Office of the Privacy Commissioner of Canada

Contributions Program

Implementing PIPEDA: A review of internet privacy statements and on-line practices

Submitted by Rajen Akalu
May 6, 2005
Centre for Innovation Law and Policy
Faculty of Law
University of Toronto
78 Queen's Park
Toronto, ON
M5S 2C5

Contributors

Rajen Akalu – Lead researcher, Bell University Manager (Law), Centre for Innovation Law and Policy

Aniz Alani – Researcher, JD Candidate, Faculty of Law

Lisa Austin – Research Advisor, Associate Professor, Faculty of Law

Barbara Bressolles – Researcher, LL.M Candidate, Faculty of Law

Nadia Caidi – Research Advisor, Associate Professor, Faculty of Information Studies

Andrew Clement – Principal investigator, Professor, Faculty of Information Studies

Sooin Kim – Co-researcher, Librarian, Centre for Innovation Law and Policy

David Ley – Web Master, MISt Candidate, Faculty Information Studies

Robert Luke – Researcher, PhD Candidate, Faculty of Information Studies

Sapna Mahboobani – Researcher, MISt Candidate, Faculty of Information Studies

Andrea Slane – Research Advisor, Adjunct Professor, Osler, Hoskin and Harcourt LL.P

Executive Summary

This document constitutes the final project report of an investigation funded by the Office of the Privacy Commissioner (OPC) Contributions program. A project proposal was submitted to the OPC on August 13, 2004 and an award of $48,300 was publicly announced on January 27, 2005 with a completion date of March 31, 2005 for expenditure of funds related to the project.

Research was undertaken by the Centre for Innovation Law and Policy in close partnership with the Information Policy Research Program (IPRP). This culminated in a full day conference which highlighted preliminary research on March 18, 2005. The conference was webcast and included leading experts in the field of information privacy.

The central aim of this project has been to evaluate the implementation of the Personal Information and Protection of Electronic Documents Act[1] ("PIPED Act") by reviewing privacy policies posted on the Internet by companies in the telecommunications, airlines, banking and retail sectors.

Where possible we have made use of publicly available information regarding corporate information management practices and combined this with a discussion of topical issues facing the target industry sector in light of developments at the national and international levels.

There are four substantive papers included in this report based upon investigations into three federally regulated industry sectors and the retail sector. Since the PIPED Act had been applied to federal works since its enactment, we were interested in determining whether experiences in these industries could be transferred to the retail sector.

In the absence of clear legislative mandate at the federal level to regulate privacy with respect to 'all commercial activity', movements at the international level, particularly the European Union with its Data Protection Working Party Opinion on information notices and advance passenger information and passenger name record are likely to have the greatest impact on privacy discourse in this country.

What we find is that despite having considerable resources to devote to the issue of privacy the implementation of the PIPED Act has been *ad hoc* at best and non-existent at worst. Companies it would appear are motivated to communicate their information management practices in large measure as a result of business prudence rather than concerns for individual privacy.

While might be expected, the unwillingness on the part of the OPC to name respondents that are culpable of the most egregious violations of individual privacy even where so doing would be 'in the public interest' does little to cultivate the jurisprudence in this area, much to the chagrin of privacy advocates. The dual role of recognizing business interests and individual rights with respect to privacy - a value that is far from absolute results in uncertain interpretation and application of the Act. Coupled with tenuous legal

[1] R.S.C. 2000, c. 5.

drafting, this hybrid of legislative instrument and industry code is at times in many instances ill-suited to further refine our understanding of the privacy interest and the consequences of the harm caused by the loss of it.

Table of Contents

Appendices

Introduction

A central theme of this project has been a consideration of the extent to which privacy policies satisfy the requirement of "openness" pursuant to the PIPED Act. Organizations make information about their policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. An organization may make brochures in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

However in many instances this communication is motivated by a desire to obfuscate the consumers' attempt to understand an organizations' information management practice rather than clarify expectations as between company and consumer. This research has focused on the approach to communicating privacy policy and practice by organizations in the airline, telecommunications, banking and retail sectors. We selected the first three industries because they are federally regulated and the PIPED Act has applied to them since its enactment.

This principle contemplates the consumer being able to ascertain information about the organization's business practice with respect to the use collection and disclosure of personal information without unreasonable effort on the part of the individual. However, in many instances consumers (and even trained researchers!) experience considerable difficulty understanding a given organization's information management practices.

Our work involved creating a 26-point questionnaire and contacting the privacy information officers in the industries mentioned above to learn about the effectiveness of communicating privacy statements to the public. Our project team's research was significantly disadvantaged by University research ethics board requirements. However a number of chief privacy officers were willing to be interviewed and this served to inform our research. In future research we hope to make use of research instruments of the type designed in this project to provide more a more quantitative research output.

Four papers were written based on the industry sectors examined. Each paper considers a current issue facing the industry and discusses the ways in which a given organization's information management practices are communicated to the public.

The first paper titled: "Mathew Englander – Toonie or Loonie? – Assessing the impact of the *Englander v. Telus* decision" explores privacy in the telecommunications sector through an analysis of the leading PIPED Act case of *Englander v Telus Communications Inc.* In this case the court finds that identifying the purpose of collection, use and disclosure of personal information, while varying according to circumstances, must take place at the time of collection in the first instance. The Court suggests that corporate communications to the consumer can be the basis of a finding of 'tacit consent' should if it is eventually demonstrated that customers are aware of the brochures etc. at the time they subscribe.

Making more information available and accessible to consumers may, given the depersonalized relationship between consumers and corporations, eventually serve to abrogate consent in this context. The *Englander* case is in many respects an examination of different perspectives on privacy. The case also exposes the internal contraction of the

PIPED Act, an act seeking to assuage both industry business interests as well as the privacy concerns of individuals. Without commitment to providing context-specific analysis and naming respondents in cases that are 'in the public interest' the seeds of further confusion are likely to be sown.

The second paper in this report considers the online privacy statements of four Canadian airlines in light of the Article 29 Data Protection Working Party Opinion on the level of protection ensured in Canada for the transmission of Passenger Name Record (PNR) and Advance Passenger Information (API) from airlines, and the requirements of the PIPED Act. A discussion of the Working Party Opinion was considered important in this area because of the considerable influence the Working Party has on data protection in non-EU countries. The specific commitments of the Canadian Border Services Agency are currently the subject of negotiation with the EU and are currently not being made available to the public. However a comparison was made between the Working Party Opinion and the obligations placed on the airline industry pursuant to the PIPED Act. In the case of airlines the Working Party Opinion highlights a lack of uniformity in the approach taken by airlines in communicating their information management practices. The absence of enforcement powers within the Office of the Privacy Commissioner results in an inconsistent implementation of the PIPED Act and the basis of systemic privacy violations.

In the third paper, a comparison is made between the online privacy notices of two leading Canadian banks CIBC and Scotiabank in the light of the Article 29 Data Protection Working Party Opinion on more harmonized information provisions with particular reference to the proposed European information notice solution. The proposed information notice is significant from the perspective of "openness" because it seeks to improve awareness of data protection rights and responsibilities as well as enhance the quality of information on data protection. It does this through a three-tier notice system, the first layer providing 'core' information and the second and third more relevant information that is required by the EU Data Protection Directive and the national law respectively. Taken together, these would be deemed to constitute a legal notice.

A comparison of two leading Canadian banks reveals stark differences in the manner through which information management practices are communicated to the public. CIBC has its privacy policy in a long format, where as Scotiabank makes use of embedded links. While both banks would likely fail to satisfy the EU information notice requirements, Scotiabank's notice was found to be more user-friendly. It was concluded that the harmonization of information notices is likely to result in greater ease of comparison between information management practices because companies are forced to make use of an accepted information template and make information delinquencies more difficult to conceal.

The fourth and final paper examines the issues concerning the protection of personal information within the retail business sector in Canada. This paper considers the extent to which retail businesses' web site privacy statements address concerns associated with the collection, use and disclosure of personal information in this context. The paper points out that the PIPED Act fails to distinguish between industry sectors other than by differentiating federal works from other forms of commercial activity. These latter

undertakings are the subject of provincial jurisdiction and the legal remit of the federal government to legislate in this area is at present unclear.

In addition the PIPED Act does not distinguish between small and large retail industries instead imposing positive obligations on all organizations. This paper concludes by suggesting that the retail sector is following the lead of the federal undertakings, but this may well be a movement in the wrong direction. It recommends the publication of detailed privacy manuals as a means of providing consumers with a meaningful basis upon which to assess the companies' information privacy practices and hold them to account.

Project Achievements

- Pursuant to our research aim, four research papers were produced documenting our investigation of the implementation of the PIPED Act in the telecommunications, airlines, banking and retail sectors. These papers have been made available for comment and review on our project website and will be submitted to peer-reviewed journals in due course. The OPC will receive acknowledgment of support in all publicly disseminated materials.

- We were invited to participate in a forum titled: "Anonymity, Identity and the Prospect of Privacy" at the University of Ottawa on March 3, 2005. The event was organized by the Information Technology Law Association at the Faculty of Law. **(See Appendix 2)** Students participating in the discussions remained in Ottawa to attend a conference sponsored by the University. The lead researcher was invited to contribute a web log sponsored by the University of Ottawa to describe the project and its aims.

- The highlights of the project was a full day conference held at the University of Toronto Faculty of Law on March 18, 2005. The conference featured Daniel Solove, an Associate Professor of law at the George Washington University Law School and an authority in the areas of information privacy law and cyberspace law. The conference also included a panel discussion on the impact of the recent FCA ruling in the *Englander v. Telus* case. A spirited discussion was staged between Mathew Englander and Drew McArthur, Chief Privacy Officer at Telus. A presentation by Stephanie Perrin President of Digital Discretion, and Research Coordinator, Anonymity Project (www.anonequity.org) was also made on the subject of assessing the effectiveness of the PIPED Act. Complete details of this event are available online and in the CD that accompanies this document. **(See Appendix 1)**

- A 26-point research instrument was devised as part of our research. Unfortunately, due to onerous requirements of the University's Research Ethics Board approval, which was not anticipated, the letter that was required to accompany our initial contact with external participants resulted in reluctance on the part of privacy officers to participate. The research instrument was however useful in identifying consumer concerns. **(See Appendix 3)**

- A website http://pipedaproject.atrc.utoronto.ca/ was designed to advertise our conference and disseminate information about our research. A live web cast link was established to allow remote participants to engage in our discussions.

- The research group was also selected to participate in the Faculty of Information Studies Research Day on April 1, 2005 (seehttp://www.fis.utoronto.ca/activities/researchday.htm) This was a day-long event celebrating the research of Faculty of Information Studies faculty, students and staff.

