CONSUMER PRIVACY UNDER *PIPEDA*: HOW ARE WE DOING?

Written by John Lawford

Research by Howard Simkevitz

Public Interest Advocacy Centre
1204 – ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

November 2004

With Funding from Industry Canada

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, ON
K1N 7B7

Canadian Cataloguing and Publication Data

Lawford, John

Consumer Privacy Under *PIPEDA*: How Are We Doing?

ISBN 1-895060-65-6

Executive Summary

This report assesses the efficacy to date of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), and identifies significant gaps and grey areas in the data protection regime, from the consumer perspective.

All relevant findings of the Privacy Commissioner to the end of October 2004 were considered to create an update, nearly four years after implementation of PIPEDA, on how it protects consumer privacy in the marketplace. As a practical exercise, this report revisits the targets of complaints filed by the Public Interest Advocacy Centre (PIAC) against major corporations for not properly obtaining consent to secondary marketing. This analysis shows continuing problems with these corporations' use of "implied consent" obtained by "opt-out" mechanisms.

This report concludes that PIPEDA is a sheep in wolf's clothing. As a general rule, PIPEDA has not been kind to consumers. Personal experience with the finding process has been painful, especially amongst those who found that they had to take findings of the Privacy Commissioner to Federal Court for "enforcement". The procedural decisions made by the Office of the Privacy Commissioner of Canada have been highly questionable, and greatly reduce the effectiveness of, and exacerbate the difficulties for consumers with, PIPEDA. Some findings under PIPEDA that could have significantly impacted upon an established business model have been decided to permit the continuation of that business model, despite a privacy breach.

To some extent, results that are not favourable to consumer privacy rights are to be expected in a standards-based, non-prescriptive law such as PIPEDA that seeks to balance those privacy rights with business information use. However, the depth of the negative experience of consumers under PIPEDA suggests the need for major reforms to PIPEDA to make its process more practical and effective for consumers.

Table of Contents

Introduction

The *Personal Information Protection of Electronic Documents Act* (PIPEDA) has been with us now for nearly 4 years in the federally-regulated business sector. PIPEDA has had a significant impact upon these businesses and upon consumers. However, it could have been a more positive experience for consumers. More needs to be done to improve PIPEDA, and, given its expanded application to a majority of provincially-regulated business since January 2004,[1] it needs to be done soon.

Scope of the Report

This report is divided into two parts. The first presents a review of PIPEDA and Privacy Commissioner of Canada decisions to highlight deficiencies from a consumer point of view. The second involves a review of privacy policies of certain major corporations that have been subject to PIPEDA complaints to see if they now are compliant with the Act. This report is not a wide-ranging review of the Office of the Privacy Commissioner of Canada or PIPEDA in general.[2] Neither does it review the effect of the "Electronic Documents" parts of PIPEDA, and the effect (or lack thereof) of the legal recognition of electronic documents. Rather the report seeks to highlight consumer experience with the privacy protection aspects of PIPEDA that should drive change.

Background – History of PIPEDA's application, investigations, number of findings, history of Office, etc.

Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) was brought partially into force on January 1, 2001. PIPEDA was, in effect, two acts fused at the time of introduction in the House of Commons. Part 1 deals with privacy matters. Part 2 and other ancillary parts deal with the legal validation of most electronic communications. This study deals only with the privacy aspects of PIPEDA.

PIPEDA named the Office of the Privacy Commissioner of Canada (OPCC) to oversee implementation of the privacy portion of PIPEDA. An "ombudsman" model was chosen for the Office of the Privacy Commissioner after extensive

---

[1] PIPEDA does not apply in Québec, Alberta or B.C., as these provinces have passed their own "substantially similar" provincial privacy legislation. Recent StatsCan figures show 49% of business enterprises and 47% of the labour force in the private sector are in B.C., Alberta and Québec.

[2] The Public Interest Advocacy Centre intends to comment upon the technical aspects of PIPEDA in the context of the five-year review mandated by s. 29 of the Act, in January 2006. For PIAC's comments on revising the CSA Privacy Standards which form the Schedule to PIPEDA, see "CSA Model Code for the Protection of Personal Information, CAN/CSA-Q830-96, 2002-2003 Review, Comments of Philippa Lawson, Public Interest Advocacy Centre", October 20, 2002 (online: < http://www.piac.ca/Proposed%20Revisions.htm>.

input during the drafting process.[3] Consequently, the Privacy Commissioner has few traditional enforcement powers (such as order-making powers and the ability to fine offenders) under PIPEDA. PIPEDA is in fact "enforced" by the complaints of individuals to the OPCC that an organization may be violating PIPEDA.

The heart of PIPEDA, the "ten privacy principles," is attached in a schedule to the act. PIPEDA's schedule of privacy principles is based upon an industry standard for privacy protection developed under the auspices of the Canadian Standards Association (CSA). Incorporating a CSA code so explicitly represents something of an innovation for a Canadian federal act.

In addition, PIPEDA took an interesting tack on the question of federal jurisdiction over privacy, an area that would seem to infringe significantly upon provincial constitutional competence in the area of property and civil rights. During the first three years of the PIPEDA's existence, it applied only to the federally-regulated entities or to any entity disclosing personal information across provincial or international borders for "consideration". However, provincial governments would be permitted to pass "substantially similar" acts and be exempted from the application of PIPEDA within the provinces. So far, Québec, Alberta and British Columbia's private sector privacy acts have been declared "substantially similar" by the federal government; however, this has not prevented Québec from challenging this innovative federal foray into provincial affairs in court as constitutional overreaching.[4]

As noted, for the first three years of its existence, PIPEDA applied only to federal organizations and those disclosing data interprovincially or internationally for consideration. This means the bulk of the act's application and its interpretation by the OPCC has focused on federally-regulated businesses such as federally-chartered banks, airlines, telecommunications and broadcasting companies, Internet service providers and interprovincial transport providers such as railways and trucking lines. As a result, these companies have become the "early adopters" of the legislation. Therefore this study will necessarily concentrate on these players; however, this should not be seen to indicate that these companies are any less, or more, privacy law-compliant than any other businesses.

During the period 2001-2003, the Privacy Commissioner issued 257 findings.[5] The OPCC also received more than 13,000 inquiries and complaints in 2001, over 14,000 in 2002 and over 8,000 inquiries and 300 complaints in 2003. It is fair to say that during this period, the OPCC was busy.

---

[3] The first Privacy Commissioner of Canada, Bruce Phillips, strongly promoted this vision of the OPCC during the negotiations leading to its drafting.

[4] See Michael Geist, "Fighting privacy law questionable", *Toronto Star*, January 19, 2004. Online:< <http://shorl.com/dukuhagytrasu>.

[5] See Murray Long & Associates Inc., "Spreadsheet of Privacy Commissioner of Canada Findings to December 24, 2003". (Long Spreadsheet). The author is indebted to Murray Long for his permission to use this resource.

Concerns with OPCC Process

A conscious decision was made to model the OPCC on the "Ombudsman model", a conciliatory model where the parties are encouraged to sort out their differences amicably, facilitated by a state official, the "Ombudsman". Under PIPEDA, although the Privacy Commissioner has the power to summon witnesses and enter premises to investigate a complaint, there is no power to enforce his or her "findings". The findings themselves are not "decisions" and respondents are not bound to follow the recommendations.[6] The Federal Court of Canada has the power to enforce the Act and to impose fines. However, an individual, or the Privacy Commissioner,[7] must bring an application to that court for enforcement of the Act. The enforcement proceeding is an original court process, with all of the attendant court costs to litigants. There have been few Federal Court proceedings since PIPEDA came into force. This may be because the ombudsman model seeks mediation at every turn, or that complainants generally were satisfied with the results. However, it should be noted that the provinces that have their own privacy acts all have eschewed the ombudsman model (although these acts also promote mediation where possible) and instead operated with a traditional administrative tribunal and commissioner with enforcement powers.

The ombudsman model's reliance upon individual complaints leads to an ineffective "argument" of the dispute from the consumer side. On the positive side, the complaint process requires only an informal letter to set it in motion. However, although the complainant is interviewed, there is no process for the complainant to respond to the formal response of the company to the Privacy Commissioner, or to the respondent. The absence of the usual adversarial approach in an administrative tribunal means the companies respond more formally and legalistically, while the complainants never get this chance and consequently their complaints seem unsophisticated.

As a result of the ombudsman model, the absence of traditional administrative tribunal structures and the lack of clear enforcement powers, the federal OPCC has developed more unorthodox procedures for dealing with complaints.

Naming Names

The Privacy Commissioner to this day refuses to name the names of respondents or complainants, even in findings. This is so despite a possible

---

[6] See decision of the Federal Court Appeal in *Englander* v. *TELUS Communications Inc.*, *infra*. The Federal Court (Trial Division) in the same case had found "the PCC is entitled to some deference with respect to decisions clearly within his jurisdiction".

[7] Respondents are not permitted to bring an application to Federal Court on a PIPEDA matter. This has the perhaps perverse result that businesses are more likely to ignore a ruling than comply in the interim, and fight the principles in court.

power to do so.[8] The OPCC has taken the position that the law does not permit naming as a matter of course, but might be justified for "repeat offenders". The OPCC promised it "will give serious consideration to the question" of naming names where there are "compelling reasons to do so" in January 2004, [9] but so far no such naming has occurred.

Even under a system of naming only "repeat offenders", however, a privacy violation by a company must be complained about, and a formal finding made at least twice on the exact same issue before naming the would be considered by the OPCC. It seems counterproductive and unfair to not allow consumers to make a judgment on whether a business is systematically dealing poorly with privacy issues based on all the findings regarding the business.

While complainants are theoretically free to make full findings public, individuals simply do not, likely for fear of more invasions of personal privacy. It is clearly inappropriate to place the full pressure of deciding whether to publicly name a company for a privacy violation on an individual. Recent calls from many quarters to publish the names of respondents in findings have been rebuffed. This is a truly bizarre situation, in that individual complainants (or respondents) are free to post the entire decision (as PIAC has done) but the Commissioner is self-censoring. However, it is not appropriate for an individual to bear the weight of making their name and complaint public – after all, it was a *privacy* complaint.

Findings Summaries

Secondly, the public findings published on the OPCC website are simply summaries of the full findings. The complainant and the respondent are instead the only parties provided a full letter of finding – but this letter may exist in different versions.[10] Lawyers and privacy consultants have complained that the summary findings limit their ability to advise their clients or state the law on privacy responsibilities.[11] The findings reports are often so terse as to be

---

[8] See Public Interest Advocacy Centre, "Letter to Privacy Commissioner of Canada urging Commissioner to name names of respondents in Commissioner Findings" (December 18, 2003). Online:< http://www.piac.ca/namenames.pdf>.

[9] See letter of Privacy Commissioner of Canada to PIAC, January 12, 2004 (online: http://www.piac.ca/pccnamenames.pdf) which reads in part: "As I have stated publicly, this office will give serious consideration to the question of in what situation the identities should be made public. It must be part of a structured approach with rational, defendable reasons to support it. As you know, the law states that we "may" make public any information but it does not state that we have to. However, there may be compelling reasons to do so.".

[10] *Ibid.* It seems on the wording of s. 13 of PIPEDA that only one findings report should be issued and sent under a cover letter to each of the complainant and respondent. In fact, the complainant and respondent receive different findings letters. Most of the differences are non-material but the practice is irregular and has the potential to result in inconsistent statements to each party.

[11] See Colin J. Bennett, "The First Year of the Personal Information Protection and Electronic Documents Act: Was this the Way it was Supposed to Be?", Address to the conference on "Understanding Privacy: New Laws, New Challenges", Vancouver, March 11-12, 2001, at p. 10; see also comments of Murray Long in numerous PrivacyScan newsletters.

unusable.[12] In addition, the summary in at least one case appears to leave out important information in the full report that effectively changes the OPCC interpretation of the law.[13]

Fact "Finding"

Thirdly, there also have been continuing problems around the "facts" found by OPCC investigators. In a complaint brought by PIAC against Bell Mobility in 2002 (see discussion below) Bell Mobility was permitted to allege the OPCC got the facts wrong, and to provide a different version of the facts to the OPCC, in advance of the final finding and without notice PIAC of the new facts.[14] An "agreed statement of facts" practice has been suggested but has not been formally adopted by the OPCC. Assistant Privacy Commissioner Heather Black, in an interview, stated that the OPCC will be "going back to ***organizations***, I believe, in all cases and saying "these are the facts that we are going to rely on."" [Emphasis added.][15] It is not clear if the OPCC is also returning to the complainants to verify their version of the facts, but this was not done with the PIAC Bell Mobility and Bell ExpressVu complaints (see discussion below).

Findings Categories

Fourthly, the OPCC uses an unhelpful system for categorizing the disposition of complaints. These categories were expanded recently, and somewhat confusingly. They are: well-founded, well-founded and resolved, resolved, not well-founded, discontinued, and no jurisdiction. In January 2004, the OPCC added "Early resolution" and "Settled during the course of the investigation".[16] Commentators have complained that it is difficult to know, for example, if "resolved" should be counted as a privacy violation or not.[17] However, in the cases noted as "resolved" the vast majority appear to indeed be "well-founded". Such a system is confusing and open to abuse to hide the number of companies found to be violating PIPEDA. In addition, the new categories of "early resolution" and "settled during investigation" stem from a recent push by the OPCC to resolve most complaints not raising novel issues in a "mediation" stage. Although this mediation stage is allowed under s. 12(2) of PIPEDA, its application

---

[12] See the comments of the Federal Court Appeal in *Englander* v. *TELUS Communications Inc.*, *infra*. The court described the reasons of the Privacy Commissioner in that case as "to say the least, laconic."

[13] See the discussion below of the PIAC complaint regarding Bell Mobility and immediacy of opt-out consent.

[14] This involves one of the original secondary marketing opt-out consent complaints filed by PIAC with the OPCC in 2002. The full saga is revealed on the PIAC website at http://www.piac.ca/privacy.htm under the heading "Revised Letter Findings (November 7, 2003) in PIAC complaints to Privacy Commissioner of Canada".

[15] See PrivacyScan, March 25, 2004 which is an interview with the Privacy Commissioner, Jennifer Stoddart, and with Heather Black Assistant Privacy Commissioners and Raymond D'Aoust.

