Securing Compliance, Protecting Privacy

The PIPEDA Enforcement Evaluation Research Project

Submitted by the B.C. Civil Liberties Association (bccla.org)

To the Office of the Privacy Commissioner of Canada

Under the Contribution Program 2005-06

Principal Researcher and Author	Kirk Tousaw, Barrister & Solicitor
Project Supervisor	Murray Mollard, Barrister & Solicitor BCCLA Executive Director

March 2006

Table of Contents

PIPEDA – ENFORCING PRIVATE SECTOR PRIVACY:
A report by the British Columbia Civil Liberties Association

Executive Summary

This report contains an extended analysis of the *Personal Information Protection and Electronic Documents Act.* The choice of the ombuds-model is discussed and critiqued. PIPEDA is compared to other privacy legislation within Canada and, specifically, to the provincial private sector laws in Quebec, Alberta and British Columbia. PIPEDA is also compared to models in use in Australia and New Zealand. Finally, the PIPEDA model is compared to other non-privacy administrative legislation in Canada, specifically in the fields of human rights and telecommunications regulation.

Ultimately, the Association concluded that while the OPC presently has a significant commitment to privacy protection, the tools at its disposal are insufficient. Increasing the power available to the OPC would, in the Association's view, move the regulated parties toward more substantial compliance with the law. A number of potential reforms are discussed in the final section of the report and several recommendations, summarized below, are suggested.

Summary of Recommendations

A Reforms Requiring No Change to PIPEDA

Recommendation 1

Establish a policy preference for the use of agreed statements of facts in investigation reports.

Recommendation 2

Implement a formal policy ensuring that each party has a full opportunity to respond to the other party's factual account.

Recommendation 3

Review policies and ensure that reports sent to complainants and respondents are substantially identical.

Recommendation 4

Retain current level of factual detail in published reports.

Recommendation 5

Implement a permanent review process designed to measure compliance and publish the results in the Commissioner's annual report.

Recommendation 6

Increase funding. Additional funding for the Office would both increase its capability to enforce compliance with the legislation and signal to the regulated parties that government is committed to a vibrant private-sector privacy regime. For example, additional funding could be utilized to provide complainants with legal assistance in

launching court actions under section 14. The model for provision of legal services to human rights complainants in British Columbia may be a useful model for consideration.

Recommendation 7

Begin to utilize site visits by initiating contact with regulated parties and seeking consent to discuss and review existing privacy policies. Finalize and publish guidelines for use of the audit power and use such powers in appropriate circumstances.

Recommendation 8

That the Office of the Privacy Commissioner publish its formal policies online and, upon request, provide copies to the public in printed form. In addition, the Office should conduct regular reviews of its own compliance with internal policies and publish the results in the Commissioner's annual report.

Recommendation 9

An independent and comprehensive review of compliance with the legislation should be conducted.

B. Reforms Requiring Changes to PIPEDA

Recommendation 10

The legislation should not be amended to allow suits in the Federal Court prior to disposition of a complaint by the OPC.

Recommendation 11

The legislation should be amended to allow representative complaints before the OPC and to allow complainants (including, perhaps, third-party representatives) to file class actions suits in the Federal Court.

Recommendation 12

The Commissioner should be explicitly given the power to issue orders that are able to be filed with the Federal Court and made immediately enforceable.

Recommendation 13

The Commissioner should not be given the power to issue fines against respondents.

Recommendation 14

The legislation should be amended to allow the Commissioner to award compensation to complainants and, in egregious cases, to award punitive damages against respondents.

Recommendation 15

The option of creating industry-specific codes of practice, either by industry with OPC approval or by the OPC with industry consultation, is worthy of additional study as a potential future compliance tool.

I. Introduction, Objectives, Methodology and Outline

A. Introduction

In mid-2005, the British Columbia Civil Liberties Association[1] ("BCCLA" or the "Association") received a project grant from the Office of the Privacy Commissioner of Canada (the "OPC" or "Office") in connection with the Contributions Program of that Office to conduct research into the enforcement mechanisms contained in the *Personal Information Protection and Electronic Documents Act* ("PIPEDA" or the "Act")[2] and undertake a comparative analysis with other legislation designed to protect personal information. The general goal of the project was to provide analysis and evaluation of alternative models for enforcement including the current enforcement model. This report is the culmination of that project.[3]

The Association believes that this enforcement evaluation of PIPEDA will be an important and useful tool in making assessments about the efficacy of the current structure of and experience with the legislation as well as alternative mechanisms for protecting personal information. This report should also prove to be important for the preparation of submissions to be made as part of the Parliamentary review of the legislation required to begin in 2006.[4]

---

[1] The Association is Canada's preeminent defender of civil liberties. It has been an advocate for the protection of personal information for many years and has previously commented on privacy legislation at the federal and provincial levels.

[2] *Personal Information Protection and Electronic Documents Act*, (R.S. 2000, c. 5) (PIPEDA).

[3] This report is primarily a product of the research of Kirk Tousaw, the principal researcher, in consultation with BCCLA Executive Director Murray Mollard. The Association anticipates undertaking further research and deliberation on the issues raised in this report in 2006 in preparation for making submissions in connection with the 5-year review.

[4] PIPEDA section 29(1).

The BC Civil Liberties Association would like to thank all those individuals who provided their time and insights as part of our research regarding the enforcement of PIPEDA. It is only through the provision of this information that we have been able discern with greater accuracy how enforcement on the ground is actually carried out by the Office of the Privacy Commissioner of Canada and in other jurisdictions. Providing effective and constructive analysis and evaluation of the PIPEDA model and other model very much depends on a clear picture of what enforcement tools exist not only in legislation but also how they are applied in practice. Indeed, the only caveat that we have is that time and resources have not permitted us to meet with more regulators in other jurisdictions.

The BCCLA would also like to than the Office of the Privacy Commissioner of Canada for funding under their Contributions Program for making this project possible.

B. Specific Objectives

The Association had four specific goals in connection with the Project:

1. Evaluate the current PIPEDA enforcement regime by examining the enforcement provisions within the Act as well by identifying the current and past enforcement practices.

2. Identify enforcement models (in legislative provisions and actual practice) in other regimes (both domestic and foreign) and assess their efficacy.

3. Make recommendations with respect to (a) enhancement of the current enforcement model contained in PIPEDA; and, (b) options for change.

4. Communicate those recommendations to the Office of the Privacy Commissioner of Canada, key stakeholders and participants in the project.

C. Methodology

The research combined academic literature review with interviews. In addition, comparative analysis of various privacy regimes within and outside Canada was conducted, along with analysis of the practical effects of different choices in enforcement mechanisms.

The interviews consisted of discussions, by telephone and in person, with persons responsible for enforcement within both the Office of the Privacy Commissioner of Canada and other privacy regulators in Canada. Additional interviews with privacy advocates, privacy consultants and privacy officers of regulated parties served to flesh out a variety of perspectives on the Act and suggested reforms to the PIPEDA enforcement scheme.[5] A list of the persons interviewed appears in Appendix A. The opinions and recommendations contained in this report are those of the Association alone, not those of the interviewees.

The interviews with privacy regulators, regulated parties and advocacy groups provided context for the literature analysis. The research highlighted certain gaps between powers that are granted to regulators and those that are, in fact, used by those regulators. The Association also sought to determine which enforcement mechanisms are actually used, those that are not used, the reasons behind this (non)utilization and the efficacy of law and enforcement practice with a view to maximizing compliance.

Finally, the Association compared the enforcement schemes embodied in PIPEDA with other, non-privacy, administrative tribunals and agencies. The purpose of this comparison was to determine whether privacy enforcement in Canada takes place in

[5] The opinions and recommendations expressed in this paper, though shaped by the interviews, are those of the Association alone. Any errors or omissions, similarly, are those of the researcher and not of the interviewees.

a manner similar to enforcement of other legislation regulating private-sector entities and, if not, to gain an understanding of the reasons for the different methods and whether reform of the overall model is desirable.

The Association's criterion for evaluation of enforcement mechanisms was straightforward: to what extent does or will a particular enforcement tool engender compliance with the Act. It was not the Association's intent to determine whether, for instance, any particular enforcement procedure fit with the existing ombudsman model or would require a shift in emphasis. Instead, the Association began with the premise that the choice of the ombudsman model was made with the intent of fostering compliance with the law and, to the extent that the goal of compliance could be furthered by departing from that model, such a departure was warranted.

In addition, the decision to utilize the ombudsman model was almost certainly a product of the political climate in the pre-enactment era. In 2000, the concept of federal private sector privacy legislation was new and, in order to have legislation supported among the public and the regulated parties, it may have been necessary to propose a model that would have widespread support. In addition, the requirements of the Act were new and, in the early days, it was necessary to both educate the public and regulated parties and to allow the regulated parties a window within which to achieve compliance.

That is no longer the case; regulated parties should be familiar with the requirements of the Act and how to comply with it. Accordingly, the Association has taken the position in this report that the ombudsman model may, or may not, be the proper scheme by which widespread compliance is achieved. Throughout the report, the Association has attempted to be both descriptive and analytical, with the ultimate goal of

helping further the understanding of which model and what tools are best suited to achieving compliance with the Act.

C. Outline of Report

This Report begins with a general history of PIPEDA and its implementation. The overall structure of the legislation is examined and basic facts and figures are outlined. The ombuds-model is explained and critically examined. Certain preliminary conclusions are drawn, from which the remainder of the analysis follows.

Next, PIPEDA is compared to other Canadian privacy legislation. Specifically, the similarities and differences between the federal enforcement scheme and those of the provinces of British Columbia, Alberta and Quebec are examined. Those differences that appear pertinent to enforcement and compliance are highlighted and the practical effects of those differences examined.

Following the comparison to provincial privacy legislation is a review of PIPEDA in comparison to extra-Canadian privacy protection. The privacy schemes from Australia and New Zealand are explained and, again, critical differences are highlighted.

Next, the overall structure of PIPEDA is compared to other Canadian administrative schemes. Canada has a variety of federal-level administrative tribunals or decision-making bodies with varying responsibilities and enforcement mechanisms. The Report first provides a general overview and then focuses in on two archetypes, at different ends of the regulatory spectrum, for purposes of drawing direct comparisons to PIPEDA.

The Report concludes with a series of suggested reforms. This section is broken into two parts. The first section outlines those reforms that could be accomplished with no changes to the existing legislation and existing practices. Second, those reforms that would require amendments to PIPEDA or significant changes to the procedures of the Office of the Privacy Commissioner are explained. In both sections, a particular issue is identified, a discussion of the issue is conducted and the Association's recommendation explained.

II. The Personal Information Protection and Electronic Documents Act

A. History

The process leading up to PIPEDA coming into force on April 13, 2000 entailed "considerable debate" along with "more than a few anxious moments for privacy advocates."[6] A number of political, social and economic factors converged in Canada, creating the preconditions for Parliament to propose legislation that would bind the private sector.[7]

Christopher Berzins identifies "four key developments" that set the stage for the implementation of federal private-sector privacy legislation: (1) the recognition (both among the public and in government) that the private sector presented real and substantial threats to privacy; (2) the development of an international consensus on fair information principles; (3) the blurring of the lines between the public and private sectors; and, (4) that self-regulation would be unlikely to "meet the 'adequate level of protection' standard established by the European Community to regulate transborder data flows."[8]

The fourth factor was quite important in the ultimate determination that federal legislation be crafted. Put simply, Canadian business would have been prevented from any relationships that involved the transfer of personal data to or from the Member States of the European Community if it had not "ensure[d] an adequate level of protection" for that data.[9] Because of this, by the time PIPEDA began to coalesce, the Canadian private sector had already enacted a series of voluntary codes. Principal amongst these was the

---

[6] Berzins, Christopher "Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building" 27 Queen's L.J. 609 – 645 (2002).
[7] Public sector privacy protection already existed at the federal level in the form of the *Privacy Act* (R.S., 1985, c. P-21) enacted in 1985.
[8] Berzins, *supra*, at paragraphs 9 – 20.
[9] Directive 95/46/EC, Chapter IV, Article 25, Principle 1.

Canadian Standards Association Model Code for the Protection of Personal Information enacted in 1996.[10] This Model Code contained ten key privacy principles that would, ultimately, be imported whole-cloth into PIPEDA. Those principles are:

Principle 1 — Accountability
Principle 2 — Identifying Purposes
Principle 3 — Consent
Principle 4 — Limiting Collection
Principle 5 — Limiting Use, Disclosure, and Retention
Principle 6 — Accuracy
Principle 7 — Safeguards
Principle 8 — Openness
Principle 9 — Individual Access
Principle 10 — Challenging Compliance[11]

The wholesale importation of this voluntary code was not without controversy, despite that the Model Code was developed by "a consensus, which included business representatives, consumer advocates, privacy experts, and representatives from privacy commissioners' offices."[12] Again, Berzins is instructive: "For most privacy advocates, the PIPEDA was unquestionably a commercially-driven piece of legislation and, from their perspective, most of its weaknesses stem from this fact."[13]

B. Brief Overview of PIPEDA Enforcement Process

This section briefly outlines the process of enforcement under PIPEDA. Each of the various tools available to the Commissioner is explained in more detail later in this report.

Most PIPEDA compliance investigations begin with a complaint from an individual. The Commissioner may also initiate a complaint on her own, but this power

[10] The Canadian Standards Association (CSA) is "Canadian Standards Association is a **not-for-profit membership-based association** serving business, industry, government and consumers in Canada and the global marketplace" (bold in original). See the CSA website at www.csa.ca for more information.
[11] *See* PIPEDA Schedule 1 and the CSA Model Code (http://www.csa.ca/standards/privacy/code/Default.asp?language=English).
[12] Berzins at paragraph 26.
[13] Berzins at paragraph 33.

is rarely utilized. Following receipt of a complaint, an investigation is conducted. Investigators talk to both complainant and respondent, and are able to utilize a variety of powers during the course of the investigation. An attempt at mediation is made and, if unsuccessful, a report is prepared for the Commissioner at the end of the investigation. The Commissioner (or, currently, the Assistant Commissioner in the exercise of delegated powers) makes a finding and issues that finding to each party.

The Commissioner is unable to issue binding orders. Complainants are, however, entitled to seek recourse in the Federal Courts in order to have the Commissioner's findings enforced. Of course, any such action is subject to the respondent's right to present a defense and to appeal from adverse rulings.

In addition to investigating complaints, the Commissioner is entitled to conduct audits on regulated parties. "Reasonable grounds" must exist in order for the Commissioner to utilize the audit power. Finally, the Commissioner has an educative function, and attempts to inform both the public and the regulated parties about the requirements of the Act.

C. Implementation and Statistical Information

The implementation of PIPEDA began on January 1, 2001, when the legislation became applicable to all federally-regulated businesses in possession of personal information (except health information). The first stage also included those organizations that disclose information outside the boundaries of one province or country.