Telecommunications: "Mathew Englander – Toonie or Loonie? – Assessing the Impact of the Englander v. Telus Decision"

by Rajen Akalu

This paper considers privacy in the telecommunications sector through an analysis of the recent case of *Englander v Telus Communications Inc.*[2] as well an in depth discussion with Drew McArthur, CPO at Telus who was interviewed as part of our research.

Introduction

The *Englander* case concerns the interpretation of the PIPED Act with respect to the personal information published in telephone directories. The complainant in the case asserted that in failing to obtain the consent of its first time customers, Telus had contravened the knowledge and consent requirements of the PIPED Act. It was also alleged that the charging of a $2 fee for providing a Non-Published Number Service (NPNS) was in contravention of the spirit, if not the letter, of the PIPED Act. The Federal Court of Appeal agreed with Mr. Englander's reasoning in relation to the knowledge and consent issue, but rejected the latter argument.

The case is significant from the standpoint of privacy for the following four reasons which will be examined in turn: First, it provides a view of privacy based on a particular set of facts from a number of perspectives. As privacy is a value that must be viewed in its context, we are afforded an analysis of privacy as applied to a specific set of circumstances. Second, the case highlights the problem of self-regulatory codes enshrined in legislative enactment. Third, the Court in *Englander* provides some interesting commentary on the principle of openness and consent and finally, there are some valuable insights on the role of the Office of the Privacy Commissioner that can be distilled from the case.

Perspectives on Privacy

Central to the privacy debate in the consumer context are three different perspectives: the activist perspective, the corporate perspective and the centralist perspective.[3] The activist perspective argues that harmful social costs will be incurred if free-market forces and technological advancements proceed unchecked.[4] The corporate perspective by contrast takes the view that companies have a fundamental business imperative to collect, use, and disclose personal information in the course of operations. The imposition of unfettered restrictions in this regard may, in certain cases, introduce market distortions and impede an organization's ability to compete efficiently. Lastly, there is the centralist perspective. Here, proponents contend that consumers require choice. These choices can be made more meaningful if 'reasonable' corporate access to personal information is permitted.[5]

---

[2] [2004] FCA 387.
[3] M. Culnan and R. Bies, "Consumer Privacy: Balancing Economic and Justice Considerations" *Jnl of Social Issues*, Vol. 59, No. 2, 2003.
[4] S. Garfinkel and D. Russell, Database Nation: The death of privacy in the 21st century. 2000.
[5] R. O'Harrow, "Night and day, computers collect information" *The Washington Post* p. G10 2001.

These perspectives are seen in the *Englander* case. Mathew Englander, could well be characterized as an activist; championing the cause of privacy and vindicating his rights on behalf of Canadian consumers. Telus typifies the corporate perspective on this issue, viewing privacy as a variable (and there are many) in the organization's operational equation. The court in the *Englander* case arguably takes a centralist position in partially ruling in favour of the complainant on the consent issue but agreeing with Telus with respect to the charging of a $2 fee for NPNS.

Breach of Consent Requirement

At the core of the three perspectives on privacy lies the perennial question of who controls information given by consumers. This is of particular salience in this case since the PIPED Act will not apply to information deemed publicly available.[6]

The argument for regarding personal information contained in a telephone directory being readily available is supported by the Canadian Radio-Television and Communications Commission (CRTC).[7] The telecommunications sector is unique among federally regulated industries with respect to privacy. This is because in addition to the requirements of the PIPED Act, telecommunications companies (telcos) are also subject to regulation by the CRTC which also has as part its mandate, the protection of privacy.[8]

The CRTC has expressed the view that "the provision of directories form an essential part of, and significantly enhance the value of, the company's basic telephone service."[9] As a result telcos are required to distribute directories free of charge to customers.[10] Moreover, in reporting on directory listings the CRTC commented that "…subscribers currently expect that, unless they request an unlisted number, their telephone numbers will be published in the telephone companies' directories and will be available through directory assistance."[11]

However the increased accessibility of subscriber information and the ability to manipulate this data make de-listing one's name perhaps the only way of affording the consumer some measure of control concerning how their data is subsequently used. Taking the above factors into account the Commission found it appropriate to require telcos to provide NPNS at a rate that does not exceed $2 per month for residential subscribers.[12]

The Court makes the important observation that while publicly available information can be collected, used and disclosed without consent, this cannot apply to the organization

[6] PIPED Act, s. 7 . See also Regulations Specifying Publicly Available Information (P.C. 2000-1777, SOR/2001-7 (a) and (b).
[7] Report on Directory Subscriber Listings and on Unlisted Number Service 1996 ("CRTC Report").
[8] Telecommunications Act, s. 7.
[9] Telecom Decision CRTC 94-1.
[10] Telecom Decision CRTC 97-8.
[11] CRTC Report, *supra*.
[12] Telecom Decision CRTC 98-109.

that initially collects the information for the purpose of publishing a telephone directory, which, once published, will become publicly available.[13]

The Court goes on to note that consent for information that will be made publicly available must take place on or before the time of enrolment in the service.[14] The court's centralist position with respect to privacy is seen in the statement that:

> First-time customers have the right to know before their personal information becomes "publicly available" within the meaning of section 7 of the Act, with all the consequences that might flow from such publicity, that they can exercise their right to privacy and choose not to be listed. This seems to me, a fair compromise between one's right to privacy and the industry's needs.

Though correct, it is unfortunate that the Court declined the opportunity to comment on information in the public sphere. The increased sophistication of data manipulation technology permits even publicly available information to be aggregated to provide a detailed digital portraiture of an individual.[15]

Thus the *Englander* decision can be regarded as a narrow holding in this regard. Whether industries beyond the telcos sector will inform their customers of the consequence of initial collection remains to be seen. Though this is unlikely, the case deals with a regulated industry sector pursuant to a fact pattern that is not likely to recur in future cases. Thus its applicability across the spectrum of businesses would appear limited. Other telcos however will no doubt be revising their policies to inform customers of their right to have their information excluded from the directory for a fee.

Charging of Fees

The complainant, as well as others, is fundamentally opposed to the imposition of a fee for the right to control how their personal information is subsequently used.[16] The view taken is that there are circumstances (such as a victim suffering spousal abuse) that warrant NPNS as a matter of necessity. Although it was not argued that there can never be a fee charged for asserting rights to privacy this could only be accomplished under the PIPED Act if the statute provided for it.[17] However it was found that the CRTC, in approving rates and services and taking into account the protection of the privacy of Canadians, signals Parliament's intent that the imposition of fees for providing privacy services were indeed contemplated.

There was also mention of the fact that fees for this service may also constitute an economic barrier to low income groups. The Court made short work of this argument in stating that while this proposition "may have validity from an access to services perspective, the use of fees is not specifically a protection of privacy issue."[18]

---

[13] *Englander,* para. 54.
[14] *Englander*, para. 67.
[15] Daniel Solove, *The Digital Person,* New York University Press: New York, 2004.
[16] See Submission made to the CRTC by the Information Privacy Commissioner cited in *Englander* at para. 32.
[17] *Englander*, para 81.
[18] *Englander*, para 34.

The PIPED Act and Self-Regulation

Of relevance in the *Englander* case are the comments made about the PIPED Act and self-regulation. Self-regulation takes the traditional governmental regulatory model of legislation, enforcement and adjudication and applies them to the private sector.[19] The fair information practices are rules created for a self-regulatory regime.[20] While there is wide support for the principles as sound public policy, the question that remains, even after the enactment of the PIPED Act, is whether legislation is the appropriate regulatory instrument in this context. This is of particular relevance in the advent of the review of the Act scheduled next year.[21]

The stated purpose of the PIPED Act is "…to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances…" In providing its historical account of the factors influencing the enactment of the PIPED Act, the Court examines the tension between the Council of Europe model for privacy[22] and the fair information practices, championed by the OECD.[23] The OECD principles were intended to be non-binding but helped to build trust and promote disclosure of personal information which in turn, facilitates relationship marketing.[24] The Council of Europe model by contrast favoured implementation in to national law. The tension between the legislative and self-regulatory approach to privacy protection in the commercial context was a central theme in the discussions which led to the creation of the Canadian Standards Association Model Code of the Protection of Personal Information.[25]

Part 4 of the CSA Standard became Schedule 1 to the PIPED Act. Perrin et al[26] state that "with the full support of the industry players who contributed to the CSA Standard, but to the great bewilderment of privacy experts and legal scholars everywhere, the drafters of this legislation set the task of incorporating the text of the standard in the law." As a consequence modifications of the legal text of the Act would invariably ensue.

The problem with this approach is that industry codes serve entirely different functions to legislation. Codes express a general aspiration which is in the main voluntary, normative, non-binding in orientation and of general applicability. Legislation on the other hand is prescriptive and creates specific binding legal rights and obligations. The Court in *Englander* notes that the CSA Standard was "the product of intense negotiations between competing interests, which proceeded on the basis of self-regulation and which did not use nor purport to use legal drafting."

---

[19] P. Swire, "Markets' self-regulation" 1997.
[20] Culnan, "Protecting privacy online: Is self-regulation working?" *Journal of Public Policy and Marketing vol 19(1)* Spring 2000, p.20.
[21] PIPED Act s. 29.
[22] The Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data E.T.S. No. 108, Strasbourg, 1981.
[23] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Annex to Recommendation to the Council, September 23, 1980.
[24] M. Culnan and P. Armstrong, "Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation" *Organization Science, vol* 10 1999. p.104.
[25] CAN/CSA-Q830-95.
[26] S. Perrin, *The Personal Information Protection and Electronic Documents Act: an annotated guide* Irwin Law, 2001.

The incorporation of a voluntary instrument into law presents difficulties for analysis of issues in this context. This is because the rules of statutory construction are of little application in the context of interpreting a code. This is underscored by s. 5(2) of the PIPED Act which states that the use of 'should' does not impose a legal obligation. The Court therefore concluded that "[i]n these circumstances, flexibility, common sense and pragmatism will best guide the Court."[27] This marked departure from legal reasoning is problematic in the context of privacy discourse since the value of a decision based on 'common sense' will be of limited application in future cases.

Coupled with the protean nature of privacy, which makes it highly elusive to definition with any legal precision, we find a situation where we are further away from understanding what is meant by an expectation of privacy as well as the harms caused by a loss of privacy. Clearly, privacy is not an absolute value but the present regulatory framework does little to further our understanding of this concept. The resulting uncertainty is problematic for both business as well as consumers.

Consent and Openness

As noted above the Court in *Englander* held that Telus infringed the consent requirement of Schedule 1 of the PIPED Act in failing to inform its first time customers, at the time of enrolment, of the primary and secondary purposes for which their personal information was collected and not informing them of the availability of the NPNS.