[16] See OPCC, "Definitions for each category of finding under the Personal Information Protection and Electronic Documents (PIPED) Act". Online: <http://www.privcom.gc.ca/cf-dc/def_e.asp>

[17] See PrivacyScan, December 1, 2004 (Revised), p. 2.

to a bulk of decisions, and the reporting of the results of these mediations as "early resolved" or "settled" again serves to hide if a privacy violation had occurred and also reduces the number of "well-founded" complaints.

"To Tell the Truth"

Fifthly, the new Privacy Commissioner of Canada, Jennifer Stoddart, has seen fit to delegate the making of all PIPEDA findings to Assistant Commissioner Heather Black. Although the appointment of an Assistant Commissioner is permitted under PIPEDA and the *Privacy Act*, it seems a possible violation of the legal principle of non-delegation (in latin legalese: *delegatus non potest delegare*). That is, in matters the Privacy Commissioner was appointed to decide, it is inappropriate for her to completely divorce herself from writing the findings, at least nominally, when this has been the traditional role of the Privacy Commissioner since PIPEDA came into force. It also appears to be contrary to the text of s. 13 of PIPEDA, which reads in part: "13. (1) The **Commissioner** shall . . . prepare a report that contains: (a) the Commissioner's findings and recommendations . . .". The Commissioner may delegate the investigation of complaints (s. 12(3)) and the audit of a business for privacy compliance (s. 18(2)). However, there is no provision permitting the delegation of the making of findings. Considering that Parliamentary hearings were required for the appointment of the Privacy Commissioner, but not the Assistant Privacy Commissioner, it appears the public has not been provided the legislatively selected candidate in her official role as final arbiter of privacy opinions. To quote an old game show: "Will the real Privacy Commissioner please stand up?"

The Importance of Trust

Sixthly, there lately has been a palpable move in the OPCC to accommodate business interests in the application of PIPEDA. This spring, the new Privacy Commissioner of Canada announced in a speech to delegates of the Canadian Marketing Association that the OPCC had "reviewed the finding" on the issue of requiring an immediate method of opting out of secondary marketing and decided it no longer applied.[18] This contradicted a previous finding on magazine subscription opt-out to secondary marketing[19] (as well as cases brought to the OPCC by PIAC in 2002 (described below)) to the effect that immediate opt-out was required when using personal information for secondary marketing. In due course, findings relying upon this interpretation of opt-out consent by the OPCC were issued.[20]

---

[18] See "The Importance of Trust", an address by Jennifer Stoddart, Privacy Commissioner of Canada to the Canadian Marketing Association's 2004 National Convention & Trade Show, May 4, 2004, Ottawa, Ontario. Online: http://www.privcom.gc.ca/speech/2004/sp-d_040504_e.asp.

[19] *PIPED Act* Case Summary #167. Also see finding #238.

[20] See, for example, *PIPED Act* Case Summary #263.

This speech showed the OPCC flip-flopping on an important point (immediacy) in the central issue of opt-out consent (see below discussion of "Consent"). However, more importantly, this speech to the CMA, signaling a "policy" change at the OPCC to accommodate business concerns, seems inappropriate once the issue had already been the subject of findings. This episode indicates a proactive accommodation of business interests by the OPCC – a trend that also continues provincially[21] – but one that may shortchange consumers with less lobbying power than big business. There has been no similar proactive contact with consumer groups.

<u>You</u> Do It

Finally, of very great note is the OPCC reticence to engage in privacy audits of businesses and industries for systemic privacy violations, as is permitted under s. 18 of PIPEDA. So far, the OPCC has not a single systemic audit. The OPCC seems either content to wait and define PIPEDA solely through individual complaints, which is a method that relies upon the types of complaints it receives and is scattershot, or it is functioning on only half its powers for some unknown reason. Neither approach is effective or defensible in a climate where guidance on privacy rules is needed.[22]

"Whack a Mole"

Finally, the very large elephant in the PIPEDA room is the legacy of the Radwanski era on the present OPCC. The controversy over Mr. Radwanski and his reluctant resignation left the OPCC understaffed and bureaucratically hamstrung. It is also impoverished.[23] Legislative oversight of the approval of Jennifer Stoddart as Privacy Commissioner was appropriately stringent as befits this important public office. However, despite her appointment, the legacy of administrative excess has left the OPCC too weak to adequately protect the privacy rights of Canadians as outlined in PIPEDA. For example, so far in 2004 the OPCC has only published 38 findings, of which the latest 12 were of the "early resolved" and "settled" variety, offering almost no discussion of the problem and no PIPEDA analysis. This is to be contrasted with an average of 80-100 in the first three years.[24]

Despite the enlargement of PIPEDA's application to the entire private sector in provinces covered by PIPEDA, this output is anemic. Commissioner Radwanski had been trying to "build numbers" of cases during his tenure. However, the present OPCC has veered completely in the other direction. Heather Black, Assistant Privacy Commissioner noted in an interview that: "We're not driven by

---

[21] For example, the Ontario IPC recently has published a joint paper on "customer relationship management" (CRM), otherwise known as consumer profiling, again with the CMA.

[22] Given the OPCC's reluctance to use its systemic audit power (see below), the findings summaries are the only guidance on PIPEDA for consumers and business.

[23] See PrivacyScan, November 15, 2004, p. 1.

[24] See Murray Long and Associates, "PrivacyScan", November 25, 2004.

numbers any more. We're not playing "whack-a-mole" or whatever".[25] Canadians have every right to demand a little mole-whackin', however, during the infancy of PIPEDA when both consumers and business are looking for guidance from this key office.

There is no federal-level "champion" of privacy rights in Canada besides the OPCC. Even if one accepts that the OPCC should be a simple mediator and facilitator, even this role appears to be falling by the wayside. Consumers and citizens should ask this office be adequately funded in accordance with the importance of PIPEDA to them. If government budgets do not include Canadians' privacy rights, innovative measures may need to be sought. These could include giving the OPCC the power to impose fines; requiring businesses to directly contribute to the upkeep of the OPCC; or even instituting user fees for filing complaints, a step that would contradict the spirit of PIPEDA.

Lack of Follow Up

Lastly, it is often the case that the OPCC makes recommendations to companies to change a practice to either come into compliance with PIPEDA (sometimes with an actual timeframe specified) or as a suggested "best practice". Despite these exhortations, and despite the fact that several companies have been found to be "repeat offenders" (facing well-founded complaints on the same issue – some are detailed below) there appears to have been no follow up of these recommendations by the OPCC at all. At the least, companies should be warned that failure to follow recommendations would risk an OPCC-led investigation or audit.

Conclusion

Canadians should be very wary of losing their ground-breaking privacy rights regime due to these seemingly "procedural" and other administrative decisions of the OPCC that seriously undermine these rights. Although the issues seem arcane, they are a symptom that the OPCC still has significant accountability problems.

Concerns with Overall Structure of the Act

Standards appended to an act do not make a good statute.[26] Standards may work as the basis for regulations under an act, but their non-prescriptive nature makes them a poor fit for the prescriptive requirements of an act. Enforcement is purposely out; mediation is built in. Some have argued that the Act is best

---

[25] See PrivacyScan, March 25, 2004, "Interview with Privacy Commissioner of Canada, Jennifer Stoddart, and Assistant Commissioners Black and D'Aoust", p. 6.

[26] See "The Personal Information Protection and Electronic Documents Act, An Annotated Guide" (Perrin, Black, Flaherty & Rankin, Irwin Law Inc., Toronto, 2001) at p. 6. This description of the frailties of such an Act were quoted with approval by the Federal Court of Appeal in *Englander* v. *TELUS Inc.*, infra, at para. 44.

served by promoting a cooperative view of privacy compliance with a standards base.[27] While this approach has value in many cases, many others may be more are egregious and may require clear rules and sanctions.

The actual track record of consumers in OPCC complaints thus far shows the value of a stick and the ineffectiveness of a carrot. PIPEDA lacks an effective enforcement mechanism. However, at present PIPEDA not only lacks enforcement, it actively discourages it, and thereby discourages consumers. With this in mind, this report turns to a review of specific findings of the OPCC from a consumer standpoint. The discussion of the findings is organized by sector; concrete examples of the results on consumers are given where available.

Consumer concerns with specific industries in findings

Banks and Banking

Banks in Canada by far bore the brunt of complaints leading to findings over the first three years of the implementation of PIPEDA. Banks were the respondents in 118 findings out of the 255 made to January 1, 2004 (46%).[28]

Banks are among Canada's largest businesses and arguably have the most, and most direct, contact with Canadian consumers. Banks also deal with sensitive financial information. Therefore, banks are somewhat unfairly highlighted by the limited application of PIPEDA within the first three years of its application, although this attention is justified by their importance to consumers.

In addition, banking in Canada is a lightly regulated industry at the consumer level. It is possible that consumers with other frustrations with banks used the new privacy complaint tool, with its low (or no) cost structure and high profile to register customer dissatisfaction. At another level, and as is repeated incessantly by privacy consultants and privacy commissioners, privacy is built on trust, as is banking. It is simply a fact that the traditional duties of confidentiality in banking overlap to a great extent with the new privacy legislation and thus privacy legislation appears to have a great impact upon banking.

Whether or not banks were unfairly represented numerically in OPCC findings for these or other reasons, Canadian banks were claiming to be ready for PIPEDA before it was implemented.[29] How did they do in the first three years?

---

[27] See Colin J. Bennett, *op. cit.*

[28] Murray Long and Associates Inc., "Key Statistics on Privacy Commissioner Findings under PIPEDA" ("PrivacyScan spreadsheet"), listing all OPCC decisions and outcomes 2001-2003. As the OPCC does not keep statistics of complaints by industry, the number of complaints not investigated and/or not leading to findings is unknown. However, in the 2003 Annual Report, the OPCC indicated a wish to keep such statistics in the future.

[29] The CBA website page on "Banks and Privacy" gives the following explanation:

Most OPCC complaints dealt with improper account access, use or disclosure; secondary marketing; overcollection of personal information; income reporting questions; security problems; access problems; credit reporting and SIN use. Where these findings were examples of general consumer issues with privacy, they are dealt with below under the section of this report on general issues. Where, however, the issues are specific to banks, they are dealt with below.

"VANILLA" BANK ACCOUNTS AND CREDIT HISTORY

An interesting set of findings illustrates further the reticence of banks to implement privacy-respecting practices where that would mean changing long-established banking practices. The "vanilla bank account" findings were the result of a complaint (in finding #40) by a consumer that the bank in question would not open a bank account (for cash and cheque deposits) without first checking his credit rating. As a result of the bank's usual practice, they *required* the applicant for any bank account to release personal information (including a SIN) for the purposes of a credit check. The consumer complained that this was unnecessary, and the dispute quickly progressed to a discussion of the reason for the credit check. The bank contended that their bank accounts all allowed some form of credit – for example, overdraft protection or cheque cashing without a hold period. The bank also argued the credit check prevented new account fraud and identity theft. Finally, the bank claimed this information was also required to comply with the then relatively new *Proceeds of Crime (Money Laundering) Regulations*. The consumer countered that he was not requesting a chequing account (only deposits and withdrawals), was willing to endure hold periods and would accept an account without overdraft protection. The bank refused to honour the request to open the account.

The Commissioner, in finding #40, determined that the consumer was entitled to such a "plain vanilla bank account". The OPCC held that the bank's refusal to offer the account was a violation of Principle 4.3.3,[30] the "refusal to deal" section.

The banking industry was the first to go beyond a statement of principles and develop a comprehensive privacy code of conduct in 1986. The CBA's code was updated regularly to meet the changing needs of consumers. The values in this code are now reflected in the federal government's Personal Information Protection and Electronic Documents Act, which came into effect January 1, 2001. It governs the activity of all federally regulated industries – including airlines, banks, broadcasters and telecommunications companies - in how they collect, use, disclose and provide access to their customers' personal information.

Prior to January 2001, banks conducted a thorough review of their operations to ensure they complied with the Act and designated a senior officer responsible for upholding its rules. Most bank customers have noticed little change, as the Act's guiding principles and most requirements are the same as the voluntary standards banks have followed for many years.

[30] Principle 4.3.3 reads:
4.3.3 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 fulfil the explicitly specified, and legitimate purposes.

That principle states that a business must not refuse to offer a service where the consumer is justified in not providing personal information. In order for the bank to have been able to say no, the bank would have had to demonstrate that the personal information was required for "explicitly specified, and legitimate purposes", which were, in turn, germane to the customer's request.

Although the purposes for the credit check information were not *explicitly* specified by the bank on the authorization, the OPCC took real issue with the legitimacy of the bank's refusal. In brief, the OPCC finding held that the bank's reasons were not legitimate. The OPCC held that the consumer must be actively seeking credit to justify a credit check, which was a privacy-intrusive measure.[31] Here, the consumer was largely a "passive" potential credit receiver, only because the bank's own "policy of automatically providing new customers with overdraft protection and immediate access to deposited funds [caused the problem] whether or not the customer specifically sought such privileges".

Had the analysis ended here, the finding would have been quite useful to consumers. This finding would have been a precedent for the principle that the "legitimate purposes" test of principle 4.3.3 is to be viewed from the perspective of the individual consumer (subjective test), and not the business. The wording of principle 4.3.3 is unclear on how to judge "legitimate purposes" and has been criticized. However, it is certainly arguable that "legitimacy" could be, or should be, in the eye of the consumer, not the business.

The OPCC went further to base the decision upon the "reasonableness" test in s. 5(3) of the Act. The OPCC noted "a reasonable person would not have considered the purpose appropriate in the circumstances". Section 5(3) is therefore being used as a general "purposes reasonability" test here. [32]

---

[31] It is difficult to know the extent of "new account fraud" whether that term means loss to the bank through a customer running up bounced payments on overdraft or depositing bad cheques and then immediately withdrawing the funds, or whatever. The CBA has no figures on these frauds. These are claimed to be business secrets of the individual financial institutions. However, there is much merit in a consumer's ability to obtain a simple deposit service without having to undergo a credit check.

[32] This quote from PrivacyScan (July 4, 2003, p. 19) shows that there is debate about the appropriateness of judging all references to purposes for collection, use or disclosure in the Act by the standard of reasonableness:

> "Note: In our view, this is another example of subsection 5(3) being inappropriately used. [. .] Our over-arching concern is that subsection 5(3) is an essential component of the Act intended to fix a serious shortcoming in the Identifying Purposes Principle that, while purposes had to be identified, they did not have to be justifiable by any objective standard. However, subsection 5(3) was never intended as a general purpose reasonability test. A requirement for reasonable treatment of personal information is built into many of the CSA clauses and can be relied upon without the need to cite subsection 5(3) as the root of an obligation to act reasonably. Expanding the scope of subsection 5(3) beyond its application to purposes both undermines its value and leads to improper application of the law. This is a recurring problem."