The second stage of implementation made PIPEDA applicable to covered personal health information held by organizations to which PIPEDA applied during the first stage. This second stage became applicable on January 1, 2002.

The third, and final, stage of PIPEDA implementation began on January 1, 2004, when the legislation became applicable to all commercial private entities throughout Canada in possession of personal information, except those covered by the substantially similar privacy legislation in British Columbia, Alberta and Quebec.

During the first two stages (when PIPEDA was only applicable to federally regulated entities), there were a total of 673 complaints filed under the legislation. Of these, 467 cases were finalized and the Office of the Privacy Commissioner of Canada, the agency tasked with oversight and enforcement of the law, found 155 of the complaints to be well-founded. 190 were found not well-founded and the remaining 122 were either settled, discontinued or found to be outside the Commissioner's jurisdiction.[14]

In the year after PIPEDA fully matured (January – December, 2004), the Commissioner received 723 complaints, more than double the amount received in 2003. This increase can likely be attributed to the expansion of PIPEDA's scope and, perhaps, increased public awareness of the possibility of utilizing PIPEDA to achieve redress of claimed access and privacy violations.

Final statistics for 2005 were not available when this report was finalized. The Office of the Privacy Commissioner advises that "significantly fewer" complaints were received in 2005 than in the prior year. The breakdown of dispositions was relatively constant, as was the ratio of complaints by industry sector.[15]

[14] Lawson, Philippa, "The PIPEDA Five Year Review: An Opportunity to be Grasped" prepared for the Canadian Internet Policy and Public Interest Clinic, Canadian Privacy Law Review. [CIPPIC Report]
[15] Email communication with staff of the Office dated March 3, 2006.

A total of 321 findings have been made public by the Commissioner since the Act came into force in 2001. Another 16 cases were "settled" and 1 finalized by way of "early resolution."[16]

D. Structure of the Act

1. Purpose

The Act contains an express statement of purpose:

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[17]

This statement of purpose has often been referred to as a "balancing" between the privacy interests of the individual and the business need to use personal information. This description, however, is not uncontroversial. The Commissioner, for example, has said that the term is "not an entirely apt one" because it fails to recognize that the ombuds-model also "enables the Privacy Commissioner to *assist* individuals and organizations in arriving at an appropriate balance so that the needs of all are met and respected through consensus."[18]

The balancing description is susceptible to another criticism – that it fails to fully recognize that the goal of legislation is *compliance* and not simply consensus. In other words, while the statement of the Act's purpose does envision the striking of a balance,

---

[16] The terms "settled" and "early resolution," are defined below (along with the other possible outcomes of complaints filed with the Commissioner) and have only been used since January, 2004.
[17] PIPEDA section 3.
[18] Stoddart, Jennifer "Cherry Picking Among Apples and Oranges: Refocusing Current Debate About the Merits of the Ombuds-Model Under PIPEDA" at page 5 (*publication forthcoming in the Canadian Journal of Business Law*) [Stoddart].

and while the use of the ombuds-model does allow for the Commissioner to provide assistance to individuals and organizations, that balance and that assistance must be understood to be means, not ends-in-themselves.

By incorporating prescriptive principles into the Act, Parliament must have intended to convey that the proper means to achieving the "balance" is for those organizations that are subject to regulation under the Act to *comply* with the principles set out in the Act. Indeed, an early pre-PIPEDA discussion paper put it this way, "The first issue anyone charged with overseeing the new legislation must address is: Are the people and organizations complying with the law?"[19] Any discussion of the Act's purpose, the choice of the ombuds-model, the enforcement tools provided for in the Act and reforms or alterations to these items has to take compliance – not consensus – as the launching point.

2. The Ombuds Model

Under PIPEDA, the OPC has an ombuds function. The Commissioner does not have order-making authority but, rather, functions as a sort of mediator and conciliator. The Commissioner must investigate complaints received from the public and may initiate her own complaints on reasonable grounds.[20] PIPEDA gives the Commissioner wide investigative powers (more fully detailed below) and authorizes her to seek to resolve complaints using dispute-resolution mechanisms.[21] Upon conclusion of the investigation, the Commissioner must deliver a report including her factual findings, recommendations, details of any settlement reached by the parties and what additional steps a complainant

[19] "The Protection of Personal Information: Building Canada's Information Economy and Society" Task Force on Electronic Commerce, Industry Canada and Justice Canada (January 1998) at page 18.
[20] PIPEDA section 11.
[21] PIPEDA section 12.

may take.[22] The Commissioner is also required to report on the activities of the Office of the Privacy Commissioner.[23] The Commissioner describes "these powers and functions" and the "hallmark characteristics of the ombudsman role."[24]

Despite having these hallmark characteristics, the Commissioner's powers and responsibilities under PIPEDA have been described as "quite unique in their application."[25] This uniqueness flows from the "novel" use of the ombuds-model to regulate a wide range and variety of private-sector activity as opposed to public administration.[26] As we will see in the comparisons with other privacy and non-privacy regimes below the Commissioner is correct to describe the PIPEDA structure as unique.

According to the Commissioner, this uniqueness has been the source of "misunderstanding" about the role of the Office of the Privacy Commissioner; a misunderstanding that is "rooted in a fundamental mismatch between the conceptual nature and characteristics of the ombudsman role and the regulatory-type controls governments are expected to wield over 'nefarious' private sector activity."[27] In the Commissioner's view, this misunderstanding has been the source of "much…confusion…in current debates about the use of the ombudsman model in overseeing PIPEDA."[28]

If, however, the ombuds-model is seen to preclude use of powers such as the ability to award damages to complainants or the ability to issue binding orders, it is unclear how that conception is reconciled with the private-sector privacy models

[22] PIPEDA section 13.
[23] PIPEDA section 25.
[24] Stoddart at page 4.
[25] *Id*.
[26] *Id*.
[27] *Id*.
[28] *Id*.

currently in place in British Columbia, Alberta and Quebec. As outlined in the discussion of these models, below, each incorporates to one extent or another, the hallmark characteristics attributed to the ombuds-model. Yet each provincial Act provides its respective Privacy Commissioner with enforcement powers greater than that enjoyed under PIPEDA. Surely, then, there is room within the ombuds-model for increasing the enforcement powers of the Privacy Commissioner.

According to the OPC, the ombuds approach appears to be working: "Some 40 per cent of the complaints closed during [2004] were settled, and another seven per cent resolved – an indication that suasion, a prominent feature of the ombudsman approach, is an effective tool."[29] The OPC's take on these numbers – and, indeed, the effectiveness of the overall ombuds-model – is not universally shared. Privacy watchdogs have generated significant criticism, noting that the three provinces with "substantially similar" private-sector legislation (Quebec, Alberta and British Columbia) all chose to go in a different direction.

[29] OPC Annual Report to Parliament 2004, page 3.

3. The Enforcement Toolbox[30]

In order to understand the scope of the enforcement practices under PIPEDA, it is worth noting the self-description by the OPC as an "*investigator* and *auditor* with full powers to investigate and initiate complaints, conduct audits and verify compliance under both Acts."[31] At a practical level, the OPC's enforcement role, to date, has primarily been as an investigator of citizen-initiated privacy complaints. The audit function has only been utilized once, in connection with the cross-border flow of information by the Canada Border Services Agency.

This disuse has led to criticism by privacy advocates of the effectiveness of the model in achieving compliance with the legislation: "Business compliance is best measured through a carefully planned series of spot audits that focus on business practices, not just stated policies."[32] According to the Commissioner, the audit powers are currently being enhanced. A full time director of the audit branch has been hired and the development of standards and building of resources is underway.[33]

The foregoing leads directly to a key caveat: it is beyond the scope of this project to determine whether the various enforcement models currently used by various privacy regulators have, or have not, been able to achieve substantial compliance with the laws. Instead, this report focuses on the enforcement practices and makes attempts to logically speculate into whether changing the practice would, or would not, lead to more substantial compliance by regulated parties.

---

[30] The concept of a privacy toolbox or toolkit is one that privacy expert Colin Bennett has raised in his writings on the topic.
[31] 2004 Annual Report, page 7 (emphasis in original).
[32] CIPPIC Report, page 4.
[33] "Annual Report to Parliament 2004" Office of the Privacy Commissioner of Canada 2005 at pages 75 – 76.

The enforcement toolbox, however, does not consist solely of investigative and audit powers. The Commissioner also has an education mandate that, properly understood, forms a part of the enforcement model. Education takes place in a variety of formats. For example, the Commissioner can use the filing of a complaint and the subsequent investigation as an educational and transformative exercise; providing information directly to complainants and regulated parties on the correct understanding of privacy rights and responsibilities under PIPEDA.

Education can also occur outside of the complaint process. The Commissioner engages in outreach to members of the public and to regulated parties through direct communications, public appearances, the preparation of annual reports and the posting of educational material and guidelines on the OPC website. Increased education, presumably, will have the direct effect of broadening compliance with the Act and the indirect benefit of reducing the number of complaints that tax an already-overburdened Office. This advisory mandate is an important piece of the overall enforcement and compliance puzzle and should not be overlooked. Indeed, there has been some suggestion that the Commissioner would, either practically or effectively, lose this mandate if it was granted significant enforcement powers.

The section that follows outlines the complaint process in detail, from inception by a member of the public through final determination by the Commissioner and litigation in the Federal Court. Following the complaint discussion is a brief analysis of the audit power. Finally, this section of the report concludes with a brief discussion of existing attempts to measure compliance with the Act.

4. The Complaint Process

Procedurally, a complaint is filed by an individual[34] and the entity against whom the complaint is lodged is provided an opportunity to respond. There is no required format for complaints and, often, complaints are simply letters or emails received by the Inquiries Branch of the Office. Upon receipt of a complaint, the Commissioner must initiate an investigation though "investigation" is not a defined term and the scope of each investigation varies on a case-by-case basis.

a. Investigations

After receiving a complaint, the file is assigned to an investigator. The investigator's first step is typically to contact the complainant in order to clarify the role of the Office and to obtain additional factual information. At this point, the investigator has the first opportunity to attempt to clear the file by referring the complainant back to the regulated party to attempt a resolution without further interference from the Office. The success of this initial attempt is largely dependent on the party involved and the nature of the complaint. For example, employee/employer situations are very rarely able to be referred back while customer/entity situations are more likely to be resolved in this manner.

Assuming that the complainant wants to proceed, the investigator will prepare an investigation plan. This plan includes a written synopsis of the allegations, evidence and sections of the Act at issue. In addition, the investigator will set out a list of questions, witnesses and documents that might be necessary. The plan contains a description of the

[34] As noted above, the Commissioner is also empowered to initiate complaints on "reasonable grounds" though the exact parameters of this power are unclear. PIPEDA contains no guidelines on what constitutes "reasonable grounds." For all practical purposes, complaints are initiated almost exclusively by members of the public.

evidence that would be required to prove the alleged violation in order to allow the investigator to determine whether a case can be made.

The next step in the investigative process is to contact the respondent. The investigator explains the nature of the complaint and obtains the respondent's initial position. Respondents are questioned about the factual circumstances and, according to the Office, are typically quite cooperative. The investigator (by delegation from the Commissioner) has the power to, but is not required to, summon witnesses, obtain documents and enter premises to investigate a complaint.[35]

According to the Office, however, these powers are rarely utilized because most respondents are cooperative with the investigators.[36] This cooperation is attributed to several factors. First, the investigation staff has good credibility with the regulated parties. Next, the organizations place a value on positive non-adversarial relationships with the Office. Also factoring in is a perceived reluctance on the part of regulated entities to expend the resources necessary to take an adversarial posture. The Office attributes the existence of many of these factors to the conciliatory role existing in the ombuds-model.[37]

The interaction with the responding parties also provides an educational opportunity. Investigators are able to explain the Office's role as an independent party (as opposed to an advocate of the complainant) and to provide guidance to the respondent on the particular factual and policy issues presented by a complaint. Investigators explain

[35] PIPEDA section 12.
[36] *See*, for example, the 2004 Annual Report's description of pending federal litigation, filed in 2003, involving the Commissioner's first use of her power to order production of records pursuant to section 12(1)(a) and (c) of PIPEDA. Annual Report 2004 at page 87.
[37] In interviews with OPC staff, no suggestions for additional investigative powers were made and the Association believes that the existing investigative powers are sufficient.

what the respondent can or must do in order to meet the requirements of the Act and, in return, are themselves educated on the particular business being investigated.[38]

After concluding inquiries, an investigation report is drafted. This is an internal document generated by the investigator in accordance with formalized procedures within the Office. The report includes a summary of the complaint, a statement of facts and an analysis of the application of PIPEDA to those facts. The investigator makes a recommendation as to whether the complaint is well-founded or not. Also included are conclusions with citations to the particular privacy principles at issue. The report contains a recommendation to the Commissioner with respect to the findings and the possible remedial recommendations to be made to the respondent. Finally, the report will include any communications with the parties and any comments the parties may have made on the matters at issue.[39]

b. Commissioner's Findings

The Commissioner then issues findings.[40] These findings are communicated to the parties, who receive substantially identical letters.[41] In addition to the letters sent to the parties, anonymous summaries of the Commissioner's findings are made public. Both the publication of summaries and the anonymity have engendered criticism from privacy advocates. The summary findings have been criticized as having limited utility. The practice of not (or very rarely) publicizing respondent's names has been criticized by

[38] This self-education by the investigators allows for some efficiency gains. In the intake process, an attempt is made to direct complaints to investigators with pre-existing experience in a particular field of business or a particular type of complaint (access requests or video surveillance, for example).
[39] The Association requested a template of the investigation report but, to date, the Office of the Information and Privacy Commissioner had not provided one.
[40] The current practice of the Office is that the Assistant Commissioner actually issues the findings.
[41] The nearly-identical nature of the reports issued to the complainant and respondent has been questioned. Some privacy advocates have alleged that the versions sent to the complainant and respondent can differ significantly, however, the Office maintains that the only differences are in format, not in substance.

those who point out that publication of the names of businesses that violate privacy laws has a twofold function; providing businesses with incentives to comply and allowing consumers to know which entities have been the subject of privacy complaints. These criticisms, and the responses to them, are discussed in more detail below.

c. Outcomes

The Commissioner's findings are categorized into six categories:

Settled during the course of the investigation

This disposition is used when the Office has helped negotiate a solution during the course of the investigation that satisfies all involved parties. The Assistant Privacy Commissioner does not issue a finding.

Early resolution

This new disposition is applied to situations where the issue is dealt with before a formal investigation is undertaken.

Not well-founded

There is no evidence to lead the Commissioner to conclude that the complainant's rights under the Act have been contravened.

Well-founded

The organization failed to respect a provision of the Act.

Resolved

The allegations raised in the complaint were substantiated by the investigation, but the organization agreed to take corrective measures to rectify the problem, to the satisfaction of this Office.