The Court highlights Principle 2, "Identifying Purposes"[28] and 3 "Consent"[29] to be of particular relevance in the Englander case. These principles, the Court remarks "…clearly impose on the organization the burden of making clear to the individual all the purposes for which the personal information is collected at or before the time of collection." The obligation on the part of the firm will vary depending on the circumstances and type of information being collected.

The Court also remarks that in complying with Principle 8, "Openness," which requires an organization to make available specific information about its policies and practices relating to the management of personal information may be the basis of a finding of 'tacit consent', should it be demonstrated that first time customers are aware of the brochures at the time they subscribe.[30]

A central theme of the "Implementing PIPEDA: A review of Internet privacy statements and on-line practices" project has been the extent to which companies are open about their privacy practices. Ideally, openness should mirror knowledge and consent, but the reality is that an information asymmetry exists between company and individual in a depersonalized arrangement. The absence of a clear legal recourse makes the need for organizations to provide information about their personal information management practices far greater. Cavoukian has suggested that consumers are "far less willing to

[27] *Englander*, para 46.
[28] PIPED Act, Sch. 1, cl. 4.2.1.
[29] PIPED Act Sch. 1, cl. 4.3.1.
[30] *Englander*, para 61.

entrust their personal data to organizations that, at a minimum, don't have a posted privacy statement."[31]

The Role of the OPC

The Office of the Privacy Commissioner has a clear policy making mandate to promote privacy through the research and development of information programs to foster public understanding on the subject of privacy as well to encourage organizations to develop detailed policies and practices, including organizational codes of practice to comply with the PIPED Act.[32]

The PIPED Act however seems to suggest that its role is both conciliatory as well as adversarial when it comes to handling individual privacy complaints and protecting privacy as a whole.

In practice it would appear the OPC has a strategy of conciliation and confidentiality with respect to the handling of individual complaints. This is entirely appropriate, given the sensitive nature of the information to which the Commissioner is privy. The OPC does, pursuant to the PIPED Act have the discretion "…to make public any information relating to the personal information practices of an organization if the Commissioner considers that it is in the public interest to do so."[33]

Toward the end of its judgment, the Court remarks in *obiter* that the Office of the Privacy Commissioner "…is not a tribunal and has no decision-making power under the PIPED Act. At best, the Commissioner can form an opinion on the issue and include it in his report."[34] Lawford has suggested that this is tantamount to regarding case summaries as "legally worthless.[35]" This view perhaps fails to recognize that the Commissioner serves a policy making function and has ability to issue policy statements, opinions, or in this case findings. This flows from the executive rather than judicial character of such bodies.

The reluctance on the part of the Commissioner to exercise this power is to some extent understandable in view of the fact that a practice regularly naming respondents would compromise its mediation function. However, naming can serve as a sanction for non-compliance as well as an incentive to comply if the procedures which will result in publication are clearly articulated with industry players. Suggested criteria for this process could include the severity of the breach of privacy to a given class, harm caused to the individual complainant as well as failure to promptly implement recommendations.

At present the practice of reporting case summaries with names removed provides little assistance to individuals and practitioners attempting to follow these issues as they evolve creating considerable uncertainty and frustration, particularly for privacy advocates.

---

[31] A. Cavoukian and T. Hamilton, *The Privacy Payoff* McGraw-Hill Ryerson Toronto: 2002.
[32] PIPED Act s. 27.
[33] s. 20 (2) PIPED Act.
[34] *Englander* para 71
[35] J. Lawford, "Consumer Privacy under PIPEDA: How Are We Doing?" *Public Interest Advocacy Centre*: Ontario *available at* http://www.piac.ca/PIPEDAReviewFinal.pdf 2004.

Conclusion

The *Englander v. Telus* decision is not a 'David and Goliath' story but rather an examination of competing perspectives on issue of privacy. The case provides a good illustration of the activist, corporate and centralist perspectives in the privacy debate. All of these positions have intrinsic validity, but fail to fully address the problem when taken individually. If nothing else the *Englander* decision provides a context for discussion on the issue of privacy with respect to these perspectives.

In this context the PIPED Act is shown to suffer from an internal contradiction as to purpose, attempting to satisfy the needs of both industry and individuals. The case also illustrates the difficulties in enshrining industry codes in law. This approach is understandable given the fact the privacy value is not absolute and difficult to define. However if we are to move beyond decisions based on 'common-sense' and refine our understanding of what is meant by an expectation of privacy and the harm that results from its loss, a willingness to cultivate the jurisprudence in this area will be needed. The OPC can contribute to this development if it is prepared to name respondents under prescribed circumstances. This, it is submitted, would add greatly to privacy discourse by providing a more substantive basis for discussion between the activist and corporate viewpoints.

Airlines: "Assessing the Level of Protection Afforded in Canada for the Transmission of Passenger Name Record (PNR) and Advance Passenger Information (API) From Airlines"

by Barbara Bressolles

This paper compares the online privacy statements of four Canadian airlines in light of the Article 29 Data Protection Working Party Opinion on the level of protection ensured in Canada for the transmission of Passenger Name Record (PNR) and Advance Passenger Information (API) from airlines[1], and the requirements of the PIPED Act.

Introduction

The Article 29 Data Protection Working Party ("Working Party") is an independent advisory body on data protection and privacy.[2] On January 19, 2005 the Working Party adopted Opinion 1/2005 on the level of protection ensured in Canada for the transmission of PNR and API from airlines ("Opinion"). The opinions of the Working Party are of important significance given the European Commission's policy of prohibiting the transfer of personal information to nations that fail to ensure an adequate level of personal data protection.[3] The opinions more generally provide valuable insights into European data protection law and policy, which provided the international context in which Canadian data protection legislation such as the PIPED Act was born.[4] This paper examines the online privacy statements of Air Canada, WestJet, CanJet and Jetsgo in view of the conclusions reached in the Opinion. It also considers the extent to which the statements demonstrate the airlines' compliance with the PIPED Act.

The Working Party Opinion on Protection for the Transmission of API/PNR from Airlines

The adoption of the Opinion follows negotiations between the European Commission and Canada, which sought to resolve problems highlighted by the Working Party in the opinion it issued on 11 February 2004,[5] in which the Working Party concluded that compliance with the Canadian requirements by the airlines at that time raised concerns in respect of the Data Protection Directive 95/46/EC. As a result of these negotiations, the Working Party received a document dated January 18, 2005 containing Commitments by

[1] "Opinion 1/2005 of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995", WP 103 of the Working Party, issued 19 January 2005.

[2] The Working Party was set up under Article 29 of Directive 95/46/EC. Its tasks are set out in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC.

[3] The European Data Protection Directive includes a provision that prevents the transmission of any personal information outside of the European Union unless the recipient country has legislation in place that would offer substantially similar protections: see Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] It was in response to the European Directive 95/46/EC that the Canadian government introduced legislation that would be considered by Europe to be sufficiently similar to the Directive.

[5] "Opinion 3/2004 of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995", WP 88 of the Working Party, issued 11 February 2004.

the Canada Border Services Agency ("CBSA") relating to the application of its PNR program.[6] The Opinion was adopted in light of these Commitments.

In the Opinion, the Working Party analyses the level of protection ensured by Canada once airlines have transmitted API and PNR data relating to their passengers and crew members to the CBSA. Under Canadian law, all commercial carriers are required to provide the CBSA with API/PNR data relating to all persons on board commercial conveyances bound for Canada.[7] API is basic information and includes the traveller's name, date of birth, citizenship or nationality and passport or other travel document data.[8] PNR data is more detailed information, which includes the travel itinerary, address and check-in information and is gathered by airlines in their reservation, check-in and departure control systems.[9] API/PNR data is used by the CBSA to identify persons who may be subject to closer questioning or examination on arrival in Canada because of their potential ties with terrorism. Based on its analysis, the Working Party concluded that Canada ensures an adequate level of protection with regard to the processing of API and PNR data transferred from airlines to the CBSA in relation to flights concerning any person on board a conveyance arriving in Canada.[10] In reaching this conclusion, the Working Party identified several components of the Commitments that reflect the European Commission's policy that the legitimate requirements of air transport security and internal security in Canada should not contradict fundamental rights of privacy and data protection.[11]

Specific Commitments Endorsed by the Working Party

- The Working Party welcomed section 7 of the Commitments, which states that the Canadian Passenger Information System PAXIS has been configured to receive API and PNR data 'pushed' from a carrier rather than transferred through a 'pull' system. The Commitments also defined narrowly the purposes for processing API/PNR data so as to maintain balance in the approach to be taken in respect of fighting terrorism.[12]

- The Working Party commended the Commitments insofar as they reduced the number of data elements to be transferred to the Canadian authorities from 38 (which the Working Party previously considered as going well beyond what could be considered adequate, relevant and not excessive for the purposes for which

[6] As at 2 May 2005, a copy of the Commitments was not publicly available due to ongoing negotiations between the European Commission and Canada.
[7] The CBSA's authority to obtain and collect such information is s. 107.1 Customs Act, and the Passenger Information (Customs) Regulations, and paragraph 148(1)(d) of the Immigration and Refugee Protection Act, and regulation 269 of the Immigration and Refugee Protection Regulations.
[8] "Advance Passenger Information/Passenger Name Record" Canada Border Services Agency Fact Sheet, January 2005.
[9] "Advance Passenger Information/Passenger Name Record" Canada Border Services Agency Fact Sheet, January 2005.
[10] The Opinion states that Canada ensures an adequate level of protection with respect to API and PNR transferred from airlines to the CBSA in relation to those flights defined in s. 107.1 of the Customs Act, which requires commercial carriers to provide the CBSA with API/PNR data relating to all persons on board commercial conveyances bound for Canada.
[11] "Opinion 3/2004, *supra* note 5.
[12] See s. 2 of the Commitments, cited in the Opinion, *supra* note 1.

data is collected and/or further processed),[13] to 25, none of which contain sensitive personal data such as personal information revealing racial or ethnic origin, and data concerning health or sex life.[14]

- The Commitments provided for the required retention period for data to be reduced from 6 years to 3.5 years, and for the information to be increasingly de-personalized during the 3.5 year period.[15]

- The Commitments only allow for transfers of a minimum amount of data in specific cases directly related to terrorism or terrorism-related crimes, and in the case of transfers to other countries, the level of data protection granted by the receiving country figures as one of the criteria to be taken into account.[16] In addition, only countries having received an adequacy finding under the Directive, as well as EU Member States, are eligible to receive API and PNR data retained in PAXIS (being data held on passengers who are not the subject of an investigation in Canada).