However, this argument ignores the placement of s. 5(3) in the main body of the Act, as opposed to somewhere in the schedule, suggesting it *is* a general requirement. It is not clear to the author why adding

Despite this position in finding #40, there is the later finding of #219, which was effectively a repeat of finding #40 with the same bank. Again, a customer asked for a vanilla bank account, with no credit provided. Again, the same bank maintained a credit check was required for identification purposes. Again the OPCC found a violation of 4.3.3.

There is a question of what the proper scope of 4.3.3 is and about using PIPEDA to effect consequent changes to business practices. Murray Long, privacy consultant, has posed the question: "Can you be forced to offer a non-existent service that is less-privacy intrusive than your present spectrum of offerings?" It is possible to argue yes: if your service is a "lifeline service" like banking, and if you have turned it into a "retail" business with a marketing component requiring the maximization of collection of customer details, you can be forced to offer the more "utility-like" non-privacy-invasive service. If the bank had undertaken to not use this person's personal information for secondary marketing, that would have justified the fraud defence. Note that the bank did not argue this. Service industries like banking appear to want to collect personal information as the *quid pro quo* for their services, so that they can market retail services and wealth management, etc. Without this personal information their retail banking cannot become a growth industry and becomes more like a utility. Therefore it is legitimate to "call their bluff" and require businesses using such a personal information based-business model to offer a product they don't carry, because *they have changed banking into retail banking* – not "plain vanilla" banking– a new and naturally privacy invasive-form of business.

CALL-TAPING CASES

A rather extraordinary set of findings regarding a particular bank with a particular issue have highlighted recalcitrance in the industry to the full implications of PIPEDA. These findings have to do with the simple issue of tape recording customer calls to banks when performing such activities as applying for a loan or activating a credit card over the phone.

In three findings on this issue (#215, #176 and #86), the OPCC chastised a particular bank (again, which one is not identified) for repeatedly taping conversations with customers attempted to perform tasks on the telephone and for not providing an alternative method for performing the same task without such taping and without informing the consumer of this option.

---

a general purpose reasonability test (as opposed to specific individual test for certain requirements) undermines its effectiveness. Indeed, the Federal Court of Appeal, commenting upon this requirement in *Englander* v. *TELUS*, *supra*, said rather that s. 5(3) is a general purpose section and that it actually lends credence to the idea the Act is a balance of privacy interests and business uses of personal information (at para. 38): "However, there is also an express recognition, by the use of the words "reasonable purpose," "appropriate" and "in the circumstances" (repeated in subsection 5(3)), that the right of privacy is not absolute."

The bank initially argued in finding #86 that consent was not required for taping, as the Canadian *Criminal Code* permits the taping of private conversations with the consent of at least one party. As the bank (via an employee who had signed a document stating his or her consent to taping) was performing the taping, one party had obviously consented. The bank argued that the taping was the recording of customer "consent" – but consent in the sense of agreement to contractual terms. The tape recording was merely a record of that agreement.

The OPCC took an entirely different view, from a data protection and wider "role of privacy in society" position. In effect, the OPCC viewed this "banking transaction" from the perspective that taping of a conversation was, without consent of the individual being taped, naturally a privacy violation. Since the act imposes a "reasonable person" test for the purposes for which a company wishes to collect, use or disclose personal information (s. 5(3)), the Commissioner looked at what a reasonable person would think of surreptitious tape recording of conversations. Here the finding takes an *individual's view* of the process and concludes that most reasonable people will feel a sense of privacy violation in surreptitious recording of their voice and conversation, irrespective of the use to which the conversation is to be put by the other party (here, as evidence of the customer's application for a loan). The Commissioner bolstered this view by detailing how a recorded conversation is "qualitatively different" from a written record of the conversation made by a bank employee:

- It will capture incidental information that the service representative might not note - information that may not be germane to the call but could be used by the organization for other purposes;
- It will capture the caller's tone of voice, that could also be used for other purposes such as a legal proceeding; and
- It can be used to infer information about the caller, for example ethnic origin and age that is not relevant to the purpose of the call.[33]

These considerations are new in that they would not have been considered in the past under a strict legal evidentiary analysis. However, the wider scope of privacy law recognizes and validates these types of concerns and attempts to give legal protection to individuals' sense of *personal* privacy.

However, the matter did not end there. In finding #176, the same bank was faced with a complaint that a customer's call to activate a credit card had been taped without first informing the customer, and without offering an alternative method to activate the card. Further, the bank refused to, or claimed to not be able to, erase the tape made. The bank first argued that the taping procedure was outlined in documentation relating to the credit card agreement. The

---

[33] From OPCC website: *Best Practices for Recording of Customer Telephone Calls*, referenced in finding #86.

customer did not recall the booklet alleged and the OPCC found that the bank should have included information on taping *at the time of the collection*. There was therefore no consent, implicit or explicit, to the taping. The bank also argued that the taping was as a result of "employee error" – that the bank simply had not had enough time to educate its staff on the new policy (which incorporated the best practices suggested by the OPCC in finding #86). As for erasing the tape, the bank first argued that the process of taping was "equivalent to a signature" – that is, it was again, simply evidence of agreement to the terms of the credit card activation. Then the bank argued that the extraction of the correct portion of the tape was difficult. The complainant and the OPCC pointed out that this position contradicted the bank's argument that the purpose of taping was for evidence keeping.

In finding #176, the OPCC severely criticized the bank for not implementing the policy and not communicating it adequately to bank staff. One year had passed since the original complaint and undertaking in finding #86 and the OPCC found the bank continued to tape record customer credit activation similar calls as a "matter of course". The OPCC recommended that the bank implement the policy of revealing the taping of calls. That should have been the end of the matter.

However, along came finding #215 where the same bank, yet again, is chastised in identical terms by the commissioner over an identical violation. The finding is strange, in that it is almost verbatim of finding #176, with the exception of the removal of the issue of erasing the tape. The most likely explanation is that the complainant in #176 again tried to activate his credit card over the telephone, but was again taped without being asked. The Privacy Commissioner simply repeated the recommendations to the bank made all along.

These cases represent the difficulty faced by the Privacy Commissioner when he or she has no powers of enforcement. When faced with an entrenched business practice that is perceived as a core step in a business process, but is also highly privacy-invasive, it is not automatic that a negative finding by the Privacy Commissioner will alter the practice. Although the naming of the bank seems an obvious option, the OPCC has consistently refused to name respondents, even though PIPEDA would seem to accommodate such a revelation when done in the "public interest".[34] It is indeed hard to see any incentive for a large business, such as a bank, to change entrenched business behaviour that is privacy-invasive unless the Commissioner either has enforcement powers or at the least can publish names, so that the public can hold the perpetrators to account.

Nonetheless, PIPEDA should be most effective in regards to the banking sector. Banks are large organizations with adequate resources to implement privacy protection regimes based on a general guideline. Banks are familiar with duties of confidentiality and while their record is not perfect, they are generally more

---

[34] See PIAC letter to OPCC on this issue online at: <http://www.piac.ca/namenames.pdf>.

scrupulous with personal and financial information than others in the credit system.

The continuing problems in the banking sector are those that are entrenched as banking habits of convenience. These hard-core and long-term problems, (such as excessive demands for credit checks, charging high fees for access requests, excessive over-collection of personal information for possible "evidence" and a refusal to implement OPCC findings), will only be solved in accordance with PIPEDA if some pressure is brought to bear by the OPCC through enforcement. Given the extremely limited enforcement tools of an ombudsman-type Commissioner, this means that the only tool really available to change hardened banking practices is the naming of the respondent banks in findings. Banks have greatly and unjustly benefited by the effective secrecy of PIPEDA proceedings and have amply shown that they no longer deserve the benefit of this very generous deference.

Banks have been diligent in creating privacy policies, training employees and appointing privacy officers. They have been less diligent in changing the banking culture that conflicts with the new value of individual privacy. In addition, banks also suffer generally from those problems plaguing all large businesses – problems relating to aggressive collection, use and disclosure of personal information for marketing purposes. This has been aggravated to some extent by the slow diversification of banking and the general position taken by banks of implying consent to disclosure of personal information to bank "affiliates".[35] However, the main problem with banks remains the same: their huge size and significant market power, when combined with the sensitivity and amount of personal information they have about Canadians, means privacy will be a constant task for them, and they must be monitored by watchful consumers. It is truly unfortunate that the policy of not naming respondents appears to have been carried forward for banks (who have benefited from this three year period to adjust business practices) in 2004.

A CAUTIONARY TALE

Finally, we turn to a case of an individual with a privacy problem in banking who tried to use the federal court to "enforce" the finding. The results are not good.

OPCC finding #224 appears to have been a simple, open and shut case of PIPEDA violation by a bank, with a clear knuckle-rapping "well-founded" result. However, the finding report hides a terrible personal saga for the complainant and a cautionary tale for consumers relying on PIPEDA, as it presently is, for privacy protection.

---

[35] See results of Ekos survey for PIAC noting 87% of Canadians polled feel it is important that banks obtain their positive consent prior to sharing their personal information with bank affiliates (http://www.piac.ca/Direct%20marketing%20conclusions.pdf).

Lillian Szilagy first started experiencing problems with the Bank of Montreal in 1995 – well before the implementation of PIPEDA in January 2001.[36] She claimed to pay off a bank Mastercard. The bank denied she had done so,[37] and Ms. Szilagy claims the bank sued her for the account "balance". The result, she alleged, was a poor credit rating. When she complained to the bank, the bank eventually agreed to rectify the credit rating with two major credit bureaus (Equifax and TransUnion). However, she alleged only one credit bureau, not both major ones, was notified with the result that she had a bad credit rating and could only obtain loans at very high interest rates. She eventually learned of the second poor rating. She claimed her calls on the bank (to the bank's Ombudsman) to remedy this rating and her request for her banking records were to no avail.

Upon learning about PIPEDA, Ms. Szilagy filed a PIPEDA complaint, based upon the accuracy of the credit ratings and the access to her records. The Commissioner concluded that both complaints were well-founded and that the credit rating should have been rectified and that the personal records should have been provided promptly (they were provided only after Ms. Szilagy hired a lawyer despite numerous requests). This result should have been encouraging to Ms. Szilagy and she believed here complaint would be resolved. Strangely, however, the Commissioner made no recommendations in finding #224. Recommendations, as noted above, are not binding on respondents. However, they can be persuasive arguments to rectify a situation and also serve the purpose of alerting the industry in question to privacy practices that the Commissioner finds inadequate. The Commissioner arguably should provide recommendations wherever they could assist the industry in better privacy practices, as part of his or her general duty to educate the public on privacy matters. Even more seriously, since the Commissioner often makes recommendations in cases where the complainant can demonstrate a harm or loss, the lack of them can seriously prejudice a complainant.

Ms. Szilagy expected the finding to convince the bank to offer an apology and to compensate her for her extra credit costs caused by the poor credit rating. However, the Bank did not do so. Faced with such problems of "enforcement" of her rights, Ms. Szilagy commenced an action in Federal Court under s. 14 of PIPEDA. This action was quickly bogged down in procedural motions, despite PIPEDA's s. 17(1) requirement that "An application made under section 14 or 15 shall be heard and determined without delay and in a summary way unless the Court considers it inappropriate to do so." At the time of writing, Ms. Szilagy has abandoned her Federal Court attempt to enforce her PIPEDA ruling in favour of

---

[36] All factual information in this description of Ms. Szilagy's situation has been obtained from court filings or the complaint finding of the OPCC. The allegations have not been proven in court.

[37] It appears from the pleadings in later proceedings that Ms. Szilagy's payments and the bank's steps to send the account for collection and/or write it off unfortunately may have, timing-wise, passed like ships in the night.

an action for compensation in the Superior Court of Justice in Ontario.[38] However, there she faces arguments from the Bank that the PIPEDA ruling is not controlling, that she must re-prove the facts established in the PIPEDA finding, and that she should have brought her action some time well in the past (a limitations period argument). She has incurred considerable legal costs thus far.

During this Byzantine effort at vindication, Ms. Szilagy has developed a stress disorder that she claims is related to her case and its unsatisfactory result so far, as well as a lost opportunity to attend law school and the loss of a personal business she had started.

Whatever the outcome of her legal actions, the facts paint a portrait of a frustrated consumer meeting considerable roadblocks in her attempts to exercise her privacy law rights. Regarding PIPEDA, the case clearly shows the cruelty of holding out a Privacy Commissioner and extensive privacy rights with no effective enforcement mechanism. The lack of recommendations in finding #224 speaks volumes about the OPCC's lackadaisical approach to process and the OPCC's lack of tools, but also lack of effort at enforcement. With an industry as important to privacy as banking, dealing with a common problem (incorrect bank/credit card payment records leading to poorer than necessary credit ratings), it is sidestepping one's duty to refrain from comment on what is likely a recurring pattern of privacy violation. Ms. Szilagy's experience with Federal Court litigation is instructive of the high hurdles faced by any average citizen in attempting to effectively "re-litigate" a process that was meant to be transparent, accessible and low-cost under PIPEDA.

Credit Reporting

Complaints and findings dealing with credit reporting issues still were number three in PIPEDA complaints, ranking behind banking and telecommunications.[39]

Credit reports rely for their value upon personal information. The information involved is financial information – a category that PIPEDA and the OPCC itself define as "always sensitive" and requiring, generally, the highest form of consent to collect, use or disclose it – explicit consent.

SPOT THE CONSENT

Consumers appear to be caught in a consent "shell game" regarding credit reporting. In finding #188, a consumer signing up with a telecommunications company (telco) explicitly requested on the application form that a credit check not be performed. The telco accepted the application, but performed the credit

[38] Court File No. 3929/03.

[39] There were 15 findings regarding credit reporting, being 6% of reported findings in the period 2001-2003. (Source: PrivacyScan spreadsheet).

check anyways. The consumer complained to the OPCC that the credit bureau improperly *disclosed* his personal information to the telco.[40] The OPCC noted that the contract between the credit bureau and the telco required the *telco* to obtain customer consent for the disclosure of personal information, not the credit bureau. Since the contract allowed the credit bureau to rely on the telco to obtain consent, it had done nothing wrong. Such a contract was, in addition, reasonable,[41] "given the large number of information requests [the credit bureau] receives daily and the considerable amount of work this type of procedure could involve".