Discontinued

> Investigation is terminated before all the allegations have been fully investigated, for example when the complainant is no longer interested in pursuing the matter, or can no longer be located to provide additional information that is critical to reaching a conclusion.

Two of these categories ("settled during the course of investigation" and "early resolution") were added in 2004.[42]

At this point, in virtually all cases, the role of the Office is over. The Commissioner does not have any power under PIPEDA to enforce the findings and directives to the respondents. The only way to enforce the Commissioner's findings is for the complainant to go to court.

5. Litigation

An individual, or the Commissioner, may bring an action in Federal Court to enforce the results of the Commissioner's investigation, compel the organization to abide by the Commissioner's recommendations, impose a monetary fine or award damages (including, in certain circumstances, compensation for non-economic injuries such as humiliation[43]) to the complainant.[44] The Commissioner can either appear for herself or may appear "on behalf" of a complainant.[45]

The individual may only go to court after receiving the Commissioner's report and has a 45-day window to file.[46] Recourse to the Federal Court has not been widely utilized. The potential disuse of the ability to go to Court was an early criticism of the

[42] Annual Report 2004 at page 40.
[43] PIPEDA section 16.
[44] PIPEDA section 14 – 17.
[45] PIPEDA section 15. It does not appear that the Commissioner has yet utilized this power and it is unclear whether the OPC has an official policy for determining under what circumstances it would initiate litigation or appear on behalf of a complainant under section 15.
[46] PIPEDA section 14.

PIPEDA scheme and some commentators believe that the evidence bears out the validity of such critiques:

> …very few complaints have made it to the Federal Court, and those that have been filed have moved very slowly, the result being that there is very little sense of how the courts will shape the legislation. Not only does this create tremendous uncertainty, but it suggests that delay may become a fundamental aspect of the compliance environment, to the obvious detriment of complainants.[47]

a. Caselaw

The following Federal Court decisions have dealt with enforcement of PIPEDA findings:[48]

Diane L'Écuyer v. Aéroports de Montréal and Privacy Commissioner of Canada, 2004 FCA 237

This is an appeal from the dismissal of claim by the Federal Court. A letter regarding the appellant had been disclosed by his employer, the respondent, to union representatives. The trial judge had determined that the he did not have jurisdiction to hear the appellant's claim under the PIPEDA, as jurisdiction was vested solely with the grievance arbitrator. In addition, the judge held that the employer had been under a legal obligation to disclose the letter and dismissed the appellant's claim.

The appeal was dismissed with a determination of no palpable and overriding error in the findings. That was sufficient to dismiss the appeal without requiring a decision on the issue of jurisdiction (the primary ground of the trial court's decision was that neither the Court not the Privacy Commissioner had jurisdiction over the claim).

---

[47] Berzins, Christopher "Three Years Under PIPEDA: A Disappointing Beginning." Canadian Journal of Law and Technology at page 113.

[48] Other cases have touched on PIPEDA but not directly dealt with enforcement. So, for example, in *Ferenczy v. MCI Medical Clinics*, [2004] O.J. No. 1775, a civil claim, the plaintiff sought to bar the defendant from using videotape evidence gathered surreptitiously. The evidence was allowed with the court concluding that such gathering was not "commercial activity" and, thus, not within PIPEDA's ambit.

Mathew Englander v. Telus Communications Inc. and Privacy Commissioner of Canada, 2004 FCA 387

In this case, the Court of Appeal held that the federal Privacy Commissioner, and the lower court, erred in finding that Englander had no valid complaints against Telus. Englander complained that the consent allegedly obtained by Telus from its first-time customers for disclosure of personal information did not meet the standard set up in the Act. He also complained about Telus charging him a monthly fee for non-published number service which was a condition for not publishing personal information in its telephone directory.

In addition to listing its customers in the phone book and on internet directories, Telus disclosed, for a fee, the listing information of its customers through services called Directory File Service and Basic Listing Interchange Service. The information of customers who subscribed to the non-published number service was not disclosed. Englander argued that Telus failed to comply with PIPEDA because it did not inform customers that their personal information would be distributed for a fee. He also argued that Telus should have advised first-time customers that they could opt out of this disclosure and that the fee charged for this disclosure could not be permitted because customers were merely exercising their statutory right to privacy.

The appeal was allowed in part. Telus was found to have infringed the Act by not advising its first-time customers – at the time of enrollment – of the primary and secondary purposes for which their personal information was collected and by not informing customers of the availability of the non-published number service. In addition, proper consent could not have been given by first-time Telus customers with respect to use of their information in the Directory File Service and Basic Listing Interchange

Service. The services were not identified at the time of enrollment and there was no evidence that they were so connected with the primary purposes of telephone directories that a new customer would have reasonably considered them appropriate.

No effort was made to ensure that first-time customers were advised of the secondary purposes of the collection of personal information. Consent was not informed because the customer was not aware that they had the opportunity to opt out of the distribution of personal information. In terms of fee, however, the Court found that the fee charged for non-disclosure of personal information facilitated the constitutional right to privacy. Because the CRTC had approved the rate and there was no evidence that the rate was unbearable, Telus was found to be allowed to charge it.

Erwin Eastmond v. Canadian Pacific Railway and Privacy Commissioner of Canada, 2004 FC 852

This was an application by Eastmond for an order that Canadian Pacific Railway ("CP") comply with the Privacy Commissioner's report. In December 2001, CP installed six digital video recording surveillance cameras for security purposes in the mechanical facility area of its Toronto Yard. There was no CP official looking at the monitor at the time the cameras captured a person's image. Rather, that person's image was recorded on videotape. The recording was never viewed unless there was a triggering event. The recording was destroyed after 96 hours with the result that the person's image was never seen if there was no event.

In January 2002, Eastmond, a CP shopcraft employee in the diesel shop, filed a complaint with the Office of the Privacy Commissioner alleging that the cameras were violating employees' rights to privacy. In January 2003, the Privacy Commissioner issued

a report determining that the complaint was well founded. It was recommended that CP Rail remove the cameras because they were being used for inappropriate purposes.

Eastmond's application was dismissed. The Court concluded that a reasonable person would consider CP's reason for recording the images of CP employees and others on video camera appropriate in the circumstances. The collection of personal information was not surreptitious (because warning signs were displayed) and only brief, capturing only a person's image when that person was within the footprint of the camera. The collection was not limited to CP employees, as it captured the images of contractors, visitors, suppliers and trespassers and was not to measure a CP employee's work performance. Indeed, the Court found that CP could not use those images to measure an employee's productivity because such a use would be for a purpose other than that which prompted its collection (security). Accordingly, it was determined that CP established a legitimate need to have the cameras installed and to record those persons who would pass its fixed footprints.

Janice Morgan v. Alta Flights (Charters) Inc., 2005 FC 421

This case involved review of the Privacy Commissioner's decision that no breach of the Act occurred. Factually, Morgan was employed as a customer service representative by the respondent airline. The airline attempted to surreptitiously record conversations of some employees, including those of the applicant, by placing a tape recorder underneath a table in employee smoking room. The recorder was discovered by employees before any conversations could be recorded. Alta Flights admitted to having hidden the recorder with the intention of recording employee conversations in order to investigate allegations of wrongdoing by employees, including Morgan.

Morgan went to the Privacy Commissioner for a determination of whether this violated PIPEDA. The Commissioner ruled that there was no violation because no conversation was ever in fact recorded. The Court agreed; because the airline did not actually record any conversations, there was no violation of Act. Attempted breach does not exist under PIPEDA.

Turner v Telus Communications Inc., 2005 FC 1601

Telus was implementing "e.Speak" a voice-recognition technology that allowed its employees to access Telus' internal computer network through voice commands over the telephone. Four employees challenged this program as being an unlawful collection of biometric information (used to authenticate identity) without consent (and that the collective agreement did not constitute that consent). The Privacy Commissioner rejected the complaint, ruling that Telus complied with the Act.

In Court, the employees were joined by the Telecommunications Workers Union in challenging Telus' program. The union's application was dismissed because it had not made a complaint to the Commissioner. The employees' application was rejected on the basis that an organization may collect information without consent if collection is in the individual's best interest and consent could not be timely obtained.

6. Audits

The most glaring gap between the powers granted to the Commissioner and those actually utilized comes in the area of audits. The audit power has only been invoked on one occasion in almost five years of varying degrees of PIPEDA implementation. The Office has an Audit and Review Branch, tasked with three general categories of work. First, the branch engages in compliance reviews or, in other words, audits. The branch

also reviews privacy impact assessments generated by federal departments and agencies. Finally, the branch engages in a "mixed bag" of work such as responding to inquiries, needs or issues that do not fit cleanly into the other categories.

Though not yet an effective tool, the audit power has the potential to be a powerful tool for measuring and enforcing compliance with the Act. Indeed, the audit power was regarded, in the pre-PIPEDA discussions, as important to compensate for a significant weakness that may be inherent in a complaint-driven model:

> In many countries with data-protection laws, compliance is assumed unless a dispute or investigation reveals a problem. A possible weakness of this approach is that it relies heavily on the public to discover abuses, which can be quite difficult in the current climate of sophisticated dataprocessing techniques.
>
> To compensate for this potential weakness, the law could deal with compliance monitoring by empowering a central authority or privacy commissioner to do research, prepare reports on new issues such as new technologies, and perform audits or inspections proactively in addition to responding to complaints. In order for this to be as effective as an upfront registration or audit scheme, there would have to be significant resources committed to this function.[49]

It is anticipated that the Audit Branch will engage in the review of organizational privacy practices by broadly examining systems that govern how the organization collects, uses and disposes of personal information. In addition, the efficacy of the audit power could be enhanced at relatively small cost relative to the potential upside by the introduction of "site visits." These site visits would not be full scale audits but, rather, would be more akin to a quick check-up of an organization's privacy practices.[50] The

[49] "The Protection of Personal Information: Building Canada's Information Economy and Society" Task Force on Electronic Commerce, Industry Canada and Justice Canada (January 1998) at page 19.
[50] Site visits are a tool that has been utilized effectively in British Columbia and, indeed, former BC Privacy Commissioner David Flaherty was a pioneer in utilizing site visits as a compliance tool.

auditor would ask basic questions such as whether the organization has a privacy policy, how it handles information and breaches and the like.

Putting aside the question of resources, the principal obstacle to utilizing the audit power appears to be the Act's requirement that the Commissioner have "reasonable grounds to believe that the organization is" violating the Act before conducting a compliance review – whether that be a full-scale audit or the lesser site visit described above.[51] Of course, the Commissioner is free to request consent from the regulated parties to conduct either a site visit or a full-scale audit. If consent is granted, no reasonable grounds are required.

The term "reasonable grounds" is not defined in the Act and it is unclear when an audit is justified. Is a filed complaint sufficient, for example? Or what of the case where an organization has been found to have breached the Act but the evidence is unclear whether that breach was an isolated instance? The Commissioner has recognized this issue and has stated an intent to "initiate a project to determine and test a process for establishing 'reasonable grounds' to select subjects for audits."[52] Results of this project were not available at the time this report was completed.

8. Compliance Studies

Studies into business compliance with PIPEDA are few and far between. According to one privacy watchdog, a review of the literature reveals the existence of only three studies, and it has proven impossible, to date, to obtain the results of one while the other two have been described as "very limited."[53] Nevertheless, the results of these

[51] PIPEDA section 18.
[52] Annual Report 2004 at page 76.
[53] CIPPIC Report, page 4.

studies have been characterized as indicating "serious compliance problems" with the legislation.[54]

Perhaps recognizing that criticisms about the enforcement of the Act continue to be leveled, the OPC implemented new procedures in 2004: "We have introduced a formal procedure of systematic follow-ups to complaint investigations under PIPEDA. We will now be in position to monitor the progress of organizations in implementing commitments they make during complaint investigations and in response to the recommendations our Office issues to them. Equally important, our Audit and Review Branch is strengthening its capacity to audit organizations subject to PIPEDA."[55]

Further research into business compliance with PIPEDA is crucial and should be an important part of the Office's work in the future. Australia recently conducted a significant review of compliance with its private-sector privacy legislation (described below) that could serve as a model for this type of review.

[54] Id.
[55] 2004 Annual Report, page 3.

III. Legislative Comparisons: Canada

This section describes the privacy-protection regimes in five jurisdictions. Three of these are within Canada: Alberta, British Columbia and Quebec. The remaining two are outside of Canada: Australia and New Zealand.[56] A brief outline of the pertinent legislation is provided for each jurisdiction. The overall model is examined, the enforcement powers are described and comparisons to PIPEDA are drawn.

In the extra-Canadian jurisdictions, particular attention is paid to Australia. This is for two reasons. First, the Australian private-sector privacy legislation is similar to PIPEDA in many ways but certain outcomes are quite different. Second, Australia recently completed a significant review of its legislation, including detailed analysis of the model, enforcement provisions and compliance outcomes. Lessons learned from this review may prove instructive.

A. Canadian Privacy Legislation

1. Alberta

Private sector privacy in Alberta is governed by the Personal Information Protection Act (PIPA), which came into force as of January, 2004.[57] PIPA has been deemed to be "substantially similar" to PIPEDA and, thus, organizations governed by PIPA are exempted from the provisions of PIPEDA. PIPA's purpose is substantially identical to that of PIPEDA:

> The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and

[56] These countries were chosen because, among other things, each are English-speaking countries with private-sector privacy legislation that are comparable, but not identical, to PIPEDA.
[57] *Personal Information Protection Act*, Chapter P-6.5.

> the need of organizations to collect, use or disclose personal information for purposes that are reasonable.[58]

PIPA is overseen by the Office of the Information and Privacy Commissioner of Alberta (the "Alberta Office" or "Alberta Commissioner").

As with PIPEDA, the enforcement process is largely complaint-driven. Individuals are entitled to complain to the Alberta Commissioner if an organization is not complying with the Act. Individuals may also request that the Alberta Commissioner review a decision of an organization taken in response to the individual's request to that organization with respect to personal information.[59] The Alberta Commissioner is also given the ability to initiate an investigation.[60] Finally, the Alberta Commissioner has investigatory powers similar to those granted in PIPEDA.[61]

In addition, the Alberta Commissioner may:

- refer individuals to another grievance, complaint or review process;[62]
- give an advance ruling on a matter that could be investigated under the Act;[63]
- authorize mediation or investigation to settle a complaint;[64]
- hold an inquiry;[65]
- issue Orders that are binding;[66]
- allow an organization to take more time to respond to an individual's request for personal information;[67] and,
- authorize an organization not to respond to requests in certain situations.[68]

[58] PIPA section 3.
[59] PIPA section 46.
[60] PIPA section 36(1) and (2).
[61] PIPA sections 38.
[62] PIPA section 46(3).
[63] PIPA section 36(3).
[64] PIPA section 49.
[65] PIPA section 50.
[66] PIPA section 53.
[67] PIPA section 31.
[68] PIPA section 37.