- Finally, s. 21 of the Commitments provides that the CBSA will provide information to passengers relating to the collection of data and that the CBSA is committed to administratively extending certain rights under the Privacy Act to citizens who are not present in Canada, including rights of access, correction and notation with regard to personal information.[17] Such an extension of the Privacy Act would bring the Act in line with the international scheme of privacy protection that reaches over borders. Indeed, the PIPED Act was implemented in light of threatened restrictions on cross border-border data flows caused by the European Directive.

The above elements of the Canadian API/PNR program, as endorsed by the Working Party, may be taken to constitute indicators of a balanced approach to information collection and sharing for national security purposes. It is useful to consider these components in assessing the privacy policies and practices of airlines more generally. Whether or not airlines deal with personal information in a manner consistent with the above Commitments commended in the Working Party's opinion, will now be considered.

Airline Compliance with CBSA Commitments

To establish whether privacy policy and practice in the airline industry is consistent with the Working Party's Opinion the web site privacy policies of four Canadian based airlines: WestJet, CanJet, Air Canada, and Jetsgo were reviewed.[18]

---

[13] Article 6(1)(c) of Directive 95/46/EC provides that personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."
[14] See art. 8 (1), Directive 95/46/EC.
[15] See ss. 8 and 9 of the Commitments, cited in the Opinion, *supra* note 1.
[16] See ss. 2-15, 16-19 of the Commitments, cited in the Opinion, *supra* note 1.
[17] See s. 30 of the Commitments, cited in the Opinion, *supra* note 1.
[18] Jetsgo ceased operations on or about 11 March 2005. The issue of Jetsgo's obligations regarding personal information about individuals in its possession is not discussed in this paper although the use and

The Issue of 'Push' and 'Pull'

A 'pull' system for transferring data is a system whereby airline passengers' data are directly accessed by the authorities concerned on a continuous basis. A 'push' system, as adopted in the CBSA's Commitments and welcomed by the Working Party, is a system whereby only information submitted by the collecting airline may be received by the CBSA. Under a 'push' system, access to personal data by Canadian authorities is limited to only that which is necessary for the purpose of fighting acts of terrorism. A 'push' system reflects the Working Party's policy that the purposes for processing API/PNR data must bear a clear relationship with fighting acts of terrorism, and that data transferred must be adequate, relevant and not excessive. This policy finds expression in Canadian law through s. 5(3), and Principles 4 and 5 of Schedule 1, of the PIPED Act.

Section 5(3) of the PIPED Act provides that airlines may only collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. What is appropriate depends on consumer expectations of privacy in the air travel industry. Increased security measures in the airline industry since September 11 have arguably reduced air travellers' expectations of privacy. However, it is equally arguable that any collection, use, and disclosure of personal information by an airline is appropriate if it is necessary to facilitate the provision of air travel and other services requested by the consumer, such as customer loyalty program membership and marketing offers.

While the collection of personal information, such as name, address and other contact details, is necessary for the purpose of facilitating air travel and related requested services, the collection of particulars of an individual's computer through "cookies" is arguably not. "Personal information", as defined in s. 2 of the PIPED Act, would appear to include particulars of an individual's computer collected through the use of "cookies". Cookies are small snippets of text code that are placed on a user's computer by a website's server. They allow for a greater personalization of a user's experience on the Internet. Air Canada, CanJet, and WestJet acknowledge the use of cookies to observe user preferences and track traffic patterns on their websites. Air Canada also provides in its policy that it uses advanced "cookie" technology in the form of "Conversion Beacons" (small, simple snippets of HTML code) to track the activity of its subscribers and measure the effectiveness of ads. Moreover, Air Canada's policy suggests that it may be more difficult for consumers to book flights online if their Internet security is set not to accept cookies. The extent to which the collection of information about an individual's computer is necessary for the purposes of facilitating air travel and other requested services is questionable and arguably contrary to the reasonable purpose requirement of s. 5(3) and the policy of the 'push' system reflected in the CBSA's Commitments.

Under Principle 4 of Schedule 1 of the PIPED Act, organizations may only collect personal information for the purposes identified, and should avoid any blanket collection of information. Both WestJet and Air Canada state in their policies that they limit collection of personal information to that which is necessary to fulfil the stated purposes for which the information is required. Jetsgo also specifies in its policy that it "does not

---

disclosure rules of the PIPED Act affect the manner in which Jetsgo uses and releases that information following the cessation of its operations.

gather any personal information for purposes other than those expressly stipulated." In contrast, CanJet's policy does not include any statement to the effect that collection is limited to the purposes identified. It is therefore not certain from CanJet's policy whether its information collection practices are limited to the purposes stated.

Under Principle 5, personal information must only be used, disclosed and retained to the extent necessary to fulfil the identified purposes. This principle mirrors the CBSA requirement to only allow for transfers of a minimum amount of data in terrorism-related cases. Air Canada purports to comply with this policy by stating in its notice that "Air Canada will not use or disclose your personal information for purposes other than those for which it was collected without your explicit consent or as required by law." WestJet similarly purports to comply by stating in its notice that its general policy is to limit the collection, use and disclosure of personal information to the purposes identified. Both WestJet and Air Canada qualify their policies by informing consumers that personal information may be required by security laws to be disclosed to legal authorities without consent. The statements of CanJet and Jetsgo however, do not provide that use and disclosure are limited to particular purposes.

Data Retention Time

The retention policy of the CBSA, as outlined in ss. 8 and 9 of the Commitments, requires data to be retained for 3.5 years and increasingly anonymized. This policy is reflected in Principle 5 of the PIPED Act, which requires personal information to be retained only to the extent necessary to fulfil the identified purposes, and to be destroyed, erased, or made anonymous once the need for it expires.

Air Canada and WestJet provide in their policies that personal information collected by them is retained only for the period necessary to fulfil the purposes for which it was collected. These statements differ significantly from those of CanJet and Jetsgo, which do not provide that retention of personal information is limited to particular purposes and therefore do not clearly delineate the airlines' retention practices. WestJet's policy was the only one to provide that when personal information is no longer needed, it is securely destroyed or made anonymous. The policies of Air Canada, Jetsgo, and CanJet failed to mention procedures for the destruction of information that is no longer required, leading one to question the existence of such procedures.

Data Disclosure/Onward Transfers

The CBSA's onward transfer policy, which requires the level of data protection granted by the receiving country to be one of the criteria to be taken into account in deciding whether to disclose data to other agencies, is also reflected in Principle 1 of the PIPED Act's Schedule 1. Principle 1 dictates that when an organization discloses personal information to a third party, it must employ contractual or other means to ensure that the privacy of the information is protected. Personal information collected by airlines is regularly disclosed to third parties, such as the CBSA and air travel service providers, all of whom require passenger information to facilitate air travel services. However, the existence of contractual arrangements to ensure the continued protection of personal

information transferred to such third parties was only evident in Air Canada's policy. Air Canada's privacy policy is Principle 1-compliant insofar as it specifies that it uses "contractual and other means to ensure that your personal information is afforded protection that meets the requirements of the PIPED Act whenever a third party agent is used to complete some or all of the stages of processing necessary to complete your travel transaction or for research or survey purposes."[19] In contrast, WestJet does not refer to the existence or otherwise of contractual arrangements with third parties to ensure the continued protection of personal information transferred to them. Neither CanJet[20] nor Jetsgo[21] referred to third party recipients of personal information, let alone the means by which transferred information is protected in accordance with the PIPED Act.

A Passenger's Right to Information

Section 21 of the Commitments, which states that the CBSA will provide information to the travelling public regarding its information handling policy and practice, finds is closely aligned with the "openness" principle of the PIPED Act. Airlines are required under Principle 8 to make information about their policies and procedures regarding personal information readily available to individuals. There was significant variation in the extent to which the airlines appeared to comply with this requirement. While Air Canada and WestJet both provide reasonably comprehensive and specific information about their privacy practices and policies, CanJet and Jetsgo maintain policies that provide only general information about their privacy practices. For example, Jetsgo's policy states that personal information is collected for the purpose of accurately processing flight bookings, but it does not specify who the information may or may not be disclosed to, nor does it specify how long the information may be held for. It thereby fails to fully inform customers what they can expect to happen to their information.

The extent to which the policies described the *uses* to which personal information may be put also varied. WestJet provided a comprehensive description of the manner in which personal information would be collected and used, and the purposes of such uses. Air Canada's policy also describes how and why information is collected and used for certain specified purposes, such as arranging travel for unaccompanied minors or persons with special needs, earning points in frequent flyer programs, and signing up for email offers. The policy also clearly states that it may be required by security laws to give border control authorities access to passenger data. Thus, airline customers are clearly informed that their information may be disclosed to customs and immigration authorities of any country in their itineraries.

CanJet and Jetsgo on the other hand specified in very basic terms the purposes of information collection and the intended uses of such information. CanJet's policy addresses disclosures required for national security purposes by providing that information will not be disclosed without the consent of the individual concerned, "unless required by law." Jetsgo's policy fails altogether to mention that it may be legally required to disclose personal information without the consent of the individual concerned.

---

[19] See http://www.aircanada.com/en/about/legal/privacy/policy.html, last visited 11 March 2005.
[20] See http://www.canjet.ca/en_privacy.aspx, last visited 11 March 2005.
[21] See http://www.jetsgo.ca, last visited 11 March 2005.

Such policies do not fully inform consumers of the possible uses to which their information may be put.

Passenger's Right of Access, Correction and Notation

Rights of access, correction and notation with regard to personal information, as provided in s. 29 of the Commitments, are similarly provided in Principle 9 of the PIPED Act. Airlines are required by this principle to inform an individual, on request, of the use, existence, or disclosure of his or her personal information. An individual is entitled to challenge the accuracy of information held by the airline, and if the individual demonstrates the incorrectness or incompleteness of his or her information, the airline must make the necessary corrections.

The four policies in question differed in the manner in, and extent to which, they appeared to provide access to personal information in the relevant airline's possession. WestJet provides contact information through which an individual may obtain access to one's personal information, an opportunity to update that information and an account of the use that has been made of it. The policy provides that requests for information may be required to be in writing and must be accompanied by sufficient information to allow the company to locate the relevant information. Air Canada similarly acknowledges that individuals have a right to access their personal information held by Air Canada and provides a link through which personal information may be accessed on its web site home page. The Air Canada policy also provides instructions on how to access personal information on travel bookings through the Air Canada Call Centre.