What this case shows is that the OPCC may not apply PIPEDA when to do so would disturb a settled business practice, especially with regard to credit granting and credit reporting. In this finding, the information was either improperly disclosed, or improperly collected, or both. The OPCC in this case made no effort whatever to assist the consumer in finding the source of the problem. If it was the telco, the OPCC should have expanded the complaint to this entity and made them a respondent. If the problem was an institutional one at credit bureaus, one could expect a finding that was made on the individual facts without a great concern for the ease of the business of credit reporting. After all, if such a practice of relying upon consent of other businesses is sometimes unreasonable, then it would be *worse* if the problem were multiplied by the "large number of information requests [the credit bureau] receives daily". At the very least, the OPCC could have issued recommendations to the telco and the credit bureau about the importance of respecting explicit consumer consent (or lack thereof) in this type of situation.[42] Instead, consumers are left with the impression that credit checks are sacrosanct or that the OPCC will let major issues of consent fall between the cracks simply because the complainant does not "understand" the complex credit reporting system.

---

[40] It is not clear from the report why the consumer did not complain about, or the OPCC did not comment upon, the telco's unauthorized *collection* of the personal information from the credit bureau. Although the application form indicated a credit check would be performed, and this is noted in the "facts" portion of the finding, the consumer clearly indicated on the form that this was not to be done. One can only assume the telco in processing the application simply ignored the instruction. However, upon accepting the application without demur, it would seem the telco was bound by the change – and in any case, the customer is not responsible for seeing to it that his request for privacy is respected.

[41] It is quite possible to argue that such a contract is NOT reasonable. The credit bureaus, as noted, deal with personal information as their core business. It would seem completely feasible to provide a consent form for the credit bureau with the telco application. After all, the credit report information is the credit bureau's not the telco's. In effect, the credit bureau has been able to shift this primary responsibility for consent to the telco by contract. It is possible that such a shift is contrary to Principle 4.3, and despite the note thereto, since the relationship between the consumer and the credit bureau is in fact a direct one – the credit bureau already holds the information on the consumer.

[42] Under the OPCC's logic in this case, how would a consumer's complaint that he or she had been unable to *withdraw* consent to a credit check being performed and the results reported be handled? Through the credit bureau only? Through the telco (credit grantors) only? Both? Neither?

MAINTAINING THE INTEGRITY OF THE CREDIT REPORTING SYSTEM

The OPCC in its other findings has not clearly laid out rules for responsibility for credit report information. This is apparent in another couple of findings, #206 and #211. These also speak to the "kid-glove" approach of the OPCC to the credit reporting industry.

The first finding (#206) involved a small-business owner complaining about the bank's requirement for a line of credit that he consent to ongoing collection of his personal credit information from credit bureaus and other financial institutions. The OPCC said the complaint was not well-founded, as the bank required the credit information as a way to assess creditworthiness on an on-going basis. However, the bank maintained it had the right to continue to provide information *to* the credit bureaus, even after the banking relationship had ended, to the limit of time allowed by provincial credit reporting acts.

The OPCC justified its decision on the basis that it was "appropriate" for the bank to "maintain the integrity of the credit granting system".

This allowed not only the bank's periodic requests to the credit bureaus but also the bank's continuing provision of information to the credit bureaus. This was so not only because the banks are "contractually obligated to do so" but also "because they are duty-bound as good corporate citizens to do so". This is frankly an insult to the consumer, and a clear violation of the Act in favour of preserving the status quo as to credit reporting.[43] Where in the Act is it mentioned that "the integrity of the credit reporting system" is a counterbalance to privacy rights? Section 3, Purpose of the Act, notes individual rights to privacy are to be balanced against the "need of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances".[44] Is it not also reasonable to view credit reporting as an unauthorized surveillance system? The OPCC instead jumped straight for the opportunity to justify the systemic privacy violation here by preserving the status quo and without considering any individual criticism of <u>the fact of credit reporting</u>. Like the sun rising, therefore, consumers appear to have to live with credit reporting as a "reasonable limit" on their privacy rights.

---

[43] See also on this point the OPCC excusing of a clear violation of privacy rights by credit bureau disclosure to a bank that had not obtained consent in finding #182.

[44] The OPCC relied upon s. 5(3) which requires any collection, use or disclosure "only for purposes that a reasonable person would consider are appropriate in the circumstances." This test was never intended to provide a "reasonableness exception" to the Act, but rather to limit the available scope of dealings with personal information to those that are reasonable to an average person after consent has been obtained. This reasonableness exception is also used in relation to credit reporting in finding #171. #171 also suffers in reasoning from a statement that consumers consent "by implication" to the fact a credit inquiry is done being added to their credit report with a largely negative effect. This violates the "Identifying Purposes" portion of PIPEDA that requires explicit detailing of intended collection, uses and disclosures.

In the second Finding (#211), a couple objected to the bank refusing their request to withdraw their consent to providing personal information to other lenders, and credit bureaus. Again, the reasons cited by the OPCC in determining the complaint was "not well-founded" were:

- It has been confirmed in other cases considered by the Office that the credit system in Canada depends upon the fulfillment of myriad contractual and legal obligations.
- If individuals could withdraw their consent to disclosure of their credit history with a particular lender, the credit system would not work.

What is not considered, in giving this glib point-form decision,[45] is the position that just perhaps, the credit system, as it now works, is privacy-invasive and contrary to PIPEDA, and should be changed, to respect the Act. One is left with the impression that privacy concerns that would undermine the credit system as it simply is are unwelcome at the OPCC.

CREDIT SCORING

It is well known that the credit reporting business involves both banks and credit bureaus. What is less well known is that banks maintain internal credit scoring systems or bank credit reports for their own proprietary use. These internal bank credit scores were the subject of an early finding that set the tone for the later credit bureau cases.

In finding #39,[46] a bank customer requested access to his internal bank credit score. The bank refused, citing concerns that should the customer obtain the score, it would be possible to reverse-engineer the algorithm the bank used for its credit scoring, which was proprietary and a closely-guarded trade secret in the competitive world of retail banking. The bank stated that if only 25 or so persons obtained their bank credit score and then compared the results, it would be possible to re-create their algorithm. The OPCC sought the advice of an expert in mathematics to advise the Office on this possibility. The expert said it was possible. After much hand-wringing in the decision, the OPCC bowed to the argument that this valuable credit scoring system would be threatened by any access to even one account and so found the complaint was not well-founded. What this analysis clearly missed is that the potential problem of fraudulent purposes by a conspiracy of applicants seeking personal credit scores was not the problem of the individual seeking access to his discrete credit score. It was a bank fraud problem; to be dealt with in whatever manner the bank chose to do so by setting up internal safeguards. In effect, the individual's clear access rights to personal information were sacrificed to the bank so that it did not have to spend the money or take the time to set up proper fraud standards. This sends a

---

45 See also the brief dismissal of the same point in finding #194.

46 See also finding #63.

message to business – namely that any possible security holes that may be opened by freer access to personal information they hold are not their problem, but rather are a deficiency in the Act to be avoided at all costs, and that these unforeseen results of PIPEDA will be dealt with by aggressive interpretations of the exceptions in PIPEDA.

There were a few bright points for consumers in dealing with credit reporting. Finding #47 required banks to provide information they had on file that was obtained from a credit bureau report, despite the bank's objection that it was contractually bound not to do so. An exception was for situations "where required by law". The OPCC rightly noted that PIPEDA was, in fact, law. The OPCC also rejected a bank argument that increased cost could excuse compliance. The OPCC found cost of compliance is not a factor, a significant ruling for consumers, as business must bear the cost of compliance, not consumers. Finally, the OPCC noted that simply because the information was available directly from the credit bureau did not negate the bank's obligation to provide access to its knowledge of the consumer's credit file. In short, a business cannot re-direct a consumer to another source of the personal information when the consumer has demanded to know what that institution in particular has collected, used or disclosed in relation to his or her personal information. This was also an important principle to establish for consumers, who otherwise might never be able to determine what happened to their personal information inside a particular business and would instead be sent on wild goose chases to find the creator of the information.

Two other notable findings in credit reporting were #150 – which clearly imposed a duty upon credit bureaus to treat information processing on credit reports carefully and to correct mistakes promptly and finding #151 – which required banks to clearly explain to consumers in credit documents the need for use of a Social Insurance Number (SIN) for credit reporting. That finding stopped short, however, of inquiring into whether credit bureaus should be using SINs as unique identifiers in an age of identity theft.[47]

Telecommunications Companies

Telecommunications companies (telcos) fared fairly well under the new privacy regime. Of the 57 complaints (22% of all complaints) brought against telcos, 30 were not well-founded and only 22 were well-founded or "well-founded and resolved". Raw numbers do not tell the whole tale of this "relative success", however.

Telecommunications is a complex area that is already highly regulated by the Canadian Radio-Television and Telecommunications Commission (CRTC). Adding a layer of privacy protection legislation to the regulatory matrix sowed some confusion with the OPCC.

---

[47] See, *infra*, OPCC, "Best Practices for the use of Social Insurance Numbers in the private sector" .

On some occasions, the OPCC exhibited deference to CRTC – to point of fault. This deference is somewhat understandable: the CRTC is a large and well-established administrative tribunal with a long history of regulating this particular industry. However, PIPEDA must apply whenever personal information is used and this will often be in regulated environments. In other situations, the OPCC directly challenged the CRTC's interpretation of privacy law in the telecommunications sphere. However, to consumers, privacy violations in telecom appear the same as privacy violations in any other industry. Overall, however, the telecommunications area has proven a particularly difficult area for consumers looking to vindicate their privacy rights.

ENGLANDER V. TELUS

Chief among the cases of privacy violations and undue deference to the CRTC is the *Mathew Englander* v. *TELUS Communications Inc.* case. This started life as finding #8, where Mr. Englander[48] essentially complained about two things. First, that TELUS breached PIPEDA principle 4.3 (knowledge and consent of the individual required). He argued the phone company did not obtain his consent to use the his name for secondary marketing purposes (lists of names were sold to charities and telemarketers, and used for reverse directory service) because these uses were not made clear to him when he signed up for phone service. Only if the subscriber inquired about unlisted number service would the full possibility of secondary disclosure of the information be mentioned. Second, he argued that the phone company should not be charging subscribers for unlisted number service.[49]

The then Commissioner Radwanski rejected both claims. Regarding fees, the Commissioner essentially declared utter deference to the CRTC to set fees for telecommunications services and did not address the thorny question of whether and how PIPEDA could apply to personal information that happened to be collected by a telecommunications company instead of any other sort of company. Regarding the consent issue, Commissioner Radwanski found that consumers were well aware that the information collected by phone companies ended up in the white pages. He then reasoned that TELUS could bootstrap its implied consent to white pages publication of telephone subscriber names to allow for disclosure for secondary marketing, since there is an exception in

---

[48] Mr. Englander self-identified to the media to promote his case. In addition, as soon as he brought his case to the Federal Court, his name was public as a matter of court record.

[49] Mr. Englander relied for this argument on Principle 4.3.3 known as the "tied selling" or "refusal to deal" section. It's aim is to prevent companies from requiring that consumers give consent to collection, use or disclosure of their personal information for a purpose that is not "explicitly specified" and "legitimate". However, the Act does not clarify in whose eyes the term "legitimate" is to be interpreted – the consumer or the company. To the company, secondary marketing of personal information may seem "legitimate" while consumers may be shocked and dismayed that this use would be required of them simply so that they could purchase a product or service.

PIPEDA that allows companies to use information that is specified in the regulations to the Act as "publicly available" for any purpose.[50]

Mr. Englander, a lawyer, noticed the logical flaw in the Commissioner's reasoning on consent and was not happy with the payment issue and took the Commissioner's finding to Federal Court under s. 14 of PIPEDA for a "hearing".[51] Mr. Englander's initial experience with the Federal Court (Trial Division) is a lesson for complainants. Mr. Englander lost his application on both issues. This may have in part been because the Court accorded "some deference" to the Privacy Commissioner's finding. This means the Court took the finding of the Privacy Commissioner as persuasive, so that Mr. Englander had to argue that it was wrong, not that the Court should simply look at the facts and PIPEDA and judge for itself. The Federal Court (Trial Division) dismissed the complaint[52] and awarded full costs of the proceeding to TELUS, as if Mr. Englander had sued TELUS in court in a typical lawsuit. The initial bill was almost $18,000.

Mr. Englander eventually persuaded the Court to reduce the fees,[53] but still was left with an almost $12,000 bill to TELUS for his efforts to vindicate Canadian phone subscribers' privacy rights.

The story would have ended there as a sad tale of betrayal of consumers by the Privacy Commissioner and proof that a trip to Federal Court for complainants ensures only frustration, enormous costs and is essentially a cruel trap for consumers. However, as this report was going to press, the Federal Court of Appeal largely reversed the decision of the trial court.[54] The Federal Court of Appeal found that TELUS did not, indeed, obtain valid consent to their secondary marketing when signing up first-time telephone subscribers, since customers had to inquire about the possible secondary uses of information, or inquire about unlisted number service, before TELUS would offer up that relevant information. As for the information being "publicly available" the Federal Court of Appeal made short work of that argument, noting that the information is not publicly available until it is in the white pages, and the information cannot go into the white pages without a valid consent in the first place.

---

[50] See PIPEDA, ss. 7(1)(d) [collection], 7(2)(c.1) [use] and 7(3)(h.1) [disclosure]. The "publicly available" information must be specified in regulations under the Act, but telephone directories are so specified (Regulations Specifying Publicly Available Information, SOR/2001-7, s. 1(a), which reads: "personal information consisting of the name, address and telephone number of a subscriber that appears in a telephone directory that is available to the public, where the subscriber can refuse to have the personal information appear in the directory").

[51] Section 14 of PIPEDA says simply that a "hearing" at the Federal Court will be granted on the issue raised by the complainant's initial finding: "14. (1) A complainant may, after receiving the Commissioner's report, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, . . .". [Emphasis added.]

[52] See *Englander* v. *TELUS Communications Inc.*, 2003 FCT 705. Online: < http://decisions.fct-cf.gc.ca/fct/2003/2003fct705.shtml>.

[53] See *Englander* v. *TELUS Inc.*, 2004 FC 276. Mr. Englander filed a motion for review of the assessment by a judge but ultimately settled with TELUS out of court.