When a complaint or request for review comes into the OIPC, the first step taken is to refer the complainant back to the organization to attempt to work out the problem without intervention by the Alberta Commissioner. Failing that, complainants are entitled to file written complaint. When this happens "a Portfolio Officer is assigned to handle the case and is the single point of contact unless and until the case proceeds to inquiry."[69]

The first step upon opening the file is to contact both the complainant and respondent to inform them of the complaint, the Alberta Office's role and the ways by which the matter can be resolved.[70] The overall goal of the process is to "resolve disputes through informal fact-finding, mediation and education processes."[71] The stated goal of the mediation process is to balance "personal information rights with the need of the organization to carry out its business in a reasonable manner."[72] The Alberta Office emphasizes that it takes a non-legal approach to mediation and that it views its purpose as involving both problem solving and education.[73]

If a mediation is successful, the Portfolio Officer "obtains verbal agreement about the resolution and writes to both [the individual] and the organization outlining the agreement, and giving both parties the opportunity to refute matters of fact within a specified timeframe."[74] Upon agreement the file is closed and an Investigation Report, which is not legally binding, may be published on the Alberta Office's website. This

---

[69] "A PIPA Guide for Individuals: Understanding the Role of the OIPC" Office of the Information and Privacy Commissioner of Alberta (September 2004) at page 4 (available at http://www.oipc.ab.ca/ims/client/upload/PIPA_Guide_for_Individuals_Oct04.pdf) [AB PIPA Guide].
[70] Interview with Alberta Office. Note that these ways include mediation, publication of a report and the conducting of a formal inquiry resulting in the issuance of a binding order.
[71] AB PIPA Guide at page 5. *See also*¸ PIPA section 49.
[72] *Id*.
[73] Interview with Alberta Office.
[74] AB PIPA Guide at page 5.

report, arrived at by agreement of the parties, may name the organization. Since PIPA came into force, a total of 14 Investigation Reports have been published.[75] All named the respondent organization(s), and the Alberta Office believes that the ability and willingness to name names, in appropriate circumstances, is a powerful tool for achieving compliance.[76]

At least one of the published Investigation Reports contained a finding that the respondent business was not at fault and had complied with the legislation. This is in line with the Alberta Office's view of the Investigation Reports as educational tools that are primarily designed to provide guidance, not to penalize. So, too, are the criteria applied when deciding whether to publish an Investigation Report; the Alberta Office primarily seeks to publish Reports that involve widespread industry problems.[77]

If either the mediation is unsuccessful or the matter is not otherwise resolved, the Alberta Commissioner is entitled to begin a formal inquiry in which the Alberta Commissioner may decide all questions of law or fact.[78] If the inquiry relates to an organization's (a) refusal to provide access to the complainant's personal information, or (b) refusal to provide information related to the collection, use or disclosure of the complainant's personal information, then the burden of proof at the inquiry is on the organization.[79]

Because of the serious nature of a formal inquiry and the resources that must be expended, the Alberta Office prefers that as few matters as possible go to formal inquiry;

---

[75] *See* http://www.oipc.ab.ca/orders/investigation.cfm. The Alberta Office would like to publish more frequently but the process is resource-intensive. Interview with Alberta Office.
[76] *Id*.
[77] Interview with Alberta Office.
[78] PIPA section 50.
[79] PIPA section 51.

though the ability to go to formal inquiry and issue a binding order is considered an important tool.[80] A formal inquiry must be resolved by the making of an order. The orders may direct organizations to take action including (a) providing the complainant with access to personal information; (b) comply with PIPA; and, (c) destroy personal information.[81] Orders may be "filed with a clerk of the Court of Queen's Bench" and, if so, the "order is enforceable as a judgment or order of that Court."[82] Orders are deemed to be final[83] and organizations "must comply" with the order within 50 days, but any party is entitled to seek judicial review.[84] As of the date of this report, no formal orders under PIPA have been issued.[85] The Alberta Office anticipates releasing at least two orders in the near future, with several more in the pipeline.[86]

Certain violations of PIPA, including a refusal to comply with an order of the Commissioner, are deemed to be offences and subject the offender to maximum fines of $10,000 (in the case of an individual) or $100,000 (in the case of an organization).[87] The Alberta Office has commenced two prosecutions under this provision of the legislation, marking the first time that privacy-offences have been prosecuted despite that the power to do so has been available for ten years in the public sector and for five years under the *Health Information Act*.[88]

Finally, when the Alberta Commissioner has issued an order against and organization (or if the organization has been found to have committed an offence under

---

[80] Interview with Alberta Office.
[81] PIPA section 52.
[82] PIPA section 52(6).
[83] PIPA section 53.
[84] PIPA section 54.
[85] *See* http://www.oipc.ab.ca/orders/orders.cfm.
[86] Interview with Alberta Office.
[87] PIPA section 59.
[88] Interview with Alberta Office. *Health Information Act*¸ R.S.A. 2000, c. H-5.

the Act), and that order or offence is no longer subject to appeal, the aggrieved party has a right of action against the organization "for damages for loss or injury that the individual has suffered as a result of" the breach or conduct.[89] The Alberta Commissioner is not a party to civil suits for damages.[90]

The Alberta PIPA does not expressly give the Alberta Commissioner the power to audit an organization's privacy practices. Indeed, the word "audit" does not appear in AB PIPA at all. Unless an "audit" is deemed to be a type of "investigation" or "inquiry" it does not appear that the Alberta OIPC is entitled to conduct audits, though the Alberta Commissioner takes the position that its investigative powers are broad enough to encompass the gathering of information in a manner substantially identical to an audit. The Alberta Office has also, in one case, taken the novel approach of requiring the respondent organization to conduct an internal audit and to report back the results to the Alberta Office for its review and comment.[91]

The Alberta Office believes that its enforcement powers are effective. Its experience is that the majority of complaints handled by the Alberta Office after the referral-back process have merit. The combination of a mediation-first philosophy and fairly significant enforcement powers (particularly the willingness to name and the ability to issue binding orders) create a climate that fosters business compliance; most organizations that are contacted by the Alberta Office want to comply with the law and to be given the tools and guidance to do so. That said, the Alberta Office also recognizes

[89] PIPA section 60.
[90] PIPA "Guide for Individuals" at page 6.
[91] Interview with Alberta Office.

that business knowledge about privacy obligations is not yet sufficient, particularly in small-to-medium sized organizations.[92]

Statistically, the Alberta OIPC received 128 complaints and 54 requests for review in fiscal year 2004 – 2005 for a total of 188 cases. Of these, 182 were initiated by the public and 6 by the Commissioner.[93] In the same time period, 35 requests for review and 69 complaints were closed.[94] Most of these were cases opened that year as the AB PIPA came into effect in 2004 and only 4 requests for review and 6 complaints were received in the period preceding the 2004/5 fiscal year (of these, 1 complaint was resolved). Every resolved case (107 total) was resolved by "mediation/investigation" and no orders were issued by the Commissioner.[95]

2. British Columbia

Private sector privacy in British Columbia is governed by that province's *Personal Information Protection Act*.[96] As in Alberta, the Act came into force in January, 2004 and has been deemed "substantially similar" to PIPEDA. The BC PIPA is administered by the British Columbia Office of the Information and Privacy Commissioner (the "BC Office" or "BC Commissioner"). The legislative purpose is also essentially identical to that of Alberta and PIPEDA:

> The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes

[92] Interview with Alberta Office (entire paragraph).
[93] The AB OIPC fiscal year runs from April 1 through March 31 of the following year. Alberta Office of the Information and Privacy Commissioner Annual Report 2004/2005 at page 12, 15.
[94] *Id* at page 12.
[95] Alberta does not specify resolution types beyond "order" or "mediation/investigation." Alberta 2004/5 Annual Report at pages 13 – 16.
[96] Personal Information Protection Act, [SBC 2003] Chapter 63.

> that a reasonable person would consider appropriate in the circumstances.[97]

All told, the British Columbia and Alberta legislation are so similar that it would be redundant to review the provisions of the BC PIPA in detail in this report. Instead, this section highlights differences between the British Columbia and Alberta legislation and provides additional information about the practices and perspective of the BC Office.

There are three principal differences between the two provincial Acts (at least with respect to the enforcement powers). First, the BC Commissioner is expressly granted audit powers.[98] Second, there is no provision in the BC PIPA for the filing of the BC Commissioner's orders in the provincial courts and, correspondingly, the immediate enforcement of those orders as orders of the Court. The BC Office considers this a detriment and believes that having such power would give the office additional enforcement leverage.[99] Finally, the language with respect to a complainant's ability to seek damages differs slightly: the Alberta Act allows civil suit for "loss or injury" while the British Columbia Act permits recovery only of "actual damages."[100]

Another difference between Alberta and British Columbia is practical, as opposed to legislative. To date, the BC OIPC has not published any Investigation Reports[101] but has, however, issued a total of 3 published orders[102] and 8 anonymous mediation summaries.[103] This lack of published Investigation Reports and small number of formal

---

[97] BC PIPA section 2.
[98] BC PIPA section 36(1)(a). A recurring theme, however, is that the existence of the power does not, because of resource issues, equate with the ability to exercise that power.
[99] Interview with BC Office.
[100] *Compare*, AB PIPA section 60 and BC PIPA section 57.
[101] *See* http://www.oipcbc.org/sector_private/orders_decisions/investigation_reports.htm.
[102] *See* http://www.oipcbc.org/sector_private/orders_decisions/orders.htm.
[103] *See* http://www.oipcbc.org/sector_private/orders_decisions/Mediation_Sum.htm.

orders is an acknowledged downside to the mediation-centered philosophy because little guidance is provided to the regulated parties.[104]

In purely statistical terms, the OIPC "received a total of 1,266 requests for review and complaints and closed 1,077, leaving a backlog of 189" in 2004 – 2005 (the annual report year ends March 31). These numbers include complaints under both the private sector legislation (BC PIPA) and the public sector privacy law.[105] According to the Commissioner, the number of complaints grew steadily as the year progressed, and the "numbers of complaints would have been higher were it not for our policy of referring would-be complainants back to the responsible organizations to attempt a private resolution of the matter before complaining formally to us."[106]

In terms of pure private-sector cases, the OIPC "received 53 reviews and 156 complaints under PIPA and closed 52 reviews and 118 complaints."[107] Three categories of complaints predominated; collection, disclosure and violation of a duty required by act.[108] The principal means of resolution was a referral back to the organization (36), followed by partially substantiated (24) and mediated (24). The final two categories to achieve double-digits were those complaints that either had no reviewable issue (15) or were not substantiated (12). Put another way, 30% of cases were referred back, 20% partially substantiated and 20% mediated.

These statistics seem to indicate that most of complaints dealt with by the OIPC had some merit (leaving aside those referred back to the organization, as it is impossible

[104] Interview with BC Office.
[105] Office of the Information & Privacy Commissioner of British Columbia Annual Report 2004 – 2005 at page 7.
[106] *Id* at page 9.
[107] *Id* at page 56.
[108] *Id*.

to determine whether these were legitimate) or at least enough merit that the organization was willing to enter into a mediated resolution. When the referral-back cases are eliminated from the statistics, the numbers show that 30% of the complaints handled by the OIPC were mediated and 30% partially substantiated.[109]

In terms of requests for review, 34 of 52 cases were "deemed refusals" (organizations that had failed to respond to a request for information within the 30-day statutory deadline), the remainder divided among partial access (10) and denials of access (8). Most reviews were mediated (34) or referred back (7) with the remainder divided among the remaining categories.

The BC Office believes that most complaints have some merit. As well, like Alberta, the BC Office uses intake as a screening mechanism and attempts to have complainants first go back to the organization and attempt to resolve the matter (armed with information and forms to assist in that process). The refer-back policy uses existing criteria; not all cases are referred back. The BC Office is currently reviewing its intake policy to determine what happens to complainants who have been referred-back.[110]

Because of the large volume of complaints and the scarcity of resources, the BC Office has an emphasis on efficiency. Staff are given wide discretion and encouraged to seek creative resolutions to disputes. Internal benchmarks and mandatory peer review of substantive communications are used to provide internal checks on this latitude.[111]

---

[109] For comparison purposes, the BC OIPC closed 96 public-sector privacy complaints in the same fiscal year. Of these, half (48) were referred back to the public body. Removing these from the equation reveals that 35% of the remainder were not substantiated (17 of 48) and 20% mediated (10 of 48) while only 18% were found to be either substantiated (7 of 48) or partially substantiated (2 of 48). *Id* at page 47. Prior to the 2004/5 annual report, the BC OIPC did not track mediation as a form of resolution.
[110] Interview with BC Office (entire paragraph).
[111] Interview with BC Office.

In terms of enforcement, the BC Office – like the Alberta Office – feels that the ability to name names is an important tool.[112] This tool provides incentive to business to pay attention to privacy obligations and, when confronted with a complaint, to work toward a mediated solution. In addition to the practical incentives, the legislative grant of power signals to the regulated parties that government believes in the legislative goals; this increases the moral suasion inherent in the legislation. That said, the BC Office also recognizes that naming names may not be appropriate in all circumstances. [113]

One tool that the BC Office suggests would be useful is the ability to be directly involved in the negotiation of damage awards. The current scheme allows the BC Office to encourage settlement, but not to be directly involved in those negotiations. In addition, the BC Office believes that the ability to directly award damages in appropriate circumstances would provide positive benefits.[114]

A final tool that the BC Office believes might be useful is the ability to issue rulings or codes of practice on specific issues. The BC Office does provide policy advice but such advice must include substantial caveats because the advice is not binding and not determinative.[115]

3. Quebec

Quebec has the oldest private-sector privacy legislation in Canada. The *Act Respecting the Protection of Personal Information in the Private Sector* was adopted on June 15, 1993 and came into effect on January 1, 1994.[116] It was declared "substantially similar" to PIPEDA on November 19, 2003. PPIPS is overseen by the Commission

[112] Interview with BC Office.
[113] Interview with BC Office.
[114] Interview with BC Office.
[115] Interview with BC Office.
[116] Statutes of Quebec, chapter 17 (supp. 1993) [PIPPS].

d'accès à l'information (the "Commission"), which has a twofold function. The Commission acts as both an administrative tribunal, with a quasi-judicial function and decision-making powers, and a regulatory oversight body tasked with (among other things) investigating citizen-initiated complaints against private sector organizations.