In contrast, CanJet provides no details in its policy about the procedure for gaining access to and correction of personal information held by it. A contact address is provided in the policy but no indication is given as to the exact procedure (if any) for requesting and obtaining access to personal information. Jetsgo appears to comply with this requirement by expressly providing in its policy that customers have the right to view any personal information it maintains as well as the opportunity to change it or delete it "if appropriate." It then provides contact information through which an individual can obtain a copy of his or her personal information. The different degrees to which these policies indicate the existence of procedures for gaining access to personal information suggest differences in the actual existence of such procedures.

Conclusion

Analysis of airline privacy policy and practice, as evidenced from the online privacy statements of four airlines, and as conducted in light of the Article 29 Data Protection Working Party's Opinion, reveals an apparent lack of uniformity in the approach taken by airlines to communicating their information handling practices online. More specifically, the online privacy statements of the two discount airlines (CanJet and Jetsgo) fail to indicate the existence of procedures for handling personal information, which is inconsistent with the balanced approach to information collection and sharing required by the PIPED Act, and reinforced in the Working Party's Opinion. Cultivating such a balanced approach through the PIPED Act is difficult in view of the fact that the Office of the Privacy Commissioner, which oversees the implementation of the Act, has few

traditional enforcement powers (such as order-making powers and the ability to fine offenders).[22]

A more accessible means of achieving this balance may be s. 18 of the PIPED Act, which permits the Commissioner to audit businesses and industries for systemic privacy violations. The Commissioner has yet to conduct any such audit[23] and given that the Commissioner has expressed little interest in changing this position, consumer education through public education initiatives is imperative to enforce airline compliance with the policies reflected in the PIPED Act and the CBSA Commitments. If consumers are informed by public education campaigns of their rights under the PIPED Act, they will engage in communications with the privacy officers of the companies they deal with. Such communication will encourage airlines to self-audit, and to adopt a more balanced approach to sharing API/PNR data, in a manner consistent with the CBSA's Commitments and the Working Party's Opinion.

[22] See J. Lawford "Consumer Privacy under PIPEDA: How Are We Doing?" November 2004 (Public Interest Advocacy Centre: Ontario), at 7.
[23] See Lawford, *supra*, at 12.

Banking: "An Evaluation of the Privacy Notices of CIBC and Scotiabank in Light of the Article 29 Data Protection Working Party Opinion on More Harmonized Information Provisions"
by Sapna Mahboobani

This paper compares the online privacy statements of two leading Canadian banks in light of the Article 29 Data Protection Working Party Opinion on More Harmonized Information Provisions, with particular reference to the proposed European information notice solution.

Introduction

The Article 29 Data Protection Working Party ("Working Party") is an independent advisory body on data protection and privacy.[1] In November 2004 the Working Party adopted an opinion aimed at harmonizing information provisions or organizations within EU member states.[2] The opinions of the Working Party are of particular concern in the Canadian context however given the fact that the EU policy of prohibiting the transference of personal data to nations failing to ensure an adequate level of protection.[3]

The adoption of this Opinion signals recognition that industry attempts at communicating information management practices have been unsatisfactory. This requirement of the communication of a company's information management practices finds expression in Canadian law through the Openness principle found in Schedule 1 of the PIPED Act.[4]

This paper examines the online privacy notices of CIBC and Scotiabank in relation to the Working Party Opinion. It also considers the notices of these banks with respect to the PIPED Act.

The Working Party Opinion on Information Notices

The Working Party Opinion on information notices seeks to encourage a consistent approach to informing data subjects about their rights. This approach it contends would ease compliance, improve awareness of data protection rights and responsibilities and enhance the quality of information on data protection.[5]

---

[1] Established pursuant to Art. 29 of Directive 95/46/EC. Its tasks are described in Art. 30 of Directive 95/46/EC and Art. 15 of Directive 2002/58/EC. See www.europa.eu.int/comm/privacy

[2] Opinion 9/2004 of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995", WP 100 of the Working Party, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp100_en.pdf

[3] Within the meaning of Art. 25(6) of Directive 95/46/EC. Shaffer suggests that collective action on the part of the EU countries has provided significant leverage in influencing U.S. data protection law: see G. Shaffer, "The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on U.S. Business Practice."*European Law Journal* 5 (4), 419-437 (1999).

[4] PIPED Act, Sch. 1, cl. 4.8..

[5] Opinion 9/2004 *supra* p. 6.

The proposal is centred upon the comprehension of data subjects and supports the concept of the multi-layered notice format, calling for the acceptance of such notices as constituting legal compliance.[6]

The Opinion contends that the information provided to data subjects should be in a language and layout that is easy to understand and is appropriate for a given audience (e.g. children). The use of multiple layers it is argued, will assist with the quality of information that is provided, better focusing a data subject's query. Taken in sum, this would be taken as acceptable at law.

The Opinion proposes three layers in the notice. The first layer, called the "short notice", would provide individuals with 'essential' information namely the identity of the privacy officer (or data controller) and the purposes of processing (except where readily apparent). The Opinion is forward in its thinking suggesting deployment of 'very short notices' in the case of mobile phones and uses of pictograms where appropriate.[7]

The second layer called the condensed notice would include relevant information as required under the EU Data Protection Directive.[8] This is taken to include:

- The name of the company
- The purpose of the data processing
- The recipients or categories of recipients of the data
- Whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply
- The possibility of transfer to third parties
- The right to access, to rectify and oppose
- Choices available to the individual.

The third and last layer of the information notice would include national legal requirements and specificities.[9] While the last layer of is of no application in the Canadian context, the short and condensed notice may be used as a marker for assessing the on-line privacy notices of Canadian companies. The banking sector is a useful industry for the purpose of this analysis as it is an industry sector purporting to have the highest standards with respect to privacy and a business model based on trust.

The PIPED Act and Banking

As a federally regulated industry the PIPED Act has been of application to the banking sector since its entry into force. The Canadian banking industry consists of 19 domestic banks, 29 foreign bank subsidiaries and 22 foreign bank branches across Canada. These institutions total $1.8 trillion in assets. The customers of the banks number in the millions

[6] *Supra*.
[7] *Supra* at p. 8
[8] *Supra* at p. 8.
[9] *Supra* at p. 9.

including individuals, small- and medium-sized businesses, large corporations, governments, institutional investors and non-profit organizations.[10]

Banks collect personal information regarding the identity of their customers such as name, address and contact information. In addition, banks also retain sensitive financial information about their customers such as accounts they own, their savings, investments, credit, and debts and even people's social insurance numbers ("SINs") that they collect for income reporting purposes.

At common law, banks are bound by fiduciary obligations owed to their customers. These duties are no doubt part of the reason that the banking industry was among the first industries to go beyond a statement of principles and develop a comprehensive privacy code of conduct in 1986. This code was updated regularly in keeping with the changing requirements of the customers' privacy needs. In fact, many of the principles in the banks' privacy codes translated directly to the principles of the PIPED Act.

After the implementation of the PIPED Act, there was little noticeable change to the procedures of the banks, as the PIPED Act's guiding principles were already reflected in the voluntary codes that the banks had already been following.[11]

Findings of the Office of the Privacy Commissioner

Given the culture of respect in the banking industry for privacy, one would have expected little or no complaints under the PIPED Act to the Office of the Privacy Commissioner (OPC). However, banks were the respondents in 118 findings out of the 255 made up to January 1, 2004, representing 46% of the findings. These findings dealt with improper account access, use and disclosure, secondary marketing, over collection of personal information, income reporting questions, security problems, access problems, credit reporting and SIN usage.[12]

For example in PIPED Act Case Summary #46,[13] a bank was accused of inappropriately demanding birth dates from applicants. The customer claimed that the bank required inappropriate information – her birth date – when she tried to open an account over the phone. When she inquired about the use of the birth-date, the representative over the phone told her that it was needed for income reporting purposes. Dissatisfied with the answer, she raised her concern to a bank supervisor, who informed her that the birth-date was indeed required, though not for income reporting purposes, but as identification information when the customer subsequently contacted the bank. The customer objected to this, stating that the bank already had other information such as the SIN, and should not be collecting information that could be used for demographic identification. The

---

[10] Canadian Bankers Association, "Consumer Information – Consumer Protections" a*vailable at* http://www.cba.ca/en/ViewDocument.asp?fl=3&sl=65&tl=133&docid=294 (2005).
[11] Canadian Bankers Association– Our Industry – Banks in Canada, retrieved March 21, 2005 from http://www.cba.ca/en/section.asp?fl=2&sl=204&tl=&docid= (2005).
[12] John Lawford, "Consumer Privacy under PIPEDA: How are we doing? November 2004 (Public Interest Advocacy Centre: Ontario) *available at* http://www.piac.ca/PIPEDAReviewFinal.pdf.
[13] Bank accused of inappropriately demanding birthdates from account applicants see: http://www.privcom.gc.ca/cf-dc/cf-dc_020426_e.asp

commissioner found that the bank was in violation of Principle 4.3 which states that the organization should collect solely the information that was required for the stated purpose, and felt that the bank had enough information to identify the customer without having to collect information. The bank was also found to be in violation of section 5(3) which states that the organization may collect, use or disclose information for only those purposes that a reasonable person would consider appropriate.

In case summary #105,[14] a customer objected to the bank's use of the SIN for credit card activation. Banks collect the SIN number in compliance with the Canada Customs and Revenue Agency's income reporting requirements. The bank had collected the SIN information when the customer had opened an interest bearing account. The customer felt that the SIN data should not be shared between the databases for the two accounts. And that by using the SIN as identification for credit card activation, the bank was using information for a purpose not previously defined. The Commissioner found the bank in violation of Principle 4.2.4 for not informing the customer of the intended use of the SIN and not gaining the customer's consent. The bank was also found to be in violation of principle 4.3.2 for not making reasonable effort in informing the customer of the new intended use of the SIN and in violation of Principle 4.5 for using the SIN data for a purpose not previously identified and without the customer's consent.

The OPC makes available the findings of PIPED Act complaints on its web-site, however there are still limitations to the kind of information that can be obtained. The names of all parties in the case are withheld. Therefore, on reading the cases, one does not know which banks were involved, and subsequently, it is difficult to gauge if the recommendations made by the commissioner have been followed. In some cases, the wording in the privacy policy suggests that changes were made based on the findings of a particular case.[15]

The PIPED Act is modeled on a complaint driven process. It is up to the aggrieved consumer that feels his or her privacy has been violated to bring the case to the attention of the OPC for investigation. This in large part is dependent on the wherewithal of the individual consumer. The number of complaints is therefore unlikely to be in line with the number of actual breaches of privacy taking place in this industry sector.