[54] *Englander* v. *TELUS Inc.*, 2004 FCA 387.

Regarding the payment for non-published number service, the Federal Court of Appeal found the CRTC had made a reasonable decision on the fee and that there is no absolute prohibition on a fee for privacy services, absent evidence of hardship on the customer to pay the fee. The appeal court also decided that under PIPEDA, the court, as well as the CRTC (due to the privacy sections in the *Telecommunications Act*), have overlapping jurisdiction. That is, privacy violations can occur in any regulated industry and that the regulation of that industry by another Act by a dedicated regulatory tribunal does not automatically oust consideration of Canadians' privacy rights under PIPEDA in a court of law.

Finally, and most significantly, the Federal Court of Appeal essentially said the Privacy Commissioner's findings are not "decisions" in the usual administrative law sense, that is, they are to be given no deference at all. This is tantamount to saying that these findings are legally worthless, although they are perhaps persuasive in the sense of convincing a company to change practices through media exposure and pressure from the OPCC. However, with a "no names" policy, Canadians must simply trust that the understaffed and overworked OPCC is appropriately pressuring business to respect PIPEDA.

Mr. Englander's efforts have been described by a well-respected privacy consultant as "quixotic". They can also be seen as brave, selfless and so far, vindicated. However, without Mr. Englander's indomitable resolve, his own status as a lawyer (he did his own legal work, saving tens of thousands dollars a regular complainant would have to pay) and his clear presentation of the issues, this justified case would have been buried under PIPEDA's soul-crushing procedure. At the very least, we call upon the drafters of the PIPEDA revision to adopt a rule/guideline that costs on a PIPEDA application will not be awarded against an individual unless the individual proceeded on an unreasonable basis. Otherwise how are PIPEDA cases going to get to court? And court, as we have seen, is now confirmed as the only place PIPEDA is actually law and likely to be respected.[55]

UNLISTED NUMBER DISPLAY

Another case involving CRTC-approved services in conflict with PIPEDA is finding #172. Again involving unpublished numbers, the complainant here had long had an unlisted number but was surprised when her name and number were revealed on call display. The telecommunications company involved informed

---

[55] At the time of writing, the Federal Court of Appeal has issued a direction to TELUS to come up with a plan for meeting the new consent requirements under the decision. TELUS has not confirmed that it will not appeal to the Supreme Court of Canada. The OPCC (which appeared as an intervenor to argue the jurisdiction issue, the "standing" issue and the deference issue. On this last issue the OPCC essentially argued *against* Mr. Englander) may not appeal the decision, as it did not act as a "party" during Mr. Englander's solo appeal.

new subscribers of this possibility.[56] This time the Privacy Commissioner of Canada sided with the complainant that a reasonable person would have expected per line call blocking to be a part of unpublished number service. He suggested the company return to CRTC to get a new decision on call-blocking and unpublished number service. This was naïve as to the extent to which the company in question would listen to the OPCC. The telecommunications company has brought no application to the CRTC and the OPCC has not followed up. It appears this issue simply will be ignored.

CREDIT CHECKS AND SINS FOR PHONE SERVICE

A spate of telecommunications cases raised the serious consumer problem of credit checks for telecom services and the routine collection of SINs by telcos. First is finding #204, where a telco required a Social Insurance Number (SIN) for identification and credit checks. This case involved the same telco as that in a well-founded complaint regarding performing a credit check even after being told not to by the customer because the company did not have a pre-authorized payment plan (#193). In finding #204, the Commissioner said the complaint was not well-founded, as the telco had by then the option of a pre-authorized payment plan, and had given the complainant a "choice" of ID to prove identification and for the credit check. However, the "choice" of ID was between the SIN, a driver's licence number and a health card number. These are all extremely sensitive items of personal information that all can be used to perpetrate identity theft.

In additional comments to finding #204, the Commissioner railed against the use of the SIN as a "de facto" identifier and suggested Canadians not provide it for this purpose. This finding therefore would have confused the complainant, for if asking for the SIN was unnecessary and invasive, how could having a "choice" of other sensitive ID not be well-founded? The OPCC has since confirmed in a document titled: "Best Practices for the use of Social Insurance Numbers in the private sector"[57] that the SIN is not even required by credit bureaus to perform credit checks, as its purpose is only identification. In addition, this document states that consumers should not provide SINs for identification unless they are informed the SIN is optional and are given a chance to opt out of providing a SIN and still receive the service with several identification options. We see no difference between the SIN and drivers' licences or worse yet, health card numbers.

---

[56] As summarized in finding #204, the company explained the CRTC's reasoning for not requiring automatic call information blocking for unpublished numbers: "The CRTC observed that providing call blocking to all non-published number subscribers would significantly erode both the value of the call display service and the effectiveness in reducing annoying and offensive calls. The CRTC concluded that a net benefit would be achieved by such a service and that it was in the public interest to approve the service."

[57] Online: < http://www.privcom.gc.ca/fs-fi/02_05_d_21_e.asp>.

Transportation

Most of the significant transportation cases involve the overcollection and improper disclosure of personal information to national security and related entities.

Transportation providers (especially airlines) have been subject to intense pressure after the events of September 11 to provide personal information to national security forces. Airlines, under new legislation must provide personal information known as "Advance Passenger Information/Passenger Name Records" (API/PNR) to national transportation security agencies. However, the privacy complaints under PIPEDA show that such a thirst for knowledge of travelers predated September 11 and extends to other transportation customers and even to pilots, despite privacy law safeguards in PIPEDA that seem in direct conflict.

First was an "incident report"[58] entitled: "Transportation company collects, discloses passengers' personal information".[59] It involved the issue of overcollection of personal information including date of birth and citizenship and their provision by the railway to U.S. Customs and Immigration authorities when a customer booked a train ticket to New York from Toronto. The finding is dated April 21, 2001, thus prior to the September 11 attacks.

The Privacy Commissioner found the practice of sharing the information for cross-border customs and immigration purposes without notice to, or consent of, the individual to be in violation of PIPEDA. The finding made clear that such information should only be obtained with the "informed consent" of the traveler, that is, the traveler should know of the customs and immigration uses before consenting.

The second finding involved the heart of the matter of (especially U.S.) national security concerns affecting Canadians' privacy rights under PIPEDA. In finding #106, a pilot complained his airline was requiring him to sign a U.S. information authorization form in order to have flight simulator training in the U.S. The simulator training was necessary for the pilot to stay certified. The U.S. form essentially allowed unlimited information gathering about the pilot and virtually unlimited sharing of the information among government and private parties in the U.S.

The Privacy Commissioner took the strong stand that the requested scope of authorization clearly would violate PIPEDA's principles on many fronts. He ruled

---

[58] The OPCC website describes the incident reports as follows: "Incidents are matters that come to my attention through various sources including issues raised in the media. These are usually issues where there is no identified victim and where no complaint has been filed. During the past 11 months my Office has looked into the following two incidents." It is notable that the "incident findings" now appear only to be reported in the Annual Reports and not in the "incident reports" or "findings" section of the website.

[59] See online report at: <http://www.privcom.gc.ca/cf-dc/cf-dc_010420_e.asp>.

the pilot could not be forced to choose between his job and this violation. In making this decision, the Privacy Commissioner noted the pilot already had Canadian security clearance that the U.S. would not accept as adequate for these screening purposes. The Privacy Commissioner recommended the airline make alternate training arrangements in another country.[60]

The third finding (#148) involves overcollection and improper use of personal information requested of a customer trying to recover lost luggage. The airline form for luggage tracing required Social Insurance Number, date of birth and occupation among other information. The complainant gave this information to the airline involved but made a complaint to the OPCC. The finding made the observation that much of the information should be optional. However, the important aspect was that the Privacy Commissioner found the complainant was not clearly informed that the information "would be filed in a tracing system used by air transport organizations worldwide and would thus be accessible to other parties." He found the consent to use the information and disclose it was thus invalid. However, the case shows how the extensive information processing technology available to transportation companies, together with an attitude of "more information = more security",[61] makes the transportation sector a dangerous place for privacy rights.

In sum, therefore, to this point the OPCC has been quite strong in defending consumer's privacy rights where they would be whittled down in the context of national security.

In the OPCC's 2003-4 Annual Report, Privacy Commissioner Jennifer Stoddart made the observation that security measures are a grave threat to privacy in these words:

> Personal information about Canadians continued to be gathered, stored, sorted and shared in alarming amounts on the basis of the idea – however unproven – that more information about individuals equals greater security against terrorists and other threats. We are concerned about the increasing integration of our border security with that of the United States, and the impetus this gives to the collection of large databases of personal information about travellers, potential travellers, and people in the transportation industry who must cross borders regularly to do their jobs. Our Office is looking very closely at the personal information handling practices of the newly created Canadian Border Services Agency.

---

[60] Another very similar complaint was #128, which involved overcollection and improper destruction of passport photocopies of airline crewmembers traveling to the U.S. in order to meet U.S. aviation security legislation. This complaint was also well-founded, but for different reasons. The Commissioner accepted U.S. aviation security requirements as a legitimate purpose, but faulted the airline for adding in another unspecified administrative purpose and for improper safeguarding of the information.

[61] See OPCC Annual Report 2003-4, p. 8.

However, an amendment to the *Aeronautics Act* was passed in 2004 that essentially removed the ability of the OPCC to investigate complaints of API/PNR collection.[62] Meanwhile, a separate amendment to PIPEDA arguably removed the ability of the OPCC to investigate any collection, use or disclosure of information for national security-based purposes.[63] Despite the Privacy Commissioner's condemnation,[64] this latter amendment to PIPEDA appears set to close the door on the OPCC real ability to make such national security findings.

Consumers may have actually seen a high-water mark in terms of protection of personal privacy to counter-balance anti-terrorism and national security efforts in the first three years of PIPEDA's existence.

ISPs

Internet Service Providers are largely unregulated by the CRTC.[65] However, they were subject to PIPEDA in that they were found, under a Canada Industrial Relations Board ruling, [66] to be telecommunications companies and therefore "federal works, undertakings, or businesses". There were 5 findings concerning ISPs during the period 2001-2003. However, one of these stands out as meriting attention for what it shows of the limitations of PIPEDA.

CARTER V. INTERLOG (INTER.NET CANADA) AND HOSTAGE E-MAIL

Nancy Carter had a billing dispute with her ISP, Interlog, which was bought during the dispute by Inter.net Canada. During this dispute, Inter.net Canada suspended her account, but withheld her e-mail. Ms. Carter alleged she missed a job opportunity that required an e-mail response. Upon learning that her e-mail was withheld, and finding the e-mail requesting her response for the job, Ms. Carter also discovered lack of direct regulatory control over ISPs.

However, Ms. Carter felt that withholding e-mail was an improper use of her personal information and alleged that Inter.net had not made this policy clear to her in her contract, meaning they had no consent for this use of "holding e-mail hostage". She made a complaint to the OPCC. Ms. Carter also talked to the media about the case and to the Canadian Association of Internet Providers. As a result, of her advocacy, Ms. Carter implies she was threatened with a lawsuit

---

62 See *Public Safety Act, 2002*, s. 5, enacting new ss. 4.7 and 4.8 of the *Aeronautics Act*.

63 See *Public Safety Act, 2002*, s. 98, amending the exceptions clause (s. 7) of PIPEDA.

64 See the comments of Jennifer Stoddart, Privacy Commissioner of Canada, to the Senate Standing Committee on Transport and Communications on Bill C-7, the *Public Safety Act, 2002*, March 18, 2004. Online: < http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp>.

65 See Public Interest Advocacy Centre, "Consumer Issues with Internet Service: Is Industry Self-Regulation Working?" (August 2004). Online: < http://www.piac.ca/PIAC_ISP_Report.pdf>.

66 See *Island Telecom Inc. et al.*, Decision no. 59, February 24, 2000. Online: <http://www.cirb-ccri.gc.ca/collections/publications/decisions/RD0059_b.pdf>

by Inter.net Canada for publicizing her case in the media and, in part, for attempting to vindicate her privacy rights before the OPCC.[67]

The Privacy Commissioner in finding #66 agreed with Ms. Carter's characterization of e-mail as personal information and that Inter.net Canada had not made the withholding purpose clear. Her complaint was well-founded on those grounds. However, the finding went on to note that Inter.net Canada had changed its agreement during the OPCC investigation to state this purpose when an account went into arrears. The finding therefore found that this new agreement would be in technical compliance with PIPEDA. The finding went on, however, to offer a suggestion of "best practices" for ISPs to "deflect" not store e-mails from suspended accounts and to ensure that subscribers had access to the stored e-mails despite the suspension of the account.

It is notable regarding the holding of e-mail hostage that the individual has a right of individual access to personal information. In the note that accompanies the statement of that right (Principle 4.9) it is stated: "In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific." Examples are then given, but none suggests a situation similar to holding e-mail "hostage" or any sort of leverage in billing or other disputes with customers.

This statement of best practices therefore seems inadequate.

Inter.net Canada's dial-up Service Agreement still asserts the right to hold suspended account e-mail hostage.[68] It reads:

> Upon suspension:
>
> (i) Inter.net Canada will continue to gather and retain any mail or other files on our servers until end of suspension; and
> (ii) all of your files including, but not limited to, e-mails and homepages will not be erased, but access will be denied.
> The suspension of your subscription does not relieve you from any amounts owing Inter.net Canada before such suspension becomes effective plus any costs including, but not limited to, costs incurred for the collection of any outstanding amounts.

Nancy Carter took her case for "enforcement" of the OPCC finding to the Federal Court and asked for damages for the e-mail withholding privacy violation. Only the Federal Court, not the Privacy Commissioner, can award damages. Ms.

---

[67] See Affidavit of Nancy Carter, filed in Federal Court of Canada, Court File No. T-1745-02, online: <http://www.lexinformatica.org/liability/carter/carter_affidavit.html>.

[68] See Inter.net Canada :: Service Agreement. Online: < http://www.ca.inter.net/en/join/agreement.php>/

Carter has settled her case with Inter.net Canada.[69] However, for others who are going to face a similar problem, the only prospect for recovery is the same painfully long route and possible personal legal complications. This can only chill similar privacy complaints.

Given the access right under PIPEDA to the personal information, the huge number of consumers who use e-mail and the potential consequences of the withholding of e-mail, the intimidating atmosphere for individuals of legal threats for going to the OPCC and the necessity to go to federal court for damages, there should be a proactive concern on the part of the OPCC to ensure that the practice of holding e-mail hostage is halted. The ideal method for this enforcement would be an audit under s. 18 of PIPEDA. To date no audit has been commenced, nor is there any indication of follow up of the "best practices" in the industry.