The purpose of the Quebec Act differs from that of PIPEDA, AB PIPA and BC PIPA:

> The object of this Act is to establish, for the exercise of the rights conferred by articles 35 to 40 of the Civil Code of Québec concerning the protection of personal information, particular rules with respect to personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise within the meaning of article 1525 of the Civil Code of Québec.[117]

This difference, notably the omission of any "balancing" language, may reflect that privacy in Quebec is a right guaranteed by that province's Charter of Rights and Freedoms.[118]

Members of the public are entitled to submit "disagreements" about the treatment of personal information to the Commission.[119] Representative complaints are allowed.[120] Members of the Commission are required to provide assistance in drawing up complaints to potential complainants.[121] Upon receipt of a disagreement, the Commission conducts an examination[122] and renders a decision in writing.[123]

The Commission is granted "all the powers necessary for the exercise of its jurisdiction" and may "make any order it considers appropriate to protect the rights of the

---

[117] PPIPS section 1.
[118] Quebec Charter of Rights and Freedoms, [R.S.Q. chapter C-12] chapter 1, section 9.
[119] PIPPS section 42.
[120] PIPPS section 45.
[121] PIPPS section 47.
[122] PIPPS section 50.
[123] PIPPS section 54.

parties and rule on any issue of fact or law."[124] A decision "by the Commission becomes executory as a judgment of the Superior Court and has all the effects of such a judgment from the date of its homologation by the Superior Court."[125] Homologation occurs by filing a copy of the decision with the Superior Court in the district where the respondent is situated.[126] Any party with a "direct interest" in the matter may appeal the Commission's decision to the Quebec Court of Appeal, though factual determinations are not appealable.[127]

The Commission may also conduct an inquiry, either in response to a complaint or on its own initiative.[128] Following an inquiry, the Commission is entitled to "recommend or order the application of such remedial measures as are appropriate to ensure the protection of the personal information."[129] The naming of organizations that refuse to comply with the Commission's directions is expressly permitted by the use of a "Notice of Non Compliance."[130] Orders of the Commission after inquiry become executory in the same manner as decisions on disagreements and are subject to the same appeal rights.[131]

PIPPS does not provide the Commission with the power to award damages. Instead, under the Quebec civil law regime, an "enterprise may become liable in damages should it collect, retain, use or disclose personal information in violation of the Québec

[124] PIPPS section 55.
[125] PIPPS section 58.
[126] PIPPS section 58.
[127] PIPPS section 59 and 61.
[128] PIPPS section 81.
[129] PIPPS section 83.
[130] PIPPS section 84.
[131] PIPPS section 86 and 87.

Private Sector Act."[132] These damages, which include punitive damages when appropriate, are sought in the Quebec courts applying the typical civil law principles (wrongful act, damages and causation).[133] Finally, violations of the Act are also punishable by fines ranging from $1,000 to $10,000 for a first offence and, for subsequent offences, from $10,000 to $20,000.[134]

Quebec has also moved in the direction of attempting to mediate disputes prior to formal decisions by the Commission:

> Generally, speaking, when a request for review or an application for examination of a disagreement is received by the CAI, the parties are asked to take part in a mediation process before a hearing is held. In over half the cases, mediation leads to a solution without the need for intervention by the tribunal.[135]

Decisions of the Commission are posted on the Commission's website – most are not anonymized in any way.[136]

4. Comparisons with PIPEDA

As can be seen from the foregoing, the provincial private-sector privacy regimes differ from PIPEDA in several ways. All three provinces allow the Commissioner to make binding orders. Alberta and Quebec provide a process by which these orders can fairly quickly and easily be made into binding orders of the respective provincial courts. In addition, the Quebec and Alberta legislation makes organizations subject to fairly significant fines for violations. Alberta and Quebec also appear to have made the policy

---

[132] "Learning from a Decade of Experience: Quebec's Private Sector Privacy Law" Office of the Privacy Commissioner of Canada at page 35. While this document is a worthwhile review of the Quebec experience, it unfortunately contains virtually no discussion of the enforcement scheme.
[133] *Id.*
[134] PIPPS section 91.
[135] "Rights of Recourse" published online at http://www.cai.gouv.qc.ca/index-en.html.
[136] *See* http://www.cai.gouv.qc.ca/index-en.html (but note that most decisions are reported in French).

choice of naming names in published decisions (British Columbia has also done this, but as a practical matter no Investigation Reports have yet been published).

The overall provincial approach to privacy protection, however, is fairly similar to that taken federally. All three provinces attempt to have complainants first seek to resolve disputes directly with the organization. In addition, a mediation or conciliation approach is the preferred course of action at both the federal and provincial levels. In practical terms, given the scarcity of resources and the increased burden that a more adversarial process requires, this may be an inevitable trend. That all three provinces are apparently able to work within a conciliation model while retaining coercive powers not granted to under PIPEDA may be a telling rejoinder to the claim that, for example, order-making power would negatively impact the ability of the federal OPC to successfully resolve disputes through mediation and/or conciliation.

IV. Legislative Comparisons: Foreign Jurisdictions

A. Australia

The Australian privacy regime is governed by the federal *Privacy Act* of 1988, as amended by the *Privacy Amendment (Private Sector) Act 2000* which enacted private sector privacy regulations. The overall focus of the *Privacy Act* is to make ten privacy principles applicable to the private sector as of December 21, 2001. These "National Privacy Principles" are similar to, but not identical with, those set out in PIPEDA:

> Principle 1 - Collection
> Principle 2 - Use and disclosure
> Principle 3 - Data quality
> Principle 4 - Data security
> Principle 5 - Openness
> Principle 6 - Access and correction
> Principle 7 - Identifiers
> Principle 8 - Anonymity
> Principle 9 - Transborder data flows
> Principle 10 - Sensitive information[137]

In Australia, complaints against an organization can be instigated by private citizens individually or as the representative of a class.[138] The website of the Office of the Federal Privacy Commissioner indicates that complainants "should" attempt to contact the organization to resolve the issue before filing a complaint and provides an online "ComplaintChecker" tool that "asks you up to eight simple questions to help you see whether or not the Commissioner may be able to investigate your complaint under the Privacy Act." [139]

---

[137] *Privacy Act (AU)*, Schedule 3.
[138] *Privacy Act (AU)*, section 36.
[139] *See* http://www.privacy.gov.au/privacy_rights/ComplaintChecker/index.html. Note that the legislation does not expressly require the complainant to first contact the organization; instead, the Commissioner is barred from investigating unless (a) the complainant did so, or (b) the Commissioner is satisfied that it would be inappropriate to require the complainant to do so. *Privacy Act (AU)*, section 40(1).

Upon receipt of a complaint, the Commissioner "shall" investigate,[140] but may decline to do so (or defer an investigation) on certain grounds. These include jurisdictional issues, complaints more that one year old, those that are frivolous, when the Commissioner is satisfied that no privacy violation occurred or when satisfied that the respondent is adequately addressing the issue or has not yet had an opportunity to address it.[141] An investigation into possible breach of privacy may also be initiated by the Privacy Commissioner, even in the absence of a complaint.[142]

Conceptually, the Privacy Commissioner takes an expressly conciliatory role. Complainants are encouraged to attempt to resolve matters with the organization and the first post-complaint step is to enter a "stage of conciliation based on accepted principles of alternative dispute resolution."[143] This conciliatory approach is consistent with the Commissioner's stated belief "that compliance will be achieved most often by helping organisations to comply rather than seeking out and punishing the few organisations that do not."[144]

The investigatory powers are similar to those under PIPEDA and include the ability to obtain documents, examine witnesses and compel attendance at "compulsory conferences."[145] Refusal to cooperate with an investigation can lead to the impositions of criminal sanctions including a fine and imprisonment.[146] After investigation, the Commissioner may make non-binding "formal determinations."[147] The determination, a

[140] *Privacy Act (AU)*, section 36.
[141] *Privacy Act (AU)*, section 41.
[142] *Privacy Act (AU)*, section 40(1).
[143] "The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act" Information Sheet 13 – 2001, Office of the Federal Privacy Commissioner.
[144] *Id*.
[145] *Privacy Act (AU)*, sections 44 – 46.
[146] *Privacy Act (AU)*, sections 65, 66.
[147] *Privacy Act (AU)*, section 52.

little-used tool, may dismiss the complaint or find it substantiated.[148] If substantiated, the Commissioner may order that the respondent cease breaching the Act, redress damage suffered by the complainant or pay compensation to the complainant, including compensation for injury to feelings or humiliation.[149]

Determinations are enforceable by the Commissioner or the complainant in the Federal Court. Plaintiffs are entitled to seek legal assistance from the Australian Attorney-General in preparing and pursuing a claim. One consideration in the AG's determination of whether to provide legal assistance is hardship.[150] The Commissioner may certify findings of fact to the Court and such findings are considered *prima facie* evidence of the facts but not of whether the organization has violated the National Privacy Principles.[151] Finally, the Commissioner is entitled to seek an injunction to force compliance with the *Privacy Act*.[152]

In some cases the Commissioner issues anonymous ("de-identified") reports of investigations posted, as in Canada, on the website. While the number of case reports is significantly greater than the number of formal determinations, the Australian Commissioner publishes significantly fewer reports than does the Canadian Privacy Commissioner.[153] The Commissioner may publish identifiable information but has stated an intent to only do so where (1) an organization's violations of the Act are repeated and/or serious; (2) the organization has demonstrated an intent not to comply with its

---

[148] *Privacy Act (AU)*, section 52. Only 8 formal determinations have been made since 1989 (this includes determinations in the public and private sectors); see http://www.privacy.gov.au/act/casenotes/index.html#2002.
[149] *Privacy Act (AU)*, section 52.
[150] *Privacy Act (AU)*, section 63.
[151] *Privacy Act (AU)*, section 55B.
[152] *Privacy Act (AU)*, section 98.
[153] For example, only 18 case notes were published in Australia in 2005 and only 54 total have been published since 2002. *See* http://www.privacy.gov.au/act/casenotes/index.html#2002.

obligations; and (3) all other actions have failed. Organizations that may be publicly identified are notified in advance.[154] A review of the case notes reveals that, to date, no non-anonymous reports have been published.

In Australia, industry sectors are permitted to develop and enforce their own codes and apply to the Privacy Commissioner for approval.[155] Codes are developed by industry and, if approved by the Privacy Commissioner, that code replaces the National Privacy Principles for organizations bound by the code.[156] The approval process, which includes public consultation[157], is spelled out in detail in the legislation and includes the requirement that the code either incorporates the National Privacy Principles or set out equivalent obligations.[158] The Privacy Commissioner has published guidelines to assist industry in the development of codes.[159] At present, only three industry-generated codes of practice are in effect in Australia, with one scheduled to be revoked in April, 2006.[160]

If a code is to be enforceable by a complaint system (which also must be approved by the Privacy Commissioner)[161] the system must meet prescribed standards for how the complaints are handled.[162] All complaints, for example, must be dealt with by an independent adjudicator in a similar manner to complaints dealt with by the Privacy Commissioner.[163]

---

[154] "The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act" Information Sheet 13 – 2001, Office of the Federal Privacy Commissioner.
[155] *Privacy Act (AU)*, section 18BB.
[156] *Privacy Act (AU)*, section 16A.
[157] *Privacy Act (AU)*, section 18BB(2)(f).
[158] *Privacy Act (AU)*, section 18BB(2).
[159] "Guidelines on Privacy Code Development" Office of the Federal Privacy Commissioner (AU) 2001.
[160] *See* http://www.privacy.gov.au/business/codes/index.html.
[161] *Privacy Act (AU)*, section 18BB(3).
[162] These standards are (1) accessibility; (2) independence; (3) fairness; (4) accountability; (5) efficiency; and, (6) effectiveness. *See* Privacy (Private Sector) Regulations 2001
[163] *Privacy Act (AU)*, section 18BB(3).

1. The Australian Privacy Study

In 2004, Australia's Privacy Commissioner was tasked with "review of the operation of the private sector provisions of the Privacy Act to see whether they meet their objectives."[164] The review, issued in March 2005, was comprehensive, including 136 written submissions, 12 stakeholder sessions in cities around the country, the input of expert panels and the review of research and statistical information.

The study lays out 85 recommendations, but added that the volume should not "equate to dissatisfaction with the provisions" but, rather, that the three years of experience with the scheme had shown areas of possible improvement. [165] Business was supportive of the existing scheme, but consumers and privacy advocates were "less satisfied."[166] In addition, the study found that while Australia had not yet been found to adequate for European Commission approval, business had not found that failure to be a major impediment to trade.[167]

Getting in on the Act is a large report that deals with many aspects of the Australian legislation beyond enforcement. The Association focuses on those "recommendations aimed at improving the transparency and fairness of the Office's complaints process, and to enable it to better identify and address systemic issues."[168]

The study section on compliance begins with a statement that tracks the overall theme of the Association's report: "For the private sector provisions to be most effective in protecting individuals' privacy and in promoting the public interest in privacy,

---

[164] Getting in on the Act: The Review of the Private Sector Provisions of the *Privacy Act 1988*. Australian Office of the Privacy Commissioner, March 2005 at page 1.
[165] *Id* at page 2.
[166] *Id* at page 3.
[167] *Id*.
[168] *Id* at page 7.

organisations subject to the private sector provisions should be complying with them."[169] Australia's OPC receives approximately 800 private-sector complaints per year and, like its Canadian counterpart, has a focus on conciliating disputes. Australia, however, has made little or no use of its other powers.[170]

In terms of its approach to compliance, the Australian OPC recommended that its conciliatory approach remain in place, but indicated that it would consider whether it should be using other powers (such as the determination making power) earlier. In addition, the Office decided to consider promoting the value of self-audits by private sector organizations (no audit power exists in the Australian legislation). A recommendation that the legislation be amended to allow complainants and respondents the right to seek review of the merits of complaints decisions by the Commissioner was made. Government was also urged to consider amending the law to require regulated parties to tell individuals how to both complain to the business and to the Privacy Commissioner. Finally, greater transparency in the overall process was urged.[171]

In general terms, business was supportive of both the conciliation scheme and the Office's overall approach, suggesting that the relatively low level of complaints received by business is indicative of a "satisfactory level of privacy compliance."[172] However, "a theme in the Office's public consultations that while many organisations are trying to comply some are not worried about implications of a breach."[173]

---

[169] *Id* at page 125.
[170] *Id* at pages 125 – 126.
[171] *Id* at pages 13 – 14 and 162 – 163.
[172] *Id* at pages 131 – 132.
[173] *Id* at page 133.