Privacy Statements: Short and Condensed Information Notices

In light of the difficulties consumers have vindicating their rights, the EU policy on information notices would appear to be a departure from the consent model of privacy.[16] A comparison of the privacy notices of CIBC and Scotiabank would tend to suggest that Scotiabank is more aligned than CIBC with the position of the Working Party. This is because the privacy policy of Scotiabank follows a layered approach, with the bank's

[14] Customer objects to bank using Social Insurance Number to activate credit cards see:http://www.privcom.gc.ca/cf-dc/cf-dc_021219_8_e.asp

[15] For example, the paragraph on SIN usage in CIBC's Privacy Policy seems to suggest that it was added as a result of Case Summary #105 *supra*.

[16] A discussion of this matter is beyond the scope of this paper and a matter for further research.

"Privacy Code"[17] presented to the user in three layers, though the format does not correspond to the Working Party's notion of a layered notice.

Scotiabank provides a three-layered notice whereby the short notice provides an overview of the scope of the code and a link to the Ten Principles of the Code, as modeled on the Canadian Standard Association's (CSA) Model Code for Protection of Personal Information.

The "condensed" layer provides a brief definition of each of the ten principles of the code. The next layer (obtained by clicking on the corresponding principle) provides a detailed description of the corresponding principle and Scotiabank's implementation of each principle.

CIBC's Privacy Policy, by contrast, is in a long notice format, with the complete privacy policy displayed on a single scrollable screen.

Scotiabank's Notice

The requirements of the suggested Working Party short notice are that information notices should provide information about the identity of the data controller (privacy officer in the Canadian context) and the purposes of processing. Additionally, there should be a clear indication as to how the individual can access additional information. While Scotiabank's Privacy Code does acknowledge the fact that senior management of each Scotiabank Group Member is accountable for the data that is collected, and that a person or persons who is responsible for the overall privacy protection and compliance of the collected information will be identified to the customer (Principle 1), it does not explicitly provide the identity of this purpose in this document. This information is, however, provided in the Privacy Brochure under "The Need for Security" as the Secretary of the Privacy Committee, along with a mailing address.

The purposes for which the information is collected is provided under Principle 2 – Identifying the Purposes for Collecting Personal Information. It states that the information collected is limited to the following purposes:

- To understand the customer's needs.
- To analyze the suitability of products or services for the customer.
- To determine the customer's eligibility for products and services.
- To set up, manage and offer products and services that meet the customer's needs.
- To provide ongoing service.
- To meet legal and regulatory requirements.
- With regards to insurance products to investigate and adjudicate insurance claims.

No information is provided on the exact nature of the information required for any of these purposes, though the Privacy Code does state that the purpose of use of the information will be provided to the customer at the time the information is collected, and in a manner that the customer will understand. The Scotiabank Group staff member will

[17] Scotiabank Privacy Code, *available at* http://www.scotiabank.com/cda/content/0,1608,CID8311_LIDen,00.html

be able to explain the purposes to the customer, who will be able to ask for information about the uses.

The Privacy Code also states that purposes that are not directly obvious will be explained to the customer at the time of collection of the information. This includes uses for references, SIN, credit information, medical information, claims and insurance history, and information regarding accounts among others.

The Privacy Code further states that the customer can access the personal information that the bank holds upon "written request", and obtain a list of third parties to whom the information has been disclosed (Principle 9). Policies and procedures are in place to make this information available to the customer, and these policies and procedures will be disclosed to the customer when requested. The information provided to the customer will be as specific as possible in terms of information on file, to whom the information has been disclosed and when and how the information was disclosed. This information will be provided to the customer free or at a cost commensurate with the effort required to retrieve the information.

As required by the suggested Working Party condensed layer, the Privacy Code should provide the name of the company, the purposes of the data processing, the recipients of the data, the reply mechanism, possibility of transfer to third parties, possibility to rectify, access and oppose information held by a company, and the choices available to the individual. Additionally, information regarding redress within the company or through the nearest data protection agency must be provided. As such, throughout the privacy code, the company is referred to as the Scotiabank Group Member. The definition of Scotiabank Group Members is provided in the short notice as "companies engaged in the following services to the public: deposits, loans and other personal financial services; credit, charge, debit and payment card services; full-service and discount brokerage services; mortgage loans; trust and custodial services; insurance services; investment management and financial planning services; and mutual funds investment services." Further, as collectors of customer personal information, these Scotiabank Group Members are the recipients of the information.

The Privacy Code states that Scotiabank will be as specific as possible about where they obtained the information, to whom the information was disclosed and how and when the information was disclosed. This information will be obtained from the customer records and will be presented to the customer in a form that will be easy for the customer to understand, with explanations of abbreviations and codes. The Privacy Code, however, does not specify what this form may be. The reply will be made within a reasonable time, though this time is not defined. The reply will also be made free to the user or at a cost commensurate with the effort required to obtain the information. In cases where a cost is to be incurred by the customer, the customer will be informed of the possible charge with the option to withdraw the request.

If a request for information is denied, the customer will be informed of reasons of this decision, unless prohibited by law. The customer can challenge this decision. The customer may also challenge the reasonableness of the cost of providing personal

information. The complaint resolution process and the person whom the customer needs to contact in such an event is part of the procedures of Scotiabank (Principle 10).

The privacy code however, does not provide any concrete information on this process or contact information, implying that it is available to the customer in a format easy to understand. The Privacy Code further states that the Scotiabank Group Member will investigate all complaints that it finds justified, and attempt to resolve it. If need be, changes will be made to the policies and procedures to ensure that other customers are not inconvenienced in the future. The customer is also encouraged to pursue other resources if he is not satisfied with the way a complaint is resolved. These different avenues are available to the customer through the Scotiabank branch and are not provided in the Privacy Code. The Privacy Code does state that the customer may file a written complaint with the Federal Privacy Commissioner if he feels that the Scotiabank Group Member's operations are not in compliance with the code.

The Privacy Code states that the customer will be informed at the time of collection, that his information may be passed on to other Scotiabank Group Members or affiliates to market other products. The customer's consent, however, is required for this, and the customer has the option to withdraw consent (Principle 3). The Privacy Code also provides information for cases where the customer's consent may not be obtained before disclosing information to third parties. While Scotiabank records most disclosures to third parties, the Privacy Code also outlines situations in which disclosure of information to a third party is not recorded in the customer's file. These include disclosing information for routine maintenance such as cheque printing, reporting to CCRA, updating of credit information, and underwriting or claims processing. Nowhere in the Privacy Code are the third parties listed, though the code does indicate that the customer could request the information from Scotiabank.

Customers are informed that the Scotiabank Group Member will keep personal information accurate and current. The customer may challenge the bank in writing if any of his information held by the bank is inaccurate or incomplete, and request that the information be amended. The bank also relies on the customer to keep certain information like contact data current. Scotiabank will revise its inaccurate information and inform all third parties that could use this information. The customer is also given the option to challenge the bank if it refuses to amend the incorrect information that it holds.

CIBC's Notice

CIBC's privacy notice does not follow a layered format.[18] The policy is presented on a single, scrollable screen. The requisite information is provided without the need for embedded weblinks. Discussion of CIBC's privacy policy is therefore done in relation to the actual content of the policy, rather than the layered property of the notice.

The purposes for data collection are stated as follows:

- Establish your identification;
- Protect you and us from error and fraud;

[18] CIBC Privacy Policy, *available at http://www.cibc.com/ca/legal/privacy-policy.html*

- Understand your needs and eligibility for products and services;
- Recommend particular products and services to meet your needs;
- Provide ongoing service; and
- Comply with legal requirements.

These purposes are broadly defined and do not mention the kinds of information required. The special case of the SIN is illustrated as required for tax reporting purposes, and can be used – with the consent of the customer – for identification purposes.

The privacy brochure broadly defines other recipients of the customer's information as outside companies that may be used to process the data, and a court of law, or other regulatory authority for legal reasons. It is also stated that information will be shared within the CIBC group, as permitted by law. No other recipients or categories of recipients are identified.

The CIBC privacy policy also states that the customer's consent will be obtained before information about him is collected or used. Certain cases are explicitly specified such as checking employment, obtaining a credit report, offering products and services and making it available (subject to legal restrictions), to other CIBC groups.

Consent is also obtained before collecting the SIN. The policy also states that consent can be implied or explicit, and the customer can withdraw consent after he has given it. Special mention is made with regards to credit reporting – the customer cannot withdraw consent to allow the bank to update the credit bureau as long as the customer has credit with the bank.

The policy also provides that if the customer does not provide consent for the collection and use of certain information, the bank will not be able to provide certain products and services to the customer. While these situations are not explicitly described in the policy, it does state that the customer will be advised at the time of collection of the information. The customer can also withdraw consent from receiving direct marketing material, but this does not limit the information that the customer receives with their monthly statement or in discussions with the personal banker or customer service representative.

In addition the CIBC Privacy policy explicitly states that the customer's consent is obtained before sharing information with third parties. This includes all subsidiaries within the CIBC group. The policy mentions outside companies that provide the expertise to process the information, information that is released to third parties for legal reasons and in circumstances to protect the interests of CIBC. While the policy assures the customer of the standards employed while ensuring the security of the information, the policy does not explicitly identify companies or organizations to which information could be disclosed.

The customer is informed that he can access his information and verify its accuracy. This request may be asked to be put in writing. The policy also states that certain information may not be made available to the customer, but does not elaborate on what types of information are covered.

The customer can also request the names of persons and companies that the bank had shared the customer's information with. However, this does not include third party companies that do work for the banks like cheque printers, or T5 reports to Revenue Canada or regular updates to the credit bureau. All requests will be responded to within 30 days, with explanations provided for delays, if any. CIBC will also correct any information that the customer feels is inaccurate. If the bank has obtained incorrect information from a credit bureau, the bank will provide the customer with the contact information of the concerned party so that the customer may have his or her information corrected.

The customer is also provided information on how to make complaint. Three steps are provided – talking to the bank directly, contacting customer service and contacting the ombudsman of the bank.

While both banks provide the customer with information on how the data is collected and used, the form of presentation and content of this information is not, at present, in compliance with the Working Party requirements for information notices.

Implementing Layered Notices

Online privacy notices differ vastly between different companies, even those in the same sector. Scotiabank and CIBC are both major players in the Canadian banking sector yet their approach to informing their customers about their information rights varies greatly. These notices are in themselves difficult for the customer to grapple with. Furthermore, it is difficult for the customer to make comparisons between notices of the different banks, to assess the information practices of the different companies. This is largely due to the difference in use of language, amount of information presented to the customer, and the way this information is structured.

The Working Party proposes that the language and layout used in online information notices should be simple to understand and geared toward the target audience. The proposal also stresses multi-layered formats for simplicity and consistency in information notices. The adoption of such a proposal in the banking sector would mean that online information notices would be consistent enough with each other to allow customers to do a quick and easy comparison of the banks' practices. If all banks, and other industries, followed the same format, they arguably would lead to an increase in customers' awareness of their data protection rights as they see certain types of information regarding their data repeated in different company notices. In addition this practice would force companies to play by an agreed set of rules with respect to how an organization's information management practices are communicated to the public.

