consent to third party disclosures is merely being assumed (through an opt out consent) has all the more reason to expect the organization to be forthright and diligent about explaining its intentions in affording an opportunity to opt out. As a result, the Commissioner will give weight to the "knowledge" principles in 4.2.3 (identified purposes should be specified at or before the time of collection) and 4.3.2 (to establish "knowledge and consent", organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which their information will be used); and to the individual's reasonable expectations under Principle 4.3.5 of the CSA Model Code.

The Commissioner recommended that the magazine:

- "include a purpose statement and a checkoff box on its subscription form";
- "display the statement prominently in regular type size and include in it a description of the items to be disclosed (i.e., name and address) and the organizations to which the disclosures are to be made" (identifying these organizations at least by type).

Provided that these steps are carried out and the items of information to be disclosed remain limited to name and address, the Commissioner found that the magazine may continue to use the "opt out" form of consent:

- "for ongoing use, provide and prominently advertise a mechanism whereby subscribers may conveniently, inexpensively, and promptly withdraw consent, such mechanism to include a toll-free telephone number"; and
- "...to present the Commissioner's recommendations to the CMA and, ... convey [the Commissioner's] expectation that all CMA members will quickly adopt [the recommendations] by way of setting a new industry standard of compliance".

**Note:** *In this case, the Commissioner sets the standard for a valid opt out form of consent where disclosure to third parties (*i.e.*, non-affiliates) for secondary marketing purposes will be compliant with PIPEDA.*