In terms of the complaint process, concerns were raised over a perceived lack of transparency, delay and the lack of appeal rights.[174] It was suggested that the Office publish its complaint handling procedures online and to publish more complaint outcomes including more detailed information about complaint resolutions.[175]

On the enforcement end, participants suggested that the lack of any schedule of penalties, the lack of an audit power and the fact that the Office did not "out" privacy violators added up to a climate in which "organizations are lax about compliance."[176] Concern over systemic issues was also expressed, with some stakeholders noting that reliance on individual complaints, combined with the lack of incentives to correct systemic flaws, resulted in a situation where the cost of dealing with complaints is less than the cost of ensuring the accuracy of data in the first instance.[177] Finally, some participants expressed concern over the Commissioner's lack of coercive power, noting that "respondents are free to ignore recommendations and the only remedy for individuals is then to make a further complaint."[178] It was suggested that the Commissioner be given power to enforce directions coming from "own motion" investigations, be empowered to audit the private sector and be able to issue binding codes of conduct.[179]

The Office, however, accepted business submissions that overall compliance, while not optimum, may be substantial. It based this, in part, on the fact that "the number of privacy complaints received is very small given the millions of transactions involving personal information each day."[180] It recognized that good reasons exist for greater

[174] *Id* at pages 137 – 142.
[175] *Id* at page 142.
[176] *Id*.
[177] *Id* at page 134 – 135.
[178] *Id* at page 136.
[179] *Id* at pages 144 – 145.
[180] *Id* at page 146.

transparency, more publication of de-identified outcomes of complaints, expanded use of its enforcement powers and implementation of audit powers.[181] Ultimately, the recommendations in the area of enforcement included:

> 41 The Australian Government should consider amending National Privacy Principle 1.3 to require organisations to tell individuals how they can complain to the organisation; and that, if the complaint is not resolved, they can also complain to the Privacy Commissioner or (where relevant) the code adjudicator.
>
> 42 The Office will review its complaints handling processes and will consider the circumstances in which it might be appropriate to make greater use of the Commissioner's power to make determinations under section 52 of the Privacy Act.
>
> 43 The Office will also consider measures to increase the transparency of its complaints processes and complaint outcomes.
>
> 44 The Australian Government should consider amending the Privacy Act to:
>
> - expand the remedies available following a determination under section 52 to include giving the Privacy Commissioner power to require a respondent to take steps to prevent future harm arising from systemic issues
> - provide for enforceable remedies following own motion investigations where the Commissioner finds a breach of the NPPs
> - provide a power for the development of binding codes and/or binding guidelines in cases where there is a strong public interest, where more detailed guidance is warranted or complaints reveal recurrent breaches (see recommendation 7).[182]

[181] *Id* at page 149 – 157.
[182] *Id* at pages 162 – 163.

B. New Zealand

The New Zealand privacy laws are set out in the *Privacy Act 1993*. The overall scheme is based on 12 "Information Privacy Principles" in the following areas:

Principle 1 – Purpose of the collection of personal information
Principle 2 – Source of personal information
Principle 3 – Collection of information from subject
Principle 4 – Manner of collection of personal information
Principle 5 – Storage and security of personal information
Principle 6 – Access to personal information
Principle 7 – Correction of personal information
Principle 8 – Accuracy, etc. of personal information to be checked before use
Principle 9 – Agency not to keep personal information longer than necessary
Principle 10 – Limits on use of personal information
Principle 11 – Limits on disclosure of personal information
Principle 12 – Unique identifiers[183]

The New Zealand Privacy Commissioner ("NZ Commissioner" or "NZ Office" has a conciliatory role[184], with enforcement being vested in a Human Rights Review Tribunal.

According to the NZ Office, an average of 800 complaints per year are received.[185] The NZ Office has three investigators dedicated to intake, utilizing a triage process in which the intake officers attempt to either resolve clearly meritorious complaints by contacting the respondent or by dissuading complainants where a review of the facts discloses no violation of the Act. This intake process resolves a fairly large portion of the complaints without the need for an investigation.[186] The NZ Office does

[183] *See* http://www.privacy.org.nz/people/peotop.html.
[184] *Privacy Act (NZ)* section 69.
[185] Interview with NZ Office. For comparison purposes, the population of New Zealand is approximately 4 million.
[186] Interview with NZ Office.

not, however, utilize a refer-back system and does not require that individuals first seek to resolve complaints with the regulated party.[187]

If the matter goes forward past intake, the NZ Commissioner has wide investigatory power and broad discretion and can decide to take no action on a complaint or to seek to resolve the matter without an investigation.[188] If an investigation is conducted, the NZ Office focuses on attempts to settle the issue, including by requesting that the offender makes assurance of non-repetition of the privacy violation.[189] Unlike the Canadian jurisdictions, one typical aspect of resolution in New Zealand (for complaints with merit) is the payment of compensation to the complainant.[190]

The NZ Commissioner does not become involved directly in negotiating the amount of possible compensation. The NZ Office does, however, attempt to manage the expectations of both the complainant and respondent by discussing past, similar, cases and by pointing the parties to existing, published, case reports that often contain descriptions of compensation paid. Payment of compensation fits into the NZ Office's philosophy (also embodied in the overall legislative scheme which fits privacy rights into a human rights framework) that the focus of efforts should be individual dispute resolution.[191] The NZ Office is not, for example, focused on creating precedent or on proving breaches of the Act.[192]

If the Commissioner is unable to settle the matter, or if the complaint involves breaches of past assurances, the NZ Office renders a preliminary opinion on the facts and

[187] Interview with NZ Office.
[188] *Privacy Act (NZ)* sections 71 and 74.
[189] *Privacy Act (NZ)* section 77.
[190] Interview with NZ Office.
[191] Interview with NZ Office.
[192] Interview with NZ Office.

the applicable law, including whether a breach has occurred. This opinion is forwarded to the party on the losing side of the dispute for comment. The NZ Office sees this as another good opportunity to settle a matter.[193]

Failing a settlement, the NZ Office process is essentially at an end. The NZ Commissioner may refer the matter to a "Director of Human Rights Proceedings" for determination of whether further proceedings should commence.[194] The Proceeding Commissioner is able to bring the matter before the Human Rights Review Tribunal on behalf of an individual or a class (who are not parties unless joined in the action by the Tribunal).[195] The complainant is also entitled to bring proceedings if the Director either agrees, could proceed but chooses not to, or if the NZ Commissioner refused to go forward because of a belief the complaint lacked substance.[196] Many referred cases end up settling and no private sector cases have gone through the entire process to its culmination.[197]

The Tribunal, but not the Privacy Commissioner, is entitled to make declarations, issue orders related to conduct and award damages and costs.[198] The damages can include actual pecuniary loss, humiliation and lost expectation.[199] Actions before the Tribunal carry with them the potential of a cost award against the loser, and the process has been described as essentially judicial in nature.[200]

The NZ Office believes that the bifurcated system has worked well. Settlement rates are high, and the NZ Office does not believe that the lack of direct coercive power

[193] Interview with NZ Office.
[194] Interview with NZ Office.
[195] *Privacy Act (NZ)* section 82.
[196] *Privacy Act (NZ)* section 83.
[197] Interview with NZ Office.
[198] *Privacy Act (NZ)* section 85.
[199] *Privacy Act (NZ)* section 88.
[200] Interview with NZ Office.

leads regulated parties to believe that the Office has little power. There is a need, of course, to use persuasion and to ground opinions well in the facts and law. Overall, the NZ Office does not consider that adding powers such as order-making and "naming and shaming" would provide significant benefits. One tool that might be worthwhile (if resources were also made available) is the audit power.

In addition to the investigation/complaint mechanism, the New Zealand Privacy Commissioner seeks to create broader compliance with privacy protection principles by issuing industry-specific "Codes of Practice." The Codes are developed in negotiation with the regulated groups in a process that Colin Bennett has said is "is spelled out in greater detail in the New Zealand legislation than in any other law."[201] These Codes carry the force of law:

> Where a code of practice is in force --
>
> a) The doing of any action that would otherwise be a breach of an information privacy principle shall, for the purposes of Part VII of this Act, be deemed not to be a breach of that principle if the action is done in compliance with the code;
>
> b) Failure to comply with the code, even though that failure is not otherwise a breach of any information privacy principle, shall, for the purposes of Part VII of this Act, be deemed to be a breach of an information privacy principle.[202]

Because these Codes carry the force of law, violations can trigger the complaints and investigations process set out in the legislation. The overall "purpose of a code of practice is to increase relevance, certainty, precision and clarity…."[203] As of the date of this report, seven such Codes had been issued and six are currently active (one having

[201] Bennett, C, "Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector" (Ottawa: Industry Canada, 1996) at page 15. *See also, Privacy Act (NZ)* sections 46 – 53.
[202] *Privacy Act (NZ)*, section 53(a) and (b).
[203] New Zealand Privacy Commissioner, *Guidance Note on Codes of Practice*, December 5, 1994.

expired).[204] In the view of the NZ Office, the Codes are an important and effective tool.[205]

C. Comparison with PIPEDA

As under PIPEDA (and the Canadian provincial legislation) both Australia and New Zealand expressly seek to resolve issues by mediation and/or conciliation. In neither country is the Privacy Commissioner entitled to directly make orders or to award damages or otherwise impose monetary penalties on organizations. Instead, Australia's system is similar to PIPEDA in that complainants (and the Commissioner) may go to Federal Court to enforce the Commissioner's determinations. It is dissimilar because the Australian Privacy Commissioner's non-binding declaration may contain monetary damage awards. New Zealand, by contrast, employs a scheme in which the non-binding decision of the Privacy Commissioner is enforced before a separate Human Rights Review Tribunal.

Australia allows for "naming and shaming" recalcitrant organizations utilizing defined criteria (though it has not used this power) while New Zealand's "case notes" are anonymous (and it has published many on its website).

The most significant difference between PIPEDA's structure and that in New Zealand and Australia is the development of industry-specific codes of practice. In New Zealand and Australia, industry sectors are able to collaborate with the Privacy Commissioner in becoming self-regulatory, up to and including the establishment of internal complaint-resolution processes.

---

[204] The active codes cover (1) credit reporting; (2) telecommunications information; (3) health information; (4) justice sector unique identifiers; (5) superannuation schemes unique identifiers; and, (6) post-compulsory education unique identifiers.
[205] Interview with NZ Office.

V. Non-Privacy Legislation and Administrative Tribunals

Due to the number of administrative tribunals existing just at the federal level in Canada, any comprehensive analysis of these varying regulatory bodies is beyond the scope of this report. This section, accordingly, contains a general overview and focuses on two models for illustrative purposes. These two models represent different models of regulation. One, the CRTC, is a traditional "regulatory" scheme while the other, the Canadian Human Rights Tribunal may be the paradigmatic "rights tribunal" model.

A "rights tribunal" has been described as:

> …tribunals that are court-like in terms of their dominant responsibility for adjudicating disputes about relatively tightly defined, and private, statutory rights or benefits. These are the tribunals whose adjudicative functions and responsibilities are in point of fact indistinguishable from the adjudicative functions and responsibilities of provincial courts, when those courts are exercising their civil-law jurisdictions in, for example, family-law matters.[206]

These rights tribunals "are to be distinguished from tribunals with more general, public interest oversight responsibilities, or those that exercise delegated political powers – tribunals that are, indeed, appropriately labelled [sic] 'regulatory agencies' or, in some cases, perhaps 'government agencies' [such as] the CRTC."[207]

A. Canadian Human Rights Act

The Canadian Human Rights Act[208] ("CHRA") provides a worthwhile comparison to PIPEDA mainly because human rights and privacy rights are more similar interests than, for example, privacy and radio broadcasting rights. In fact, some have argued that privacy *is* a human right and should be entitled to protection in much the

[206] Ellis, Ron, "A Smoking Gun Reform Strategy for Rights Tribunals" speaking notes from the Canadian Council of Administrative Tribunals 19th Annual Conference (June 2003).
[207] *Id*.

same way. Certainly the New Zealand model explicitly treats privacy as a human right, vesting enforcement power in the Director of Human Rights Proceedings.

In Canada, the Canadian Human Rights Commission tries to resolve complaints of discrimination filed against federally regulated employers, unions and service providers. If a complaint cannot be resolved, the Commission may investigate the case further, and may ultimately request that the Canadian Human Rights Tribunal hear the case.[209]

Like the Privacy Commissioner and privacy rights, the Human Rights Commission has a mandate to educate and promote human rights, including reporting to Parliament on legislation.[210]

Human rights complaints are initiated by the complainant, by a third-party (with the consent of complainant or else Commission can refuse to investigate) or by Commission itself.[211] The Commission "must deal" with complaint unless one of five factors (failure to exhaust other remedies, other Act more appropriate, no jurisdiction, complaint trivial/frivolous/bad faith, acts happened more than 1 year ago or too long ago in Commission's opinion) are present.[212]

Human rights investigators have ability to obtain warrants from Federal Court.[213] After investigation, a report is prepared and sent to Commission. The Commission then decides whether to refer the complainant to another appropriate authority[214] or to request

---

[208] Canadian Human Rights Act, R.S. 1985, c. H-6 [CHRA].
[209] *See* http://www.chrc-ccdp.ca/complaints/default-en.asp.
[210] CHRA section 27.
[211] CHRA section 40.
[212] CHRA section 41.
[213] CHRA section 42.
[214] CHRA section 44(2).

that the Human Rights Tribunal begin an inquiry.[215] The Commissioner may dismiss the complaint if it is satisfied that an inquiry is not warranted, if it has no jurisdiction, if the complaint is frivolous or if the complaint is too old.[216]

In addition, the Commission may appoint a conciliator after a complaint is filed in an attempt to settle the matter.[217] If a settlement is reached by the parties, the Commission has power to approve or reject settlements. Settlements may also be enforced by application for an order from Federal Court.[218]

If Commission makes request for Human Rights Tribunal inquiry, the Tribunal Chair shall institute the inquiry.[219] The inquiry is conducted either by a single Tribunal member or, in complex cases, a panel of 3 members is appointed by Chair of the Tribunal.[220]

Proceedings before the Human Rights Tribunal are supposed to be as informal and expeditious as possible.[221] The Tribunal decides questions of law and fact[222] and has powers of superior court to summon witnesses, administer oaths and accept evidence[223] but may not receive inadmissible evidence.[224] A conciliator appointed by the Commission may not testify.[225]

[215] CHRA section 44(3).
[216] CHRA section 44(4).
[217] CHRA section 47.
[218] CHRA section 48.
[219] CHRA section 49(2).
[220] *Id*.
[221] CHRA section 48.9.
[222] CHRA section 50(2).
[223] CHRA section 50(3).
[224] CHRA section 50(4).
[225] CHRA section 50(5).

The Tribunal can dismiss the complaint if it is determined not to be substantiated.[226] In addition, the Tribunal can make orders including those that command the respondent to cease the discriminatory practice and take measures to redress the practice or to prevent the same or a similar practice from occurring in future.[227]

In addition, the Tribunal can order that (1) the person make available to the victim the rights, opportunities or privileges that are being or were denied the victim as a result of the practice, (2) the person compensate the victim for any or all of the wages lost and expense incurred, (3) the person compensate the victim for any or all additional costs of obtaining alternative goods, services, facilities or accommodation and for any expenses incurred by the victim as a result of the discriminatory practice.[228]

The Tribunal is also entitled to award $20,000 maximum in compensation for pain and suffering and award an additional $20,000 maximum for willful or reckless discrimination.[229] If the complaint came from a "hate message" the Tribunal can also order the person to cease doing it and redress the problem including by adopting a plan, paying up to $20,000 in compensation for pain/suffering, and paying up to $10,000 as a penalty.[230] Tribunal orders become effective by filing in Federal Court.[231]

B. Canadian Radio-Television and Telecommunications Commission Act

The Canadian Radio-television and Telecommunications Commission (CRTC) was established by Parliament in 1968. The CRTC is an independent public authority constituted under the *Canadian Radio-television and Telecommunications Commission*

[226] CHRA section 53.
[227] *Id.*
[228] *Id.*
[229] *Id.*
[230] CHRA section 54(1).
[231] CHRA section 57.