With information provided to the customer in multiple layers, allowing the customer to control the amount of information he needs, the online information notices would appear less intimidating and daunting, and would encourage customers to study the more important and relevant details of notice.

For layered notices to be most effective, the banking industry needs to arrive at a common template. Most banks collect the same types of information, and use them for the same purposes. However, there may be differences with respect to how the banks handle the processing of their customers' information and disclosure of information within their subsidiary groups. While a comparison of the information notices of these banks should make these differences apparent, the layered notice template that is used needs to be flexible enough to allow for this. As has been seen by the examples of the two banks, the purposes of data collection as reported to the customer tend to differ, even though both banks provide the same services to their customers.

A consistent format for reporting purposes of collection will need to be developed that provides the customer with enough information on why the banks collect information. The question of understandable language is subjective, and needs to be addressed so that all banks are consistent. This would make it easier for the customers to distinguish between the practices of different banks.

The information required of the different layers as suggested by the proposal would need to be revised when applied to the information notices of the banking industry in Canada.

Conclusion

In the case of banks the PIPED Act Openness principle suggests that organizations should be forthcoming about their procedures and policies with respect to how information is collected, used and disclosed. Companies give effect to this provision through a mixed array of brochures, fine print on application forms and online notices. This puts the organization in the position of educator and adversary since there are instances where disclosure will not be in the company's best interest or the customer wishes to hold the organization accountable for failing to honour its commitments.

The Working Party proposal on information notices would consolidate the process of disseminating information about its information management practices as well as provide the banks with a consistent means of implementing the PIPED Act Openness principle in the online context.

By providing the banks with guidelines on how relevant information needs to be presented to customers, it removes some of the decision making process from the bank itself, making it easier to formulate an understandable privacy notice. As such, the Working Party proposal serves as a good complement to the Openness principle in educating customers about their privacy rights.

Retail: "An Industry-Specific Approach to Privacy Statements in the Retail Sector"
by Aniz Alani

The purpose of this report is to examine issues concerning the protection of personal information within the retail business sector in Canada and, in particular, the extent to which retail businesses' web site privacy statements address these concerns.

Introduction

As of January 1, 2004, the PIPED Act purports to apply to virtually all organizations engaging in commercial activity, including retail businesses carrying on businesses entirely within a single province. The PIPED Act does not apply, however, in provinces where "substantially similar" legislation has been enacted. British Columbia, Alberta, and Quebec have passed substantially similar privacy statutes. The PIPED Act continues to apply, however, in all cases where personal information is transferred outside of a province.

For the purpose of this report, "retail business" includes any organization which engages in the sale of commodities or goods to an ultimate consumer.

It is noteworthy that the PIPED Act does not distinguish between industry sectors except to the extent that some sectors, such as airlines, banking, and telecommunications, are considered to be federal works and undertakings. The federally regulated industry sectors are clearly within the legislative jurisdiction of the Parliament of Canada under s. 92(10) of the *Constitution Act, 1867*.[1] The application of the PIPED Act to the retail sector has been particularly controversial because, unlike federal works, businesses and undertakings, retail businesses operating entirely within a province are governed by provincial legislation with respect to "property and civil rights" under s. 92(13) of the *Constitution Act, 1867*.

The Government of Canada has very clearly expressed its view that the PIPED Act is a valid exercise of Parliament's legislative jurisdiction in areas of trade and commerce under s. 91(2). Former Minister of Industry John Manley made the following remarks in the House of Commons with respect to jurisdiction over the PIPED Act:

> The bill is a legitimate exercise of the federal government's authority to legislate in respect of trade and commerce in Canada. The increasing ubiquity of networks and the speed of the technology means more companies are collecting more information, circulating it more widely and combining it more ingeniously than ever before.[2]

In order to ground the PIPED Act as a valid exercise of Parliament's authority over trade and commerce, specifically in areas otherwise falling within provincial jurisdiction, the following five conditions must be satisfied: (1) it is part of a general regulatory scheme; (2) the scheme must be monitored by the continuing oversight of a regulatory agency; (3) the legislation must be concerned with trade as a whole rather than with a particular

---

[1] *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II, No. 5.
[2] Government of Canada, Debates of the House of Commons (Hansard), No. 9 (22 October 1999) at 1100, online at http://www.parl.gc.ca/36/2/parlbus/chambus/house/debates/

industry; (4) the legislation should be of a nature that the provinces jointly or severally would be constitutionally incapable of enacting; and (5) the failure to include one or more provinces or localities in a legislative scheme would jeopardize the successful operation of the scheme in other parts of the country.[3]

The constitutional validity of the PIPED Act, specifically whether it represents a valid exercise of Parliament's authority under the general trade and commerce power, has been challenged by the Government of Quebec. A reference question on this issue has been submitted to the Quebec Court of Appeal.

Without addressing the merits of the constitutional arguments in any depth, it is noteworthy that one of the five requirements under the general trade and commerce power under *General Motors of Canada Ltd.* v. *City National Leasing* is that the legislation be concerned with trade as a whole rather than with a particular industry. Because the legislation cannot be industry-specific, there is very little opportunity for *the PIPED* Act to provide for significant exceptions in terms of the organizations to which it applies.

The PIPED Act does not distinguish between small businesses and larger chain operations. Instead, it imposes positive privacy obligations on all organizations conducting commercial activity in Canada. Despite the economic reality which makes it more difficult for an independent retailer than a large retail chain store to learn its obligations about the PIPED Act, devise a privacy policy, implement suitable privacy practices, and develop an infrastructure for responding to customer access and correction requests or complaints, the PIPED Act appears to impose the same duty on each indiscriminately. Instead, every commercial organization, regardless of its age or size, is required under the PIPED Act to comply with specific positive obligations. Although this study focused on companies with privacy statements posted on their Internet websites – incidentally, a subset of commercial organizations which enjoys relative expertise and sophistication vis-à-vis independent small business owners – there is an apparent vacuum of privacy knowledge and awareness at the level of small business. If the protection of personal information is, as stated, the purpose at which the PIPED Act is aimed, additional steps must be taken to ensure the PIPED Act is enforced broadly across all organizations which purportedly fall under its application. If the PIPED Act were only taken seriously by or in respect of relatively large commercial organizations, the federal government would likely lose its claim to jurisdiction under the general trade and commerce power since it would no longer concern trade as a whole. Privacy itself is arguably a matter of property and civil rights and thus an issue of provincial jurisdiction. It is only by addressing privacy as a general trade issue that the federal government has been able to assert jurisdiction over privacy protection. The alternative argument, which is not explored in this paper, is that the protection of personal information is a matter of national concern and thus a valid exercise of Parliament's jurisdiction to legislate for the "peace, order and good government of Canada" under s. 91.

Until the federalism issues have been definitively resolved by the courts, consumers and businesses must be familiar with applicable privacy legislation at both the federal and

[3] *General Motors of Canada Ltd.* v. *City National Leasing*, [1989] 1 S.C.R. 641 at 663.

provincial level. Of possible interest for future research is the manner in which businesses operating in multiple jurisdictions have adapted their privacy statements and practices to comply with issues of overlapping jurisdiction.

Methodology

In order to acquire information about retail organizations' privacy practices, I contacted 19 companies by e-mail, inviting the privacy manager at each company to participate in our privacy study. A comprehensive questionnaire was prepared, which was intended to solicit generally objective indicators of companies' privacy practices. As part of the invitation process, I selected 19 retail organizations with internet websites. I then located the e-mail address listed for each company's privacy manager, and submitted a standard form invitation letter to the address.

Companies Contacted

The following 19 companies were contacted with requests to participate in our study: Future Shop, RadioShack Canada, Staples, Office Depot, Indigo, Hudson Bay Company, Holt Renfrew, eBay, London Drugs, Black's Photography, CanadaFlowers.com, Pizza Pizza, CanadaHelps.org, The Shopping Channel, Henry's, Starbucks, Tim Horton's, McDonald's Restaurants of Canada, and Subway.

Responses

Of the 19 companies contacted, the following 5 companies responded by e-mail expressly declining to participate in our study: Indigo, London Drugs, Radio Shack, Future Shop, and Black's Photography. Only one company, McDonald's Restaurants of Canada, agreed to participate in the study. The 13 remaining companies did not respond to the invitation in any manner.

Role of the Privacy Statement Within Privacy Policy

Although a focus of this privacy study was to examine retail businesses' privacy policies as published on internet websites, it is clear that a website privacy statement forms only a part of a company's overall privacy policy. Essentially, a website privacy statement describes a company's general policy with respect to its use, collection and disclosure of personal information within the course of its commercial activity. As described below, the language of website privacy statements is typically vague, leaving a reader with very little information about a company's privacy policy beyond what is already generally provided under the PIPED Act. Of far greater use to consumers is a company's detailed implementation manual, which typically describes specific examples of when a business practice engages a privacy interest and is affected by the company's obligations under the PIPED Act.

As part of my interview with McDonald's, I had the benefit of reviewing an implementation handbook prepared for internal use by McDonald's Restaurants of Canada Ltd. The handbook contains an itemized explanation of the company's privacy principles (mirroring those recognized in the PIPED Act) and a description of how each

privacy principle is reflected in the day-to-day operations. Also included are hypothetical fact patterns describing situations in which privacy obligations may operate and how a store manager or employee might respond to the situation within the spirit of the company's privacy policy.

The level of detail included in the implementation handbook is certainly in contrast to the level of abstraction used generally in published privacy statements. By making this observation I do not intend to discourage the use of broad privacy statements. Indeed, privacy statements serve a useful purpose insofar as they generally inform readers about a company's macro-level commitment to privacy protection and compliance with the PIPED Act. Instead I suggest that companies be encouraged to publish or make available handbooks or implementation guides similar in scope to the operational manuals published by government with respect to administrative procedures for access to information legislation.[4]

The PIPED Act requires that "organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable."[5] The Act further provides that the information made available shall include "a copy of any brochures or other information that explain the organization's policies, standards or codes."[6]

Relying on this provision, an individual may request a company to provide a detailed implementation guide setting out the recommended practices or policies with respect to specific examples of personal information use by the particular company. However, companies would be understandably reluctant to provide this information for two main reasons.

First, the preparation of a detailed implementation guide represents a significant investment by the company of its time and resources. Sharing this information with the public may be seen to deprive the company of an acquired competitive advantage over another company which has not made the same investment.