Further, it appears PIPEDA should include a clear statement of the illegality of withholding personal information to extract consumer payment. A retaliation lawsuit shielding provision should be contemplated to protect individuals going to the OPCC. A private right of action should also be considered, allowing individuals to go to a consumer-friendly court, such as small claims, to get compensation for losses attributable to privacy violations. Alternatively, the OPCC should finally be given power to fine offenders and require payment to complainants, as well as order-making power to ensure compliance.

Physicians' prescribing habits, IMS Health and "work product"

The issue of professional "work product" or, in other words, the personal clues about a doctor, lawyer, dentist or other professional based on the conduct of their practice is a disturbing one. Although not an issue affecting consumers directly, the resolution of this question had the potential to limit what was considered "personal information" under PIPEDA. If a complaint does not meet this initial threshold, that it is "personal information", the OPCC will state it has no jurisdiction and be unable to make even a finding. Consumers have an interest in defining person information as broadly as possible in a world where buying habits and other daily routines are monitored and tracked by business. Unfortunately, in finding #15, the issue of "work product" was decided in a way that may limit consumer use of PIPEDA for controlling such "profiling". It was also decided in a way that distinctly did appear to tread on doctors' personal privacy.

---

[69] See a discussion of her case in S. Lott, "Corporate Retaliation Against Consumers: The Status of Strategic Lawsuits Against Public Participation (SLAPPS) in Canada", Public Interest Advocacy Centre (August 2004) at 19-20. Online: <http://www.piac.ca/SLAPPS.pdf>.

IMS HEALTH CANADA INC. COMPLAINT

Prescribing habits of physicians are tracked by companies to provide the data to drug companies for marketing and, to a lesser extent, for purposes related to medical research. There are two ways that such companies can obtain copies of physicians' prescription information: either directly with the consent of the physician or indirectly by approaching pharmacists for the information. In both cases, the data is aggregated and "de-identified" to remove personal patient details in an effort to avoid divulging personal health information. The Canadian Medical Association thinks the indirect method of obtaining the prescribing information is wrong. They decry the lack of consent of the physician, who is charged with protecting patient confidentiality and they are also concerned with the disclosure of information about the physicians' prescribing habits, which they claim is a reflection of their method of practice.

The OPCC does not agree with the physicians. The OPCC decided that the physician's prescribing habits, once the information was aggregated and de-identified, was not personal information of the doctors. In other words, this collection, use and disclosure of information was not covered by PIPEDA, as it did not fit the definition of "personal information"[70] in s. 2 of the Act.[71]

This complaint, brought against health "data miner" IMS Health Canada by a competitor, decided that such information was "work product" of a professional and not included in the definition of personal information.[72] In the IMS decision, the OPCC created the concept of "work product" in the sense of being something that was an exception to the concept of "personal information". Note that there is no definition of "work product" in PIPEDA and the concept appears borrowed from the law of evidence, and privilege in particular. The IMS decision did not attempt to define "work product" exhaustively, despite its importance. Instead, the OPCC sought to define the term through example, examples that seem to trivialize the possible importance of the issue:

> If the prescribing patterns of a physician-for instance, a tendency to prescribe one medication rather than another for a given ailment-were

---

[70] Although there is a definition of personal health information in the Act, it ceased to be relevant once transitional provisions for the health sector came into force on January 1, 2002. As noted in PrivacyScan's compilation of the Act in a Note: "The definition of personal health information ceased to have meaningful effect as of January 1, 2002 when personal health information, as a distinct category, became subject to Part 1. As of this date, there is no longer a practical distinction between personal information and personal health information."

[71] S. 2 definition of "personal information" reads:
"personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

[72] OPCC Finding #15 "Privacy Commissioner releases his finding on the prescribing patterns of doctors".

> deemed to be information "about" the physician, then the same determination would logically have to be made about identifiable patterns with regard to the work products arising from a broad variety of other activities.
>
> Does the chef in a restaurant predominantly focus on cooking fish, does she have a heavy hand with the tarragon or use very little salt? Does a contractor tend to use the very newest roofing materials, or does he predominantly stick with what was in vogue 10 years ago? Does a garage mechanic tend to fix only the problem that was reported, or is there a pattern of discovering other purported problems that run up the bill?
>
> Therefore, regarding the patterns discoverable in such work products as personal information could have the effect of precluding many kinds of legitimate commercial consumer reporting that, while clearly of potential value, might fall outside the Act's exemption for journalistic activity.

The CMA policy, on the other hand, gives more realistic examples of the potential for what the OPCC calls “work product” information (prescribing habits) to instead be highly privacy-invasive:

> Release of the data can be a significant invasion of privacy. From the data, one can deduce **physicians' location, income, personal preferences and other very personal attributes**. Although the data are valuable in assessing certain aspects of physician performance, there is great potential for misuse. **Inappropriate conclusions about the performance or the learning needs of a physician** maybe drawn from limited data. Use of the data in this respect must reside with the physician and those in whom he or she has confidence.

A more logically coherent approach to the issue would have been to not artificially curtail the scope of “personal information” at the edges of professional practice but rather to include information produced by a professional that revealed aspects of their personality or work habit. Then, it could have been stated that as a *general* assumption, information actually produced by the professional in practice would normally carry with it *some* implied consent to *certain* uses or disclosures connected with that professional practice. Note that such a definition would allow the collection, use and disclosure of such information where it would be beneficial to the practice of that professional, such as for peer review, or quality assurance. However, as requested in the CMA 1997 Policy on *The sale and use of data on individual physicians’ prescribing*, the uses such as data-mining for individual target marketing of physicians by drug companies would be on a strict, explicit consent-only basis.

Note that in Québec, a change to the Quebec private sector privacy law essentially reversed this ruling. Quebec’s law sets out a mini-regime for dealing

with prescribing or other professional information which permits such use, but only if the professionals are notified of the use and given a periodic opportunity to withdraw consent to use of their aggregated and de-identified personal information.[73] California's Senate presently is considering a similar bill. British Columbia effectively bans the process by prohibiting target marketing to physicians based on this information, as the B.C. College of Pharmacists bylaws prohibit the sale of prescription data linked to physicians.. Manitoba has a similar ban under an agreement reached between the College of Physicians and Surgeons and the Pharmacists regulatory body. In Alberta, the provincial Privacy Commissioner ruled that IMS's practices violated Alberta's *Health Information Act*.[74] These provincial bans suggest a profound unease with the OPCC's broad "work product" definition and an attempt to keep professional information within the ambit of privacy law.

Certainly the approach taken in the provincial legislation described above suggests a more nuanced discussion of privacy rights and "personal information" in the context of one's work or professional practice. The one PIPEDA complaint on this issue should not be the end of the story. The importance of the "work product" definition to the personal privacy of professionals, and the wider implications for consumers of limiting the definition of personal information with regard to such profiling, argue for more investigation by the OPCC. Once again, the OPCC could use its power under s. 18 of PIPEDA to investigate this issue in many data mining industries.

Subject Matter Issues

We turn now from problems with specific industries to those grouped by topic.

SPAM

Despite several sections that would seem to apply to unsolicited commercial e-mail (SPAM) and a clear mandate to look into it (it is often a cross-border use of personal information for commerce), the OPCC has basically done nothing

---

[73] Section 21.1 of *An Act respecting the protection of personal information in the private sector*, R.S.Q., c. P.39.1, which permits use "without consent of the persons concerned" for "study, research or statistical purposes" if the Commission d'accès à l'information receives a written request and provided :

1) that the communication protects professional secrecy, especially in that it does not allow the identification of the person to whom the professional service is rendered, and does not otherwise invade the privacy of the professionals concerned ;

2) that the professionals concerned will be notified periodically of the intended uses and the ends contemplated and will be given a valid opportunity to refuse to allow such information to be preserved or to allow such information to be used for the intended uses or the ends contemplated ; and

3) that security measures have been put into place to ensure the confidentiality of personal information.

[74] See Alberta OIPC, ORDER H2002-003, March 19, 2003. Online: http://www.oipc.ab.ca/ims/client/upload/H2002-003.pdf. Stayed pending judicial review.

proactive in terms of using PIPEDA to control spam. Professor Michael Geist in an important article on enforcement of law against spam outlined the possible sections of PIPEDA being violated and called on the OPCC to use its audit and investigation power to probe known Canadian-based spammers.[75] Given the huge importance of e-mail to consumers and the considerable invasion of electronic privacy occasioned by SPAM, this issue should be looked at systemically instead of awaiting individual complaints.

Video Surveillance

The legal status of closed circuit television (CCTV) surveillance or videotaped surveillance by the private sector is subject to PIPEDA. Public surveillance by a public body like the RCMP is generally covered by the *Privacy Act* and outside the scope of this report.

Things started well. The very first OPCC decision, #1, involved the monitoring of a public street in Yellowknife by a private security company. The Privacy Commissioner ruled this was not permitted, stating "There is no place in our society for unauthorized surveillance of public places by private sector organizations for commercial reasons."

However, while consumers going about their daily business should not have to expect to be monitored by a corporation,[76] they will have to look for signs announcing surveillance while they are on privately owned property, such as shopping malls and banks.

One more surveillance case of an almost sickening nature shows the risks we are taking in not providing the OPCC with order-making power. The title of finding #53 "Bank accused of providing police with surveillance photos of the wrong person" tells it all. In this case the complainant was shocked to see her face in a "Crime of the Week" article in the local newspaper on suspected bank fraudsters. The photos had been provided to CrimeStoppers and from there through the police to the newspaper. However, the bank surveillance tapes had been wrongly time-stamped. Although the finding report suggests all parties were horribly embarrassed and sought to ensure the matter never would occur again, a newspaper retraction was run and other unspecified measures were apparently taken, there is nothing more than the good faith promise to see that

---

[75] See M. Geist, "Untouchable?: A Canadian Perspective On The Anti-Spam Battle", Ver. 1.1 (May 2004). Online:< http://www.michaelgeist.ca/geistspam.pdf>. For example, he notes automatic "harvesting" of e-mail addresses on the web may violate the consent principle; that some SPAM e-mails may require an opt-in consent, or that the sender may not be able to demonstrate a clear opt-out consent.

[76] This report does not detail the saga of the Privacy Commissioner of Canada's attempt to halt video surveillance of the general public by the RCMP in Kelowna, B.C.. This case was pursued under the provisions of the *Privacy Act*, and the OPCC made a decision to drop the case as a "waste of money" (it had cost upwards of $500,000 to advance the case to B.C. Superior Court) and, as the RCMP stopped taping the public area, it may have fallen outside PIPEDA's scope. However, the principle at stake is one of the OPCC's largest challenges.

promise through. Given the disastrous consequences of this type of surveillance disclosure there should be an order mandating follow-up and testing and possibly an industry-wide audit to determine if proper safeguards are in place to avoid this type of situation. Relying on an ombudsman's finding and suggestions for improvement simply is inadequate. Moreover, making an example of this bank, through being named, would have sent a stronger message to the industry.

Eastmond v. CPR Case

The treatment of employee privacy in the face of surveillance under PIPEDA was less stellar. Despite an OPCC ruling that surveillance cameras installed in a Canadian Pacific Railway yard were infringing the privacy rights of workers,[77] Mr. Eastmond and the union filed an application in Federal Court to "confirm" (in effect, enforce) the OPCC decision, but lost.[78] The Federal Court found that the use of cameras in the CP workplace fell under an exception to PIPEDA: investigating a possible crime or breach of a law: "CP may, on the facts of this case, collect the applicant's personal information without his knowledge and consent because CP benefits from the exemption provided for in paragraph 7(1)(b) of PIPEDA." However, despite the narrow basis for allowing the cameras cited in the court case,[79] many other possible justifications for surveillance have been suggested in other OPCC findings as being capable of avoiding employee consent.[80] Given the complications of dealing with employee privacy, it appears the general terms of PIPEDA are too unspecific to deal with the difficult balancing act in this area. Rather than stretching the exceptions to consent in s. 7, or making absolutist pronouncements about surveillance in the workplace, it appears prudent to add a new section on employment privacy to PIPEDA when it is reviewed in 2006.

The Consent Issue

The heart of PIPEDA's privacy rights is found in Principle 3 "Consent". It reads:

> **4.3 Principle 3 -- Consent**
> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

---

77 OPCC finding #114 "Employee objects to company's use of digital video surveillance cameras".

78 *Eastmond* v. *Canadian Pacific Railway*, 2004 FC 852 (T.D.) [*Eastmond*].

79 A similar reliance on the s. 7(1)(b) exception permitted covert surveillance of an employee by an employer for the purposes of discovering if his disability claim was legitimate, in OPCC Finding #268.

80 See OPCC finding #268 "Electronic monitoring does not yield any information, but practice is strongly discouraged" and OPCC finding #273 "After installing surveillance cameras in the workplace, a broadcasting company has agreed to inform its employees about the purpose and to adopt a policy regarding its use".

Consent, and how to get it, has become the legal battlefield of the first three years and now the fourth year of PIPEDA. Upon this principle hang all the law, and its prophets.

The difficulty with PIPEDA's consent sections is that they are confusing and contradictory to some extent. The greatest confusion and most conflicts revolve around the idea of "implied consent", which is effectively when consent is assumed due to the circumstances or the actions or inaction of a person. The only place in PIPEDA the term "implied consent" exists is in Principle 4.3.6, which states express consent should be used for "sensitive" personal information and implied consent may be used for "less sensitive" information.

Businesses have taken the implied consent ball and run with it. If consent can be found, then business can use and disclose personal information for primary marketing (selling more products to you from the same company) and secondary marketing (the disclosure of your personal information to either affiliated companies or other companies for a fee so they can attempt to sell to you). The most common form of "showing" an implied consent is the use of an "opt-out" mechanism. An "opt-out" is an assumption of consent unless the consumer does something to indicate they do not consent. Usually this involves taking the step of notifying the company in some fashion. The issue of safeguards around "implied consent" and obtaining it via "opting-out" came to a head in the complaints filed by PIAC in 2002.

Opt-out Consent and PIAC Complaints

In the PIAC complaints,[81] there were two issues: 1) was there valid consent? (did the consumer have enough "knowledge" of the proposed uses of the information to really consent); and 2) was the use of opt-out consent appropriate? If so, was the opt-out mechanism fair?