Act[232] and reports to Parliament through the Minister of Canadian Heritage. The CRTC is vested with the authority to regulate and supervise all aspects of the Canadian broadcasting system, as well as to regulate telecommunications common carriers and service providers that fall under federal jurisdiction.

The CRTC derives its regulatory authority over broadcasting from the *Broadcasting Act*.[233] Its telecommunications regulatory powers are derived from the *Telecommunications Act*[234] and the *Bell Canada Act*.[235] This report will focus on powers under the Telecommunications Act.

The CRTC has recently argued for enhancement of its enforcement powers in order to better achieve compliance with the legislation:

> The CRTC considers that its powers of enforcement would be enhanced if it could impose administrative monetary penalties. The Commission does not currently have the authority to impose administrative monetary penalties (fines) pursuant to the statutes that empower it. The Commission notes that Parliament has given the power to impose fines to other agencies and departments. The Commission considers that such a fining power would give it another tool to use in appropriate circumstances to assist its enforcement of the laws for which it is responsible. Nevertheless, the Commission continues to ensure regulatory compliance within the scope of its powers under the *Telecommunications Act* and the *Broadcasting Act.* Although the government has indicated that it is prepared to give the telecom sector the power to impose fines, and looking into it on the broadcasting side, it has not at this time introduced legislation in Parliament to do so.[236]

[232] R.S.C. 1985, c. C-22, as amended.
[233] S.C. 1991, c. 11, as amended.
[234] S.C. 1993, c. 38, as amended.
[235] .S.C. 1987, c.19 as amended.
[236] CRTC Performance Report for the period ending March 31, 2005 available online at (http://www.crtc.gc.ca/eng/BACKGRND/dpr2005/dpr2005.htm).

C. Telecommunications Act – Powers of the CRTC

The CRTC can, on application of interested person or own initiative, make inquiries and determination of telecommunications issues.[237] Among its powers, the CRTC may make mandatory and restraining orders.[238] The CRTC may also make findings of law and fact and is not bound by judicial findings (though those are admissible evidence.[239] The CRTC is granted the "powers of a superior court" with respect to the conduct of inquiries including the power to compel evidence and to enforce its decisions.[240] The CRTC is entitled to award costs, including those "of and incidental to proceedings before it" and to determine by whom and to whom those costs are paid.[241]

Other powers of the CRTC include making rules, orders and regulations respecting any matter or thing within the jurisdiction of the Commission.[242] CRTC decisions are able to be made into orders of the Federal Court or of the superior court of a province and, as such, are enforceable as if that court had issued the order.[243] To do so, the CRTC must either follow the usual practice of the court in such matters or file with the registrar of the court a certified copy of the CRTC decision.[244] The CRTC may, however, enforce its decisions whether or not the decision is made into an order of the Court.

The CRTC may appoint any person to inquire into and report back on any matter within the Commission's jurisdiction. In addition to appointing any person to make an inquiry, the Commission may designate inspectors for the purpose of verifying

[237] Telecommunications Act section 48.
[238] Telecommunications Act section 51.
[239] Telecommunications Act section 52.
[240] Telecommunications Act section 55.
[241] Telecommunications Act section 56.
[242] Telecommunications Act section 57.
[243] Telecommunications Act section 63.
[244] Telecommunications Act section 63.

compliance under any Act for which the CRTC is responsible.[245] Investigators have wide powers of inspection including the ability to review documents, enter property and utilize data processing systems of organizations subject to regulation under the Act.[246]

Persons who have sustained "loss or damage" as a result of any breach of the CRTC Act is entitled to file suit to recover those damages.[247] In addition, contravening the CRTC Act is an offence punishable on summary conviction by fines ranging, in the case of an individual, from a maximum of $5,000 (first offence) to $10,000 (second and subsequent offences) or, in the case of an organization, from a maximum of $50,000 (first offence) to $100,000 (second and subsequent offences).[248]

D. Comparison with PIPEDA

The most notable difference between PIPEDA and the CRTC and Human Rights Tribunal models is that, despite being on opposite ends of the regulatory spectrum, both the CRTC and the Human Rights Tribunal are essentially able to make binding orders. Granted, the CRTC orders are made binding by filing with the Federal Court but that is significantly different than the PIPEDA structure, which allows recourse to the Court but only in the context of an action that must proceed in the normal fashion.

The Human Rights Tribunal is entitled to award damages while the CRTC may only make an award of costs. In both cases, however, violations of the respective legislation may lead to the imposition of criminal penalties against non-compliant parties (though in the case of the CRTC, it is not able to levy fines directly).

---

[245] Canada Radio-Television and Telecommunications Act section 71.
[246] *Id.*
[247] Canada Radio-Television and Telecommunications Act section 72.
[248] Canada Radio-Television and Telecommunications Act section 73. In addition, violations of certain specific provisions of the Act can be punished by fines of up to $1,000,000.

Both the CRTC and Human Rights Tribunal attempt to resolve matters using alternative dispute resolution processes. This appears to be a near-universal trend and, as far as can be determined, is not significantly negatively impacted by the differing powers granted to each body. Most of the privacy regulators surveyed for this report utilized some form of mediation or conciliation as the primary dispute resolution paradigm.

VI. PIPEDA: Legislative Reforms and Options for Change

A. Introduction

This section of the report sets out suggested reforms to the PIPEDA enforcement regime. These reforms are grouped into two primary categories; those that require no changes, or minor changes, to the existing legislation and those that would require substantial changes to the legislation. In each section, the particular item under consideration is stated, followed by a discussion of the pros and cons and concluding with the Association's recommendation.

It should be noted that, in the case of reforms requiring legislative change, there may be no better time than now to implement these suggestions. This is because PIPEDA is up for a mandatory five year review in 2006 – legislative change will perhaps be more likely to succeed if it comes out of this legislative review. Finally, the placement of a reform in the first "minor" category is not meant to suggest any particular ease of implementation; changes in practice that do not require the legislation to be amended may, nevertheless, still require substantial alteration of existing practices and be difficult to implement.

B. Reforms Requiring No Changes to PIPEDA

1. Commissioner Reports

Item: Attempt to have complainants and respondents come to an agreed statement of facts.

Discussion: Near unanimity among privacy advocates was achieved on the issue of the means by which the OPC reaches factual conclusions. The current process received little support, and most people suggested or agreed that it would be helpful if the

investigators attempted to reach consensus among the parties on an agreed statement of facts. This would allow regulated parties a better understanding of how to comply with the legislation in particular factual circumstances. It would also enable complainants and respondents to have input into the final version of facts upon which the commissioner's decision is based. Other than an additional time commitment involved in taking this approach, there appears to be little downside to at least making the attempt to reach agreed statements of facts.

Recommendation: Establish a policy preference for the use of agreed statements of facts in investigation reports.

Item: Allow complainant the chance to formally rebut and/or comment on respondent's version of facts.

Discussion: Along similar lines to the suggestion of coming to agreed statements of fact, providing the complainant with an opportunity to comment on the respondent's version of the facts augers in favor of greater accuracy. A respondent could also be permitted to comment on the complainant's version, with the ultimate goal of coming to an agreed statement of facts (either in full or in part) upon which a decision can be based.

The OPC description of the investigative process, however, suggests that this concern is misplaced. According to the Office, investigators already engage in substantial back-and-forth and all parties are entitled to comment on the opposing party's factual assertions. Copies of the submissions of each party are forwarded to the Commissioner as part of the final report of the investigator.

Recommendation: Implement a formal policy ensuring that each party has a full opportunity to respond to the other party's factual account.

Item: Issue only one version of facts.

Discussion: This suggestion is, again, designed to achieve maximal accuracy and clarity with respect to the background facts on which a decision is based. For regulated parties looking to the decisions of the Commissioner to guide future conduct, accurate understanding of the facts underlying a decision is critical. The current system involves the issuance of potentially three differing sets of facts (to the complainant, to the respondent and that made public by the OPC).

Note, however, that the Commissioner takes the position that the reports sent to the complainant and the respondent are substantially identical. If so, this concern is less significant and turns simply on the level of detail contained in the published report (discussed below). To the extent that complainants and respondents are receiving different versions of the facts, it is unclear what benefit is drawn from this procedure but the drawbacks are apparent; inconsistent factual support makes it difficult for complainants and regulated parties to understand the interpretation of the Act.

Recommendation: Review policies and ensure that reports sent to complainants and respondents are substantially identical.

Item: Increase the detail contained in published reports.

Discussion: The public reports issued by the OPC have been criticized for lacking sufficient detail. From the perspective of regulated parties, including private consultants who advise regulated parties on compliance issues, the devil is truly in the details. As with the interpretation of case law, the interpretation of privacy decisions is dependent on both a recitation of the facts and the application of the legislation to those

facts. The current reports can be lacking in sufficient detail and, thus, have little value to guide future compliance or complaints.

The OPC response to this concern was to suggest that concerns over the specificity in the reports misapprehend the purpose. On this view, reports are not intended to be treated as binding in the way that, for example, caselaw is regarded for purposes of *stare decisis*. Instead, the published reports serve as general descriptions of results in particular factual circumstances. Increased detail, and a corresponding shift toward a model more akin to the development of jurisprudence, would remove some of the flexibility accorded to the Commissioner and the conciliatory role played by the Office in the ombuds-model.

The Commissioner argues that it "must be underscored that the ombuds-role is not simply remedial but transformative in nature."[249] With "twin goals" of resolving individual complaints and the "development of a lasting culture of privacy sensitivity…through their willing and active involvement in the process" the Commissioner takes the position that the process requires a flexibility that would be lost if reports were treated more like case law.[250]

Recommendation: Retain current level of factual detail in published reports.

Item: Evaluate the impact of the newly-implemented 30-day report back period after report issued.

Discussion: In 2004, the Commissioner instigated a process for systematically following up on complaint investigations. The goal of this process, according to the OPC, is twofold. First, it highlights to organizations that the OPC expects the

[249] Stoddart at page 7.
[250] Stoddart at page 7.

organizations to "take remedial measures in response to specific problems identified in complaint investigations."[251] Second, it "provides a reliable ongoing record of organizations' compliance with *PIPEDA*."[252] Early results from this new process are encouraging. The OPC reports that, in 2004 and early 2005, it completed more than 50 follow-ups on "significant unverified cases…involving the federally regulated organizations that had been subject to *PIPEDA* from the beginning."[253] These cases had identified particular problems and "specified remedial action" had been suggested to the organizations.[254]

The Commissioner reports a high success rate. Organizations had "fully implemented" the recommendations "about nine times out of ten" and, in 67 percent of these, had taken "some degree of systemic improvement."[255] In approximately half of the satisfactory responses, the improvements occurred as a result of the complaint investigation process as opposed to specific recommendations contained in letters of findings.[256]

Recommendation: Implement a permanent review process designed to measure compliance and publish the results in the Commissioner's annual report.

2. General

Item: Increase funding provided to the Office of the Privacy Commissioner.

Discussion: This is a relatively uncontroversial suggestion. Certainly increased resources, particularly in the case of the audit power, have the ability to make a

[251] Annual Report 2004 at page 71.
[252] *Id.*
[253] *Id*.
[254] *Id.*
[255] *Id* at page 72.
[256] *Id.*

significant impact in the Office's ability to monitor compliance with PIPEDA. It is an open question, however, whether increased resources alone would be able to deal with the increasing backlog of cases within the Office. Some privacy advocates suggest that increased resources are, at best, a temporary band-aid.

Recommendation: Increase funding. Additional funding for the Office would both increase its capability to enforce compliance with the legislation and signal to the regulated parties that government is committed to a vibrant private-sector privacy regime. For example, additional funding could be utilized to provide complainants with legal assistance in launching court actions under section 14. The model for provision of legal services to human rights complainants in British Columbia may be a useful model for consideration.[257]

Item: Increase the Commissioner's use of audit powers, including the institution of "site visits" and establish guidelines for when to use those powers.

Discussion: This, again, was a relatively uncontroversial suggestion. The concept of site visits, designed to spot-check a particular organization's compliance with PIPEDA, presents a means by which the audit power can be used in relatively resource-friendly ways. The major hurdle to increased use of the audit power (besides resources) is the lack of articulated standards as to what constitutes "reasonable grounds" to initiate the process. The OPC is currently developing such standards.

Recommendation: Begin to utilize site visits by initiating contact with regulated parties and seeking consent to discuss and review existing privacy policies. Finalize and

[257] *See, for example*, the services provided by the BC Human Rights Coalition at http://www.bchrcoalition.org/.

publish guidelines for use of the audit power and use such powers in appropriate circumstances.

Item: Publish formal policies on investigations, complaint resolutions and criteria for audits, site visits, litigation and the exercise of the discretion to identify respondents.

Discussion: This proposal goes to the transparency of the complaint resolution and enforcement process. The establishment and publication[258] of formal policies allows the public greater certainty and clarity with respect to the handling of complaints. The regulated parties would also benefit from clarity in understanding when the audit power (including site visits) would be utilized and under what circumstances the Commissioner might use more consequential enforcement powers such as naming names.

Recommendation: That the Office of the Privacy Commissioner publish its formal policies online and, upon request, provide copies to the public in printed form. In addition, the Office should conduct regular reviews of its own compliance with internal policies and publish the results in the Commissioner's annual report.

Item: Undertake a comprehensive study of compliance.

Discussion: The Australian study represented a major contribution to understanding the utility of privacy legislation and the level of public and industry knowledge and acceptance of a privacy-protection culture. The limitation of the Australian study was that it was undertaken by the Office itself, which is an important initiative, but arguably resulted in a report lacking sufficient independence. Resources

[258] In interviews with OPC staff, the Association learned that certain formalized procedures were already in place and that others were being implemented. The Association requested additional information from the OPC including the process by which the decision of whether to name names was reached, but as of the time of finalizing this report the information had not been provided.

should be found to fund a similar study by an appropriate independent third party. This would be very helpful to an overall understanding of how well the current enforcement model is achieving the goal of fostering widespread compliance with PIPEDA.

Recommendation: An independent and comprehensive review of compliance with the legislation should be conducted.

Item: Identify respondents in published reports.