Second, the publication of specific practice recommendations may be seen to expose a company to increased liability arising out of legal obligations created not by the PIPED Act but by the representations in the publication itself. Adopting this rationale, a company would be well advised to limit its publicly available policy statements so as to minimize the creation of any obligations not already imposed by the PIPED Act. While this concern would appreciably explain the typically vague language used in published privacy statements, it does little to assuage individuals' concerns about what specific steps a company is taking to protect individual privacy. If the privacy policy equates to confirming minimal compliance with the PIPED Act, there is arguably less benefit to

[4] See, for example, "Guidelines for the Routine Release of Records Information", October 1997: http://www.mser.gov.bc.ca/privacyaccess/main/rr_guide.htm
[5] Principle 4.8.1.
[6] Principle 4.8.2(d).

requiring each company to publish a broadly worded privacy statement since the reader can otherwise assume the company is aware of and intends to comply with its general obligations under the PIPED Act.

Specific Privacy Considerations in the Retail Sector

In this part, the means by which retail businesses typically collect and use personal information will be reviewed. Where these means are used, a company should specifically address them in a publicly available privacy policy. The alternative to specifically referring to each is to leave the consumer uncertain as to whether the company has recognized the information collection as one which engages a privacy interest.

Customer Feedback/Complaint Forms

For some retail organizations in which the exchange of personal information is not necessary to complete a transaction, the collection and use of customer feedback forms may form a significant proportion of a company's personal information inventory. Customer feedback forms typically invite consumers to rate their level of satisfaction with their shopping experience in a number of specific areas. Where the consumer requests that the company respond to the feedback, the consumer is invited to provide his or her contact information. In such cases, the exchange of personal information is clearly voluntary as the consumer's knowledge and consent of the collection and use is apparent when the feedback form is completed. A lingering privacy concern, however, exists with respect to the purposes for which the personal information is subsequently used and disclosed.

While all privacy statements examined during this study contained language restricting the use or disclosure of personal information for purposes other than those for which the information was collected, the typical absence of specific examples mentioned in privacy statements leaves the reader to assume that the company and the reader share identical views on which exchanges of personal information are governed by the privacy policy or applicable privacy legislation.

McDonald's specifically identifies the use of customer feedback forms and addresses the various privacy interests engaged by their use. For example, the McDonald's privacy principles speak to the use, disclosure, accuracy and security of personal information provided in customer feedback forums. Other companies' privacy policies, including companies known to use customer feedback forms, do not specifically address how the personal information contained in these forms will be used or disclosed by the collecting company.

To the extent that a company actively invites consumers to provide feedback on the company's performance, the company's privacy policy should specifically address the limited purpose for which the information contained on the customer feedback form will be used by the company, as well as how the information will be stored, disclosed, and disposed of when it is no longer needed.

Returned Merchandise

Retail businesses should review in-store return policies in light of privacy legislation. When a customer attempts to return merchandise to obtain a refund or exchange in accordance with a store's return policy, it is still the case that the customer is asked for identifying personal information as part of the return process. A customer's contact information is reasonably related to the return process since the company may need to contact the customer in case the returned product has suffered undisclosed damage disqualifying the product for a refund under the store's return policy. Personal information would not be necessary for this purpose, however, if the clerk processing the return performs an adequate inspection of the returned merchandise in the presence of the customer.

Where a company routinely requests a customer's contact or other personal information as part of its return policy, what is the effect of a customer's refusal to consent to the exchange of this personal information? Since "an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes",[7] it is doubtful an organization can refuse to provide a refund or exchange where a customer reasonably withholds consent to providing the requested personal information. If the store's purpose is indeed to retain contact information in case there is a latent problem with the returned merchandise, this purpose should be made expressly clear to the customer at the time of the return. Moreover, the retention of the customer's contact information, along with any additional information including the reasons provided by the customer for returning the product, should only be kept by the company for a reasonably brief period of time sufficient to discover any undisclosed problems with due diligence. This recommendation is not intended to create a limitation period for nefarious individuals attempting to obtain a refund for illegitimate purpose, but rather to reflect the reality that retail businesses ordinarily do not collect or retain identifying information about an individual when he or she *purchases* a product and therefore should not be granted a broad licence to collect such information when an individual *returns* a product.

Contests and Business Card Draws

A common marketing technique used in retail organizations is to offer customers a contest awarding free products. Customers enter by providing a business card or completing an entry form requesting contact information. The ostensible purpose for collecting the personal information as part of such contests, and accordingly the grounds on which consent may be implied under principle 4.3.7, is to allow the collecting organization to contact the winner to make prize arrangements. Once the information has been collected, however, the collecting organization has obtained contact information from its clientele.

Determining the purposes for which the organization may legitimately use this information, assuming an express statement of purpose was not included on the entry

[7] Principle 4.3.3, PIPED Act.

form, depends on what a reasonable person would consider appropriate at the time of collection. If a company intends to subsequently use the collected information for marketing purposes, the company should expressly state such purpose at the time of collection.

In the context of company websites, consumers are often offered opportunities to enter contests which require the collection of personal information. In addition to the entrant's contact information, the entry form may request additional information concerning the entrant's shopping preferences, income and education levels, and other information not necessary to administer the contest itself.

An example of an effective privacy statement with respect to contests and surveys is found in Future Shop's privacy policy:

> **Participate in a Contest, Promotion, or Survey**
>
> From time to time, we may run contests, promotions, or surveys. If you participate, you may be asked for contact information as well as additional optional survey information (for example, product preferences). Information from contest entries will be used to contact you if you win. We may also summarize survey information in a manner that no longer identifies the contest entrants for analysis, but will not share personal information from entries. All contests are subject to rules that will be available with each particular contest.[8]

Rebate Forms

Occasionally, a retail store selling a product which includes a manufacturer's rebate will offer to process and submit the rebate forms necessary to receive the rebate amount. In such cases, the retail store will necessarily collect personal information from the consumer including a mailing address and other details concerning the purchase. In such cases, the retail store is obliged not to use or disclose the collected personal information for any purpose other than for processing the customer's rebate claim. Since the information is no longer necessary for this purpose once the claim has been submitted to the manufacturer offering the rebate, the store's policy should provide for the timely and secure destruction of the rebate information.

An example of a privacy policy statement with respect to rebate programs is found on the Future Shop website:

> **Rebates**
>
> Many of the products you purchase through Future Shop are offered with rebates. To claim your rebate, you will usually be asked to provide your name, address, e-mail address and proof of purchase. You may also be asked by either Future Shop or the vendor to provide your consent to be added to promotional mailings and newsletters. Your consent is not a condition of receiving the rebate.[9]

Warranty Programs

[8] http://www.futureshop.ca/informationcentre/en/privacypolicy.asp
[9] http://www.futureshop.ca/informationcentre/en/privacypolicy.asp

Similar to rebate programs, some retail businesses offer customers a service which facilitates product registration for warranty program purposes. While the standard recommendation with respect to limited retention of personal information by the retail business applies with equal force as it does to a company's handling of rebate information, there is a particular concern where businesses offer a supplementary or extended warranty program beyond that provided by the product manufacturer.

For an additional cost, some retail businesses particularly in the home electronics sub-sector will offer consumers an opportunity to supplement a manufacturer's warranty with a policy that provides technical support and/or damage protection. For example, Future Shop offers a "Product Service Plan" on virtually all products sold through its retail outlets or online store.[10]

Where a retail business administers its own extended warranty program, information regarding coverage is typically connected to the individual purchasing the product. Future Shop requests the name, address and telephone number of the individual registering the warranty coverage. When a customer attends a retail outlet to request warranty service under the Product Service Plan, the customer is asked either for a store receipt or for the individual's phone number to facilitate a computer search of registered warranty information. Prior to the implementation of PIPED Act within the provincially-regulated retail sector on January 1, 2004, Future Shop routinely collected contact information from customers during every purchase. As part of Future Shop's privacy compliance program, customers were thereafter only asked for personal information when purchasing the Product Service Plan extended warranty coverage. The information recorded includes the serial number of the specific product to which the extended warranty coverage applies.

Given the uniqueness of the serial number, which prevents individuals from obtaining extended warranty service for additional products, it is arguably unnecessary to additionally collect the individual's personal information to facilitate the computer search of warranty records. Instead, the company could conduct a search by serial number of the product submitted for warranty coverage, thus enabling the consumer to obtain warranty service while retaining relative anonymity.

Interestingly, the Future Shop privacy policy makes little mention of its use of personal information in connection with its warranty program. As part of its privacy statement in respect of in-store purchases, Future Shop describes the following policy:

> **In-Store Purchases**
>
> When you purchase a Future Shop product or service, you may need to provide us with contact and payment information (such as credit card information) so that we can process your request. Examples where we need contact information include delivery services, product servicing, in-home installations, warranty coverage, and rebate requests. If we collect this information, we will also ask for your consent to use this information to send you promotional information on products and services.[11]

[10] http://www.futureshop.ca/informationcentre/en/psp_faq.asp
[11] http://www.futureshop.ca/informationcentre/en/privacypolicy.asp [emphasis added].

In the privacy statement provided above, Future Shop expressly identifies warranty coverage as a service mandating an exchange of customers' personal information. There is no mention of the personal information being used later to identify and match the product to which the extended warranty applies.

The statement is also unclear with respect to why contact information is necessary to provide warranty coverage. It may be necessary only to inform the individual of future amendments to the warranty agreement, but the lack of specificity as to purpose deprives the individual of the benefit of knowing based on the privacy policy alone whether withholding consent precludes the purchase of extended warranty coverage. The closing sentence, which notifies consumers that personal information necessarily collected for the preceding purposes may later be used with consent to send promotional information, calls into question the extent to which the company has actively minimized its information collection practices.

Conclusion

Privacy statements appear with increasing regularity on websites of companies in the retail sector. As with their counterparts in federally regulated sectors, the privacy statements produced by retail organizations typically describe privacy practices in general, abstract terms. This paper addresses some of the privacy issues specifically relevant to the retail sector as well as provides recommendations for how retail businesses might expand their privacy statements to reflect industry-specific privacy concerns. Striking the right balance between specificity and flexibility may continue to reflect a tension between openly disclosing a company's detailed privacy practices and maintaining the maneuverability provided by non-specific privacy statements affirming the general principles recognized by the PIPED Act. If the business community can overcome concerns with respect to the competitive advantage lost or the liability increased by publishing detailed privacy manuals, consumers will benefit by having a meaningful basis on which to assess companies' privacy practices, hold them accountable for non-compliance, and ultimately guide their purchasing decisions. Until then, consumers may need to rely on their own interpretations of PIPED Act and the goodwill of retailers to comply with the spirit of the legislation and the similarly non-specific finding reports published by the Privacy Commissioner.