The Privacy Commissioner in all the PIAC decisions stated PIAC's concerns regarding consent were "entirely reasonable" and several decisions dealt with the requirements for opt-out consent. In brief, those requirements were that to use opt-out consent, a company should ensure:

(1) [the] purposes are stated in such a manner that the customer can reasonably understand how personal information is to be used or disclosed, in accordance with Principle 4.3.2 of Schedule 1;

(2) [the] intended uses and disclosures are well-defined especially in respect of
- the items or types of information to be used or disclosed;
- the parties to which information is to be disclosed; and

[81] For reports of all the findings and related materials on the PIAC complaints, see: <http://www.piac.ca/privacy.htm>

- the purposes for which information is to be disclosed (e.g., direct marketing);

(3) the customer is directly notified of the opportunity to withdraw consent to specific optional purposes (e.g., direct marketing); and

(4) the customer is provided with, and directly notified of, an easy, immediate, and inexpensive means of opting-out (e.g., a check-off box or toll-free telephone number).[82]

These requirements were clearly stated and repeated as late as OPCC finding #167. However, the principles established in the PIAC cases were eroded by the re-issuing of the Bell Mobility and Bell ExpressVu[83] complaints (and the removal of the original decisions from the OPCC website). The "immediate" requirement for opting out also was watered down by a policy decision of the OPCC, curiously delivered at a speech to the CMA (discussed above).

Now the OPCC has tried to dispel the confusion around the requirements of consent by issuing a Fact Sheet entitled: "Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act". This sheet takes on the consent issue but manages to avoid scrupulously the criteria listed above for appropriate opt-out consent. Instead it adopts the more general discussion principles decided in various findings about when it is appropriate to use opt-out consent as opposed to opt-in consent in the context of sensitive and non-sensitive information. With respect, that is not the central issue in privacy law for consumers and marketers. The requirements businesses must meet to assume they may rely upon opt-out consent is the issue.

Movement to Informed Consent?

PIPEDA already requires "knowledge and consent" of the individual to the collection, use and disclosure of personal information (Principle 4.3). However, OPCC decisions (such as those whittling down opt-out consent requirements) and policy documents like the Consent Fact Sheet discussed above reduce this "knowledge" requirement to mere knowledge of the fact of the collection, use and disclosure.

However, the cases brought to the OPCC and that will be brought to the OPCC will soon require a more stringent consent requirement of PIPEDA. PIPEDA already requires that information be given to the individual about the purposes for the collection, use and disclosure. However, it only requires businesses to make

---

[82] See original Bell Mobility finding at: http://www.piac.ca/Bell%20Mobility.htm.

[83] Although the ExpressVu Complaint was upheld in decision #243, only the full text of the complaint finding provided to the parties (see PIAC's website at http://www.piac.ca/ExpressVuRevised.pdf) actually mentions the immediacy requirement. It is absent in the summary of the finding on the OPCC website.

a “reasonable effort” to bring these purposes to the consumer’s attention (Principle 4.3.2). Frankly, this is no longer good enough, as it does not expect the unexpected: risk.

We now live in a world where information, personal information, can lead to immediate and serious fraud: new scourges of identity theft,[84] “phishing”, modem hijacking[85] and similar scams based on the misuse of personal information. These “adverse events” are increasing and they are serious. Identity theft can lead to thousands in fraudulent credit and withdrawals, denied loan applications, destroyed credit ratings and lost time, effort and huge frustration for people. Disclosure and use of personal information risks having the government have access to it under the “public safety” amendment to PIPEDA discussed above.

Because of these possible “side effects”, “complications” and “adverse outcomes”, it is now incumbent upon those collecting, using and disclosing personal information to inform individuals of the risks associated with such information flows. Individuals are ill-placed to know where the information is likely to go and to whom and should be reasonably informed of this data flow. Companies are better placed to know about data flows.

This also means companies would have to mention “special data risks”, even if the probability is low, if it would cause a reasonable person to think twice about providing the data. Identity theft hopefully would be a special risk, however, depending upon the sensitivity of the information gathered (Social Insurance Numbers and Driver’s Licence numbers are very sensitive), the nature of the communication (e.g., online banking or payment processing), the length of data retention and how it is used, this could even be a usual risk.

Another “special data risk” would be the recent controversy over the outsourcing of personal information to U.S.-based or U.S.-linked data processors.[86] One would have to reveal that the information was potentially available to the U.S. government for national security purposes. This is what the Information and Privacy Commissioner of B.C. recently said,[87] and what one bank has already warned customers about. Although the bank now faces a privacy complaint for informing its customers of this risk, the bank probably did the right thing. What it did wrong was not to discuss it in terms of risk and proper informed consent.

---

[84] See P. Lawson and J. Lawford, “Identity Theft: The Need for Better Consumer Protection” PIAC, (November 2003). Online: < http://www.piac.ca/IDTHEFT.pdf>

[85] See “2004-07-07 - File #: 8665-U11-200407090 - Union des Consommateurs, Public Interest Advocacy Centre (PIAC), Option Consommateurs - Request for CRTC to intervene in "dialers" cases: modem hijackings” CRTC Part VII application. Online: < http://www.crtc.gc.ca/PartVII/eng/2004/8665/u11_200407090.htm>.

[86] See British Columbia, Office of the Information and Privacy Commissioner, Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing (October 2004). Online: http://www.oipc.bc.ca/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf (B.C. Outsourcing Report)

[87] *Ibid.*

A true “informed consent” standard would sweep away these difficulties and would help the OPCC and the courts set clear standards on the requirements business would have to meet to obtain consumer consent.

Five-year review

PIPEDA, unlike most legislation, has a five-year review mechanism in section, s. 29, that requires a House of Commons Committee (or joint committee with the Senate) to review the Act. PIPEDA is due for review starting January 1, 2006. The Committee has one year to report unless the House of Commons extends the review. The law requires this review, and while it does not specify that the law must be changed, or dropped, or strengthened (it could just stay the same), this report argues there should be changes. There is a threat of watering down the legislation to appease business; however, it is possible that business is quite content with the Act as the enforcement is minimal. The result of the non-prescriptive “guideline” nature of PIPEDA, the lack of enforcement powers in the OPCC, the unfriendly consumer aspects of the Act and the strange procedural actions of the OPCC have all added to the frustration of consumers. The public should be invited to, and should take the opportunity to, bring PIPEDA into line with the reasonable expectations that it might actually be a tool to protect their privacy rights.

PART 2

Review of Major Federally-Regulated Business’s adherence to PIPEDA

Review of Privacy Policies and Relevant Contractual Documents of Certain Businesses

In 2002, PIAC initiated complaints against several large corporations in various sectors with regard to the issue of adequacy of the consent obtained for secondary marketing. This portion of the report is a follow-up to determine whether the recommendations, laid out in findings #77 to #83 of the Privacy Commissioner, have been implemented.

The analysis was restricted to examining the corresponding online privacy policies only (relevant sections from these websites have been presented where possible). This is an important point to note given that some of the original complaints originated from paper-based materials and telephone calls. The thoroughness of this follow-up analysis, therefore, is accordingly affected.

All complaints were directed at organizations that PIAC alleged failed to obtain consent for the collection, use, or disclosure of personal information for certain

purposes. Specifically, the organizations' privacy policies were allegedly deficient in three ways:

1. they do not bring to the attention of its customers their practice of using and sharing customer data for secondary marketing purposes;
2. they failed to provide clear information as to potential secondary uses and sharing of customer data; and
3. they do not provide customers with an easy opportunity to opt-out of such uses and disclosures.

For the sake of this analysis, these three issues were sub-classified into two main areas of concern: (1) Secondary Uses; and (2) Opt-out Procedures.

It is of note that the OPCC continues to promote "opt-in" consent as the most appropriate process for organizations to use.[88] However, the OPCC has suggested that "opt-out" consent is acceptable under strictly defined situations only and, where used, must employ the following four conditions:

1. The personal information must be demonstrably non-sensitive in nature and context.
2. The information-sharing situation must be limited and well defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure.
3. The organization's purposes must be limited and well-defined, stated in a reasonably clear and understandable manner, and brought to the individual's attention at the time the personal information is collected.
4. The organization must establish a convenient procedure for easily, inexpensively, and immediately opting out of, or withdrawing consent to, secondary purposes and must notify the individual of the procedure at the time the personal information is collected.[89]

These criteria are relevant in as much as this follow-up analysis indicates that all of the organizations named in the complaints continue to employ opt-out regimes.

The Findings

HBC – Finding #77 & Finding #81

This complaint focused on the Hudson's Bay Company (HBC). However, due to PIPEDA's jurisdiction being limited in the private (largely retail) sector during the

---

[88] See the recent OPCC Fact Sheet "Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act", online: < http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp > (Version accessed Last Updated: 2004-09-28).

[89] http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030723_01_e.asp

first three years of its existence, only the complaint against the division that operates in the Yukon and the Northwest Territories proceeded. In this finding, the OPCC decision was a non-starter for improvements to the company's privacy policy. This is because the Office found that the HBC Yukon and NWT division did not participate in the HBC Rewards Program, and thus, did not collect, use or disclose personal information in connection with the HBC credit card. For this reason, the OPCC concluded that HBC was in compliance with PIPEDA.

SECONDARY USES

Despite this finding, but considering that the entire HBC is now covered by PIPEDA except in provinces with their own privacy acts, there are some issues with the current privacy policy. Although the policy does tell customers it may share the customer data for secondary marketing purposes, it remains unclear as to what the secondary uses may be. For example, the Policy states:

> "Hbc may wish to use the information resulting from your application, and information about your purchases and Hbc Rewards redemptions, to offer or communicate with you about additional products and services provided by Hbc and other organizations with which Hbc has marketing arrangements. These communications may include notifications of sales, special events, store promotions and other exclusive offers."[90]

It is unspecified which elements of the personal information that are gathered through the application and through purchasing qualify for secondary uses and when it is collected. It is also unclear whether the individual is informed at the time when information is collected, if there is ongoing collection, for such uses.

OPT-OUT PROCEDURES

Although an opt-out clause has been added to the policy, it fails to meet the standard promulgated by the OPCC in three ways. First, the Privacy notice[91] on the credit card application buries the opt-out provision in paragraph 55 of 63. Furthermore, it states:

> "Your consent to the use of your personal information for these additional purposes is voluntary and not required as a condition of obtaining or using the Hbc Rewards Card or collecting and redeeming Hbc Rewards Points. If you do not wish Hbc to use this information for these additional purposes, please contact the Hbc Privacy Office…"[92]

---

[90] HBC Privacy Policy, online: <http://www.hbc.com/hbc/privacy/default.asp#rewards>

[91] HBC Rewards Terms and Conditions, online: <http://www.hbc.com/HBCREWARDS/program/default.asp?NAV=ABOUTREWARDS&SUBNAV=&NAVSEL=ACCTER10&TF=ABOUTREWARDS&PG=terms%5Fconditions&PAGE%5FNAME=terms%5Fcond%5FLabel&PAGE%5FLABEL=terms%5Fcond%5FLabel&langid=EN&catid=&imgthu>

[92] HBC Privacy Policy, *supra*.

Second, this portion of the clause in the policy says nothing about the nature or context of the information, the intended use of the information or the limits on such uses. Finally, despite the fact that the policy is available online, there is no online resource for opting out.

Loyalty Group (AIR MILES) – Finding #78

The OPCC concluded that the complaint against AIR MILES was well-founded. The recommendations have been implemented with some success.

SECONDARY USES

AIR MILES makes it clear that it shares information only within the Loyalty Group. The definition of this group, however, reveals a very broad range of activities that lack in specificity in terms of purpose.

> "The Loyalty Group - the creator and manager of the AIR MILES® Reward Program and the AIR MILES For Business Program® in Canada. In addition, The Loyalty Group operates other businesses including EXTRA MILE TRAVEL™, EXTRA MILE Flowers™, EXTRA MILE Books.com™, AIR MILES INCENTIVES® and Loyalty Consulting™."[93]

All of the above "programs" are related businesses or disclosure networks that will use the customer's personal information. However, we feel that to an average reader the drafting of the above clause does not specify the nature of these secondary businesses. It also can be read in a manner suggesting only that the Loyalty Group does business with these outfits but not necessarily that information will be shared with all of them as if they were within one company. As such, we think this information falls short of fulfilling the OPCC's recommendation requiring AIR MILES to accurately define its disclosure activities.

OPT-OUT PROCEDURES

The policy does provide an opt-out provision.

> "2.3 AIR MILES® Collectors can opt out of receiving marketing and promotional communications in electronic, printed or verbal format, other than AIR MILES Collector…"[94]

But, once again, it is difficult to understand what secondary uses a customer can anticipate. Further on, there is a comfort clause meant to describe the disclosure of personal information. Although there is a description of the loyalty partners as "business units" of the Loyalty Group, this description is located many clauses after the opt-out provision and again it is necessary for the reader to return to the definition of the Loyalty Group and to read it the right way:

---

[93] https://www.airmiles.ca/servlet/ContentServer?pagename=Airmiles/Visitors/PrivacyCommitment
[94] *Ibid.*

> "5.1 The Loyalty Group does not give, rent or sell Collector lists from the AIR MILES® Reward Program to any organization or individual other than business units of The Loyalty Group, Sponsors of the AIR MILES® Reward Program, and companies contracted to process and manage Collector transactions, redemption requests and communications.
> In addition, a Collector's specific transaction information from one AIR MILES® Sponsor is not disclosed to any other AIR MILES® Sponsor."[95]

Despite the fact the Privacy Commissioner's recommendations in the AIR MILES finding called for an opt-out check box or toll free number on the AIR MILES online application form, none exists. However, there is a check box that asks the customer to read the privacy policy. This box must be checked before the card can be processed.

Bell Findings – # 79 (now Bell Mobility Case #243 & Bell ExpressVu Case #244), and Bell Nexxia Case #80

It should be noted that these complaints were initially directed to "Bell Canada" and then broken into complaints against four discrete lines of business, all Bell operations: Bell Canada (telephone); Bell Mobility (wireless), Bell ExpressVu (satellite TV) and Bell Nexxia (business services). One may be excused for the error in approaching Bell as a monolith in that all of these businesses currently link to the same online privacy documentation. In the original complaints, Bell Mobility[96] and Bell ExpressVu were both found to be non-compliant with PIPEDA. On the "review" of these decisions, discussed above regarding OPCC procedure, only Bell ExpressVu was found to be non-compliant.