Discussion: The naming of names is one of the most controversial suggestions for reform. Indeed, opinions are divided about whether the existing legislation allows the Commissioner to name names, much less the efficacy of the practice.[259] Privacy advocates are very adamant that the "shaming power" inherent in naming privacy violators would substantially increase the likelihood of compliance by regulated parties. This view follows from the assumption that a company might suffer negative economic/market repercussions as a result of being publicly named in an adverse privacy result.

Regulated parties are as adamant in their opposition to, at least, the routine naming of names. The argument is that regulated parties are trying to comply with the legislation but, particularly in the case of large corporations, human error dictates that some privacy violations will occur even in the most privacy-sensitive organization. Why should an entire corporation be penalized for what may well be the inadvertent error of one employee?

[259] The Association's view is that, to the extent there is uncertainty in whether this power can be utilized regularly, the OPC, which has an important responsibility for advocating strong legislative protections for privacy, should be proactive in the utilization of this power. If there is disagreement with the legislative propriety of identifying respondents, the option of bringing an action to seek interpretation of the legislation exists. Indeed, it would be important to clarify this uncertainty jurisprudentially.

Regulated parties also argue that the economic impact may be disproportionate to the violation and that some privacy complaints are lodged as a result of motivations having little to do with privacy protection. These arguments have some force and, at least in the cases of routine naming of violators names, may auger against such a policy as too extreme.

Privacy consultants also appear reluctant to endorse the naming of names. The principal concern expressed is that the potential for this outcome may reduce the overall number of published reports because the Office would, either explicitly or implicitly, begin to utilize a higher standard before making the decision to publish a report. A decrease in the overall number of published reports would adversely impact privacy consultant's ability to advise their clients in industry as to the application of the Act to specific factual situations. On this view, overall compliance may well be reduced because regulated parties would no longer have the benefit of voluminous published reports to guide their actions.

The Commissioner has suggested that the practice of naming names may be contrary to the Act: "On this issue, section 20 of PIPEDA is very explicit in binding the Commissioner and her staff to a statutory obligation of confidentiality…."[260] This duty of confidentiality "has been recognized by the courts as an essential feature of the ombuds-model."[261] On this view, the Commissioner is simply not permitted to "on a systematic basis…link…names with the outcomes of cases…" even though the

[260] Stoddart at page 9.
[261] *Id*.

legislation "does recognize that there may be exceptional situations where the obligation of confidentiality…is outweighed by the public interest…."[262]

The current practice of virtually never naming the respondents appears overly cautious; surely some complaints can be determined to be both substantial and significant violations caused by something other than human error. Moreover, the practice of naming fits with the approach taken by other regulators. The development of a set of criteria surrounding the publication of offenders' names may be a workable middle ground, particularly if those criteria contain language preventing routine disclosure and saving this power for repeat or flagrant privacy violations, or unwillingness to work toward a resolution of a dispute. The Commissioner has suggested that applicable criteria might include (a) the development of a clear record; (b) the demonstration "that the decision to disclose was made on a case-specific basis"; (c) a rational connection between disclosure and protecting the public interest; (d) a balancing of the duty of confidentiality with the public interest; and, (e) limiting the extent of the disclosure to "only that information necessary to meet the specified purpose."[263]

Recommendation: The OPC should identify respondents in published reports.

C. Reforms Requiring Changes to PIPEDA

1. Access to Justice

Item: Allow access to the court system prior to the filing and resolution of a complaint with the Office of the Privacy Commissioner.

Discussion: Given the current caseload of the OPC, one challenge facing potential privacy complainants is simply that of time. The legislation currently requires a

[262] Stoddart at page 10, *citing* PIPEDA section 20(2).
[263] Stoddart at page 10 – 11.

privacy complainant to pursue his or her remedies with the OPC prior to filing any litigation in the Federal Courts. On the one hand, this requirement makes common sense; if a matter is resolvable by the OPC, it seems inefficient to allow litigation to proceed along a parallel track.

In practical terms, however, the requirement substantially delays the ultimate resolution of the dispute (assuming it is not disposed of by the OPC process). The OPC goal is to resolve complaints within one year of filing but a lack of resources is delaying final decisions past that one year mark and the case backlog is growing, not shrinking. Given the length of time inherent in litigation, the reality faced by privacy complainants that seek redress in the Court is that a final decision may only come many years after the incident giving rise to the complaint. One way to speed along the process would be to remove the requirement that resolution be sought before the OPC before allowing recourse to the courts. The drawback to this reform might be, however, to dissuade regulated parties from substantial participation in the OPC conciliation and settlement process. On balance, reforming the legislation to allow pre-report suits is likely to have little practical effect. Most complainants will still chose to utilize the OPC process first, as it comes with little cost and little downside.

Recommendation: The legislation should not be amended to allow suits in the Federal Court prior to disposition of a complaint by the OPC.

Item: Allow representative complaints before the OPC and class-actions suits in the Federal Court.

Discussion: The current scheme does not speak to the possibility of either representative complaints before the OPC or class action suits to protect privacy rights.

The essential goal of allowing such actions is to enable complainants/litigants to utilize the economy of scale and to, perhaps in the case of class-action suits, to entice lawyers to take on privacy litigation. Additionally, on the compliance end, the potential for substantial class-action awards may prompt otherwise-recalcitrant regulated parties to take more seriously the downside of their failure to comply with the legislation.

Recommendation: The legislation should be amended to allow representative complaints before the OPC and to allow complainants (including, perhaps, third-party representatives) to file class actions suits in the Federal Court.

2. Commissioner Reports and Powers

Item: Give the Commissioner the power to issue binding orders.

Discussion: An oft-repeated criticism of the PIPEDA enforcement model is that it simply does not have "teeth." One reason for the lack of teeth, privacy advocates argue, is that the Commissioner does not have the authority to issue binding orders. When coupled with the practical reality that very few complainants have the wherewithal (either financial or in terms of time) to pursue an action to enforce the Commissioner's findings in Federal Court and the OPC's non-utilization of the section 15 powers[264], this means that regulated parties are able to ignore the Commissioner's decisions with some degree of impunity.

The response to this suggested reform has been to claim that providing order-making powers would radically alter the Commissioner's role as an ombudsman. The spillover from this change might be to make the investigation and conciliation process more adversarial, with corresponding negative effects on the number of settled cases.

[264] A review of the existing caselaw reveals that the Commissioner only appears as a respondent in all litigation under PIPEDA in which the Commissioner is named as a party.

Instead of remaining primarily geared toward consensual resolutions, the overall process may become litigious. Indeed, the Commissioner argues that an "adversarial, litigious and less flexible approach…is a necessary adjunct to the order-making model…."[265] This overstates the case. Some increase in the adversarial nature of the process may well occur, but the experience in other jurisdictions demonstrates that schemes which include order-making power are still able to resolve cases by settlement or other voluntary agreement. One can reasonably argue that such authority would provide a strong incentive to recalcitrant organizations to be more responsive to mediation and, ultimately, to comply with the legislation.

The Commissioner also suggests that her "extraordinary investigative powers…are, at least in part, the correlative of her lack of order-making powers."[266] Her role as "a trusted 'truth-finder' striving to elicit…all the necessary facts and considerations in order to reach lasting solutions" might, on this view, be negatively impacted by having the ability to make binding orders.[267] It is unclear, however, why this would be so. Certainly the other jurisdictions that also act primarily as conciliators appear not to be overly burdened in their efforts at voluntary resolutions simply because, when those voluntary resolutions prove impossible, orders may issue.

Nor is it entirely clear how the investigative powers would suffer if the Commissioner is given order-making ability. Recourse to the sweeping powers of investigation is exceedingly rare and, in those jurisdictions with order-making power, investigators retain a full range of investigatory powers.

---

[265] Stoddart at page 14.
[266] Stoddart at page 13.
[267] Stoddart at page 13.

Recommendation: The Commissioner should be explicitly given the power to issue orders that are able to be filed with the Federal Court and made immediately enforceable.

Item: Allow the Commissioner to impose monetary fines for violations of the Act.

Discussion: The Commissioner is currently not entitled to fine organizations for non-compliance with the Act. It is suggested that the legislation be amended to give the Commissioner power to impose monetary fines against organizations that have been found to have breached the Act.

Providing the Commissioner with the ability to levy fines in appropriate circumstances is a reform that has attracted a fair amount of support among privacy activists. The OPC, however, is less enthusiastic.

As we see from the discussion of administrative tribunals, above, most such bodies are granted the power to impose monetary fines. The maximum fines vary significantly, but the power is there. The most obvious benefit of allowing the Commissioner to fine violators is that it provides an additional incentive to organizations that have either failed to take steps to comply with the Act or failed to achieve compliance. Metaphorically, the Commissioner's toolbox would contain a bigger stick than it currently does.

It is difficult to determine how effective the fining power would be. In the case of large organizations, fines – unless dramatic – might be regarded as simply a cost of doing business. Small and mid-sized businesses would be more likely to be significantly impacted by fining power.

From the OPC perspective, adding a fine power would radically reconstitute the Office's role in much the same way as providing order-making power; the model begins to look less like an ombudsman and more like a quasi-judicial tribunal. It is unclear, however, whether a shift in emphasis would therefore be a significant negative. Certainly from the perspective of some privacy advocates, moving away from the ombuds-model would be a significant positive in terms of achieving compliance with the Act. That said, fining is a more punitive measure than, for example, issuing orders requiring compliance with the legislation and a greater departure from the dispute-resolution model in place in most privacy jurisdictions.

Recommendation: The Commissioner should not be given the power to issue fines against respondents.

Item: Allow the Commissioner to make compensation awards to complainants.

Discussion: Complainants who have well-founded complaints are not able to be compensated by the Commissioner for damages that flow from a privacy violation. In order to seek compensation, whether in the form of actual or special damages, a complainant must go through the Federal Court process – and only after having completed the OPC process. This inability to compensate victims of privacy breaches has been criticized.

This reform is subject to the same criticism as the provision of order-making or fining powers; it changes the model significantly. Compensation awards, however, are not as clearly punitive in the way that fines are and fit more closely with a model that emphasizes a focus on restitution for the harm caused to the complainant by the privacy intrusion. The ability to award actual damages alone, however, might not be a sufficient

disincentive to organizations that could consider such awards as a cost of doing business. In the case of particular egregious violations, the ability to impose some form of punitive damages would provide an important public condemnation of the actions of the respondent. Though punitive damages themselves might also be factored as a cost of doing business by the respondent, negative publicity attendant to an award of punitive damages may provide significant adequate incentive to comply.

Recommendation: The legislation should be amended to allow the Commissioner to award compensation to complainants and, in egregious cases, to award punitive damages against respondents.[268]

Item: Institute a process for the creation of industry-specific standards and/or codes of practice.

Discussion: This is, perhaps, one of the more intriguing possibilities. The overall concept would be to increase the role of industry in self-regulating compliance with privacy principles. Industry may welcome an opportunity to actively participate in the crafting of privacy rules that make sense in a particular field. In addition, organizations that are able to demonstrate compliance with industry-specific standards might be able to use that compliance as a positive marketing tool. And if, as in New Zealand, industry sectors are encouraged to institute their own complaint-handling procedures, the resource burdens currently facing the Office might be ameliorated.

[268] Evidently, if the Commissioner has the power to make orders and compensate victims for harm suffered due to non-compliance, the model shifts from an ombuds-model to a quasi-adjudicative one. Such a shift will inevitably raise issues of fairness and due process with respect to the OPC's role as investigator, prosecutor and adjudicator in one agency. This problem has been addressed in legislation in BC and Alberta by structuring the agency in a way that compartmentalizes the roles of staff and the Commissioners with respect to mediation/investigation vs. adjudication.

This potential reform attracted little criticism; many thought it an interesting idea but had little input because the concept was foreign. It is worth noting, however, that the provincial privacy laws do make distinctions between certain types of relationships. BC and Alberta, for example, treat the employee/employer relationship slightly differently than the customer/organization situation. Unfortunately, the experience with industry-specific codes in Australia and New Zealand is relatively minor. Few industries have availed themselves of this right, though the New Zealand Office reports that the codes are a positive part of their overall model. The reasons for this are unclear but a fair assumption may be that any perceived benefits are outweighed by what would of necessity be a fairly steep commitment of resources at the front-end.

Recommendation: The option of creating industry-specific codes of practice, either by industry with OPC approval or by the OPC with industry consultation, is worthy of additional study as a potential future compliance tool.

VII. CONCLUSION

Experience with the first five years of PIPEDA has resulted in some dissatisfaction with the lack of pro-active and vigorous enforcement of the legislation. That said, the experience of this research report suggests that there is presently a serious commitment within the OPC to enhance enforcement under the existing model. To the extent that the existing model is retained, there are a variety of important reforms that could be undertaken immediately.

Notwithstanding that fact, reforms to the current model would likely enhance compliance with PIPEDA. There are stronger enforcement tools available and in use in other privacy jurisdictions that will enhance compliance even further while still retaining the dispute-resolution focus of the ombuds-model. The time for a cautionary and cooperative approach to enforcement while organizations became familiar with their legislative obligations is rapidly passing or has passed. A stronger quasi-adjudicative model has the dual benefit of permitting mediated resolution as well as the more effective compliance tool of determining rights and obligations and making appropriate orders and compensation awards without the considerable barrier of access to justice via a formal court enforcement mechanism under the current model.

APPENDIX A: LIST OF INTERVIEWEES

Office of the Information and Privacy Commissioner of Canada

Carman Baggaley, Acting Director General, Strategic Research and Analysis Division

Stephanie Perrin, Director, Strategic Policy and Research

Ann Goldsmith, Legal Branch

Jennifer Barrigar, Legal Branch

Trevor Shaw, Audit Branch

Brian Stewart, Investigations

British Columbia Office of the Information and Privacy Commissioner

Mary Carlson, Director

Alberta Office of the Information and Privacy Commissioner

Elizabeth Denham, Director PIPA

New Zealand Office of the Privacy Commissioner

Blair Stewart, Assistant Privacy Commissioner

Privacy Consultants

David Flaherty, David H. Flaherty Inc., Privacy and Information Policy Consultants

Terry McQuay, Nymity Inc.

Privacy Advocates

Pippa Lawson, Canadian Internet Policy and Public Interest Clinic, University of Ottawa, Faculty of Law.

Murray Long, Murray Long & Associates, Inc.

John Lawford, Counsel, Public Interest Advocacy Centre.

Regulated Parties

Drew McArthur, Vice-President Corporate Affairs, Telus Communications Inc.

Academic

Philip Bryden, Dean, Faculty of Law, University of New Brunswick

Craig Jones, adjunct professor of law, Faculty of Law, University of British Columbia (Mr. Jones is also a member of the BCCLA Board of Directors and a partner in the Vancouver law firm of Bull, Houser, Tupper)

Professor Michael A. Geist, Canada Research Chair in Internet and E-commerce Law University of Ottawa, Faculty of Law