SECONDARY USES

To begin, the Bell website has several different links regarding privacy, and it is not readily evident which links provide relevant information. That aside, the secondary uses are laid out in the following paragraph:

> **"Other Parties with Whom the Bell Companies May Share Personal Information**
> While our general policy is not to provide personal information to any party outside of the Bell companies, there are certain limited circumstances, outlined below, in which it is necessary to do so. When we do provide personal information to third parties, we provide only that information that is required in the circumstances. Information provided to third parties is used only for the purpose stipulated and is subject to strict terms of confidentiality. Employees of the companies to whom we may provide information must adhere to our privacy standards. Third parties include:
> **An agent acting on behalf of Bell,** such as a company hired to perform installation or maintenance on our behalf;

[95] *Ibid.*
[96] See the original, full finding on Bell Mobility at: http://www.piac.ca/Bell%20Mobility.htm.

> **Another communications service provider,** in order to offer efficient and effective communications services (e.g., to provide wireless service while roaming in another company's coverage area);
> **A collection agency,** for the express purpose of the collection of past due bills;
> **Law enforcement agencies,** in emergencies, for internal security matters, or where required by court order or search warrant; and
> **Emergency services,** in emergency situations."[97]

Of course, like the Loyalty Group (AIR MILES) above, Bell companies comprise a vast array of business activities and it would be helpful to know how far these activities extend. Depending on the extent of use and disclosure within the Bell-affiliated entities, it may not be reasonable for an average person to fully comprehend the scope of potential use and disclosure among this group. This could effectively remove the "knowledge" and consent of the customer to secondary purposes.

OPT-OUT PROCEDURES

Opting out is considerably easier on the Bell site (when compared with the others in this analysis), with the user being provided with a direct link to this facility on the main privacy page.

> "Your personal information will not be used for any other purpose without your consent.
> We share information among the Bell companies to help us identify your information, communication, and entertainment needs, and provide you with relevant information, advice, and solutions to meet those needs.
> If you don't want your information shared among the Bell companies, Click here to "opt-out"."[98]

We are pleased with Bell's immediate, accessible opt-out mechanism. We are less than impressed at the level of detail provided regarding use and disclosure within the Bell-affiliated companies.

Scotiabank – Finding #82

The OPCC decision indicated that the material presented by Scotiabank, as well as the process, did constitute a reasonable effort to advise the individual of secondary uses. As such, the OPCC decision made recommendations *for improvement* only.

---

97 "Bell Customer Privacy Policy" at 4-5 <http://www.bell.ca/shop/en/jsp/content/cust_care/docs/bccpp.pdf>.

98 http://www.bell.ca/shop/application/commercewf?origin=noorigin.jsp&event=link(goto)&content=/jsp/content/cust_care/privacy_home.jsp

Like the Bell cases above, however, Scotiabank had several different privacy links that have the effect of obfuscating content. The material was found to be scattered and difficult to locate.

SECONDARY USES

Similar to the AIR MILES provision regarding the Loyalty Group (or the Bell companies), Scotiabank employs a similarly broad term to define with whom they may share the information. It would be helpful to know exactly who are Scotiabank Group Members in the following provision:

> "5. We may give information (except health information) about you to other Scotiabank Group Members (where the law allows this) so that they may tell you about their products and services. The Scotiabank Group includes 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."[99]

OPT-OUT PROCEDURES

The opt-out clause included below has two outcomes. First, the language is negatively construed to indicate that opting out could have a detrimental impact on the ability to continue to provide the customer with services and/or products. Second, the clause does not provide a simple way to opt-out as would be recommended by the OPCC under these circumstances.

> "**Refusing or withdrawing Consent:**
> Subject to legal and contractual requirements, you can refuse to consent to our collection, use or disclosure of information about you, or you may withdraw your consent to our further collection, use or disclosure of information at any time in the future by giving us reasonable notice, provided the consent does not relate to certain information required for credit products or arrangements or insurance underwriting or claims which you apply for or accept (see below). If you refuse or withdraw your consent, we may not be able to provide you or continue to provide you with some products, services or information which may be of value to you.
> You can tell us at any time to stop using information about you to market our products and services or to stop sharing information with other Scotiabank Group Members
> If you wish to refuse consent or to withdraw consent as outlined within this agreement, you may do so at any time by contacting the branch or office of the Scotiabank Group Member with whom you deal."[100]

---

[99] http://www.scotiabank.com/cda/content/0,1608,CID847_LIDen,00.html
[100] *Ibid.*

The policy discusses identifying purposes but does not necessarily specify what these purpose are. In addition, because information is scattered throughout the site, more opt-out information is found under the link “Principle #3: Getting the Customer’s Consent”.

> “3.5 Subject to legal and contractual restrictions, customers can refuse or withdraw consent at any time as long as:
>
> - The Scotiabank Group Member is given reasonable notice of the withdrawal.
> - Consent does not relate to a credit product where the Scotiabank Group Member must collect and report information after credit has been granted. This is to maintain the integrity of the credit system.
> - Consent does not relate to the underwriting of an insurance policy, or an insurance claim where the Scotiabank Group Member must collect and report information after the application has been underwritten or the claim has been adjudicated. This is to maintain the integrity of underwriting and claims systems.
>
> The Scotiabank Group Member will let the customer know the consequences of refusing or withdrawing consent when customers seek to do so. Refusing or withdrawing consent for the Scotiabank Group Member to collect, use or disclose personal information could mean that the Scotiabank Group Member cannot provide the customer with some product, service or information of value to the customer.”[101]

As is evident in this paragraph, the Scotiabank approach is consistent, insofar as the customer is warned about how opting out may negatively impact service/product delivery. This provision, however, goes further by mandating reasonable notice – as required by principle 4.3.8 of PIPEDA.

MBNA Canada – Finding #83

MBNA Canada has updated its policy to incorporate one of the three of the OPCC’s recommendations.

First, the decision recommends that the MBNA Canada identify what personal information is to be disclosed, and how exactly the personal information will be used. To this end, the online privacy policy contains two comprehensive tables. The first table indicates the source, the type of personal information, and the proposed use. The second table indicates the types of companies with whom the information will be shared and how it will be shared.

Second, the OPCC recommends that third parties who will use the information be identified. The tables do identify the types of third parties (e.g. retailer, direct marketers, etc.) but do not mention the names of such organizations.

---

[101] http://www.scotiabank.com/cda/content/0,1608,CID887_LIDen,00.html

Third, MBNA Canada may fail to meet reasonable expectations of customers for an immediate, easy, and inexpensive way of withdrawing consent to optional, collection, use, and disclosure. As mentioned above, the online credit card application form does have a link to the privacy policy; however, it still does not provide a checkbox or way to easily opt-out. This must be done by contacting MBNA Canada.

SECONDARY USES

The online credit card application form contains a link to MBNA Canada's Privacy policy. It seems as though this facility did not exist at the time of the original complaint. The purpose of the collection is outlined below.

> **"Personal Information Collection, Protection, Use, Sharing, and Retention**
> We collect, protect, use, share, and retain personal information to:
> a) evaluate, monitor, maintain, service, and collect any account you may have with us, including disclosing or exchanging Personal Information with credit reporting agencies, to develop our relationship with you, and to offer financial products and services, including evaluating the needs, wants, and satisfaction levels of our customers and analyzing and managing our business;
> b) administer services, monitor your purchases, transactions, payments, and evaluate your credit eligibility, for the purposes set out in this notice;
> c) verify your identity (or that of any authorized user or co-applicant) concerning the account and maintain security measures aimed at the detection and prevention of fraudulent activity in relation to your account;
> d) comply with legal and regulatory requirements;
> e) promote and market products and services offered by MBNA, or by carefully selected companies, which are directly related to the account (such as balance transfers and alternative payment methods), including by means of direct marketing; and
> f) promote and market products and services offered by selected companies which are not directly related to the financial product or service we are providing to you (also known as secondary marketing), such as long distance or cellular telephone service, credit insurance, and card registry services."[102]

As mentioned above, the tables more accurately depict what information is being collected, what is shared and how it is used.

[102] http://www.mbna.com/canada/privacy.html

OPT-OUT PROCEDURES

As noted, MBNA Canada still requires customers to opt-out by contacting their customer service, not by providing and immediate, easy opt-out at the time of signing up. However, it is laudable that MBNA Canada attempts to draw the reader's attention to its opt-out provision as the paragraph below is in bold and boxed in so as to stand out from the other content. The time period for effectiveness of the opt-out (5 days) is reasonable, however, the 90-day "marketing campaign" cycle extension seems quite long. The wording is awkward, as well. No one, except perhaps the guinea pig in *Alice in Wonderland*, likes to be suppressed.

> "You may ask to be suppressed under (e) and/or (f) at any time after your account has been opened by calling MBNA Canada at 1-866-845-0980 or by writing to us at MBNA Canada, Privacy Officer, P.O. Box 9660, Station T, Ottawa, Ontario K1G 6M9. In accordance with your request, and within 5 business days, we will suppress you from direct mail marketing and telemarketing for products and services offered by MBNA, or by selected companies, which are directly related to the financial product or service we are providing to you and/or we will suppress you from direct mail marketing and telemarketing for products and services offered by select companies which are not directly related to the financial product or service we are providing to you. Please allow 90 days for full effect as marketing campaigns may already be in process. This will not limit information we may provide to you in statements or when you contact us."[103]

The next paragraph indicates that opting out may result in discontinuance of providing services or products (see Principle 4.3.8).

> **"Additional Detail: Consent**
>
> In your application for the financial product or service we are providing to you we obtained your consent for personal information collection, protection, use, sharing, and retention as set forth in (a) through (f) above. Subject to legal and contractual restrictions, you may withdraw your consent at any time after your account has been opened with reasonable notice. This will not limit information we may provide to you in statements or when you contact us. If you refuse or withdraw your consent for any purpose required to provide our financial product or service to you, we will no longer be able to provide that product or service to you. You understand that if you withdraw your consent at any time to the monitoring of your credit status or your ongoing eligibility for credit, MBNA may no longer be able to maintain your credit account."

[103] *Ibid.*

This is a straightforward explanation of the principle that a company should explain consequences of withdrawing consent.

Conclusion

The companies directly targeted for privacy complaints by PIAC in the past appear not to have completely changed their ways regarding customer consent for secondary marketing purposes. Nevertheless, these policies are entirely typical of their industries.

We found continuing confusing language in privacy policies of these companies, much of it buried deep in pages of legalese. We found continuing reference to secondary privacy policy or similar documents, unlinked to main contractual documents or which were hard to navigate to during a consumer transaction. We found many companies continue to not have an easy or immediate opt-out procedure.

In particular, we wish to note that the Ontario Information and Privacy Commissioner and Canadian Marketing Association's Joint Report "Incorporating Privacy into Marketing and Customer Relationship Management"[104] cited two of the companies studied for having the "current best practices in Canada" for "privacy policies and practices": Hudson's Bay Company and the Loyalty Group (Air Miles). We don't think so.

The AIRMILES program has an unclear definition of affiliated companies. This raises an issue with companies that write tight privacy policies but "cheat" on undefined terms and in particular, do not fully specify where the information will be shared. This also applies to companies with networks of affiliates, like Bell or Scotiabank, or MBNA Canada, that lists only general categories. This type of drafting leads to the conclusion that consumers would be better served by an "informed consent" standard under PIPEDA argued for above. With "informed consent" the company involved would be required to explain the likely results of giving consent, including the usual recipients of such data (as well as the risk of other "unusual" recipients obtaining the data – for example through data loss and subsequent identity theft). In the case of the Bell companies, they also appear to have avoided complying with an immediate online opt-out check-box suggested in the Privacy Commissioner's original finding. There is more on this issue below.

As for HBC, the failure to meet the standards for opt-out consent is more prosaic. It buries the opt-out clause 58 pages deep in a 63 page jargon-filled policy. This opt-out clause does not specify the nature of the information to be used in this section. That information is found in an entirely different portion of the document. We think an average consumer, in order to exercise his or her right to opt-out in

[104] Online at <http://www.the-cma.org/media/downloads/CRMPaper.pdf>

an informed manner, should have the description of the information collected (and its uses and likely disclosures) beside the opt-out clause. Finally, the lack of an online method for opting out of an online procedure causes a different concern.

As noted above, the OPCC seems to have retreated from the position that consumers should have an *immediate* opportunity to opt-out of secondary marketing. While this is a loss of some proportion to consumers, we would be content if there were a rule requiring that the immediacy of the opt-out match the immediacy of the deemed consent. For example, a transaction geared to be delivered instantly online, such as HBC's Rewards Program, AIR MILES, or indeed even a requirement to "register" at a newspaper site to see articles,[105] should provide for immediate opt-out. A transaction carried out in the mail could require time for the mail to be delivered and processed. Telephone orders would be somewhere in between to allow reasonable time for transcription of the oral opt-out to be added to the mailing list and other business systems. As more and more of the consumer transactions of these businesses is driven to online or other electronic access, the consumer should also benefit from the electronic nature of the transaction and not have his or her "consent" to secondary or other marketing assumed by a computer system during a "hostage" period.

Overall, therefore, the reaction of companies to PIPEDA has been to write privacy policies, but the mere writing of these documents does not guarantee that their content or the business process they force on consumers aligns fully with the requirements of PIPEDA. Until the OPCC undertakes an investigation and audit of major retailers and other businesses, which now seems increasingly unlikely, the onus will be on consumers to initiate privacy complaints under a system that seems designed to ultimately squelch dissent and preserve the information flow *status quo*.

---

[105] In this regard PIAC notes that, for example, the Toronto Star newspaper now requires (instant, online) registration to see articles but notes in *TheStar.com Privacy Policy* regarding opting out that:

> If you do not wish to receive Marketing Offers, you may opt-out at any time by doing any of the following:
>
> follow the instructions at the bottom of any email Marketing Offer you receive.
> inform your telemarketer at the time you are called with a Marketing Offer.
> call Customer Service at 1-800-279-0181 and request that your personal information not be used for Marketing Offers.
> email Customer Service at privacy@thestar.com and request that your personal information not be used for Marketing Offers.
>
> **Please allow a reasonable time (approximately 2-4 weeks) for processing of your request.** Please provide your full name, home address and telephone number in order that we may properly process your request.

Online: <http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Render&inifile=futuretense.ini&c=Page&cid=972514122141&pubid=968163964505>