Powers and Functions of the Ombudsman in the *Personal Information Protection and Electronic Documents Act*:

An Effectiveness Study

Research Report

France HOULE and
Lorne SOSSIN

August 2010

Research commissioned by the
Office of the Privacy Commissioner of Canada

The opinions expressed in this study are those of the authors of this report and do not necessarily reflect those of the Office of the Privacy Commissioner.

PREFACE

The Privacy Commissioner gave us a mandate, under subsection 58(2) of the *Privacy Act,* to conduct an analysis of the law and policies underlying the protection of personal information by the private sector.

The overall objective of this research contract is to examine the structure, mandate and powers that have been assigned to the OPC, as instituted by the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Under the terms of our contract, our analytical perspective is to conduct an effectiveness study of Part I of the *Personal Information Protection and Electronic Documents Act*. The Office of the Privacy Commissioner wants to know our opinion on the following general question: Is the ombudsman (or "Ombuds") model effective in regulating private-sector practices for the protection of personal information? More specifically, the OPC first asked us to examine the public policies underlying the origin of the Act and the history of the legal framework to date, and to analyze the functions and powers assigned to the Office of the Privacy Commissioner as well as their use by the commissioners appointed to that public office since the passage of PIPEDA. The objective of these analyses is to assess the impact of that use on compliance by the organizations subject to the Act. The next task, based on our findings on any problems identified, is to examine other Canadian and foreign institutional models (also created to regulate the use of personal information by private-sector organizations) from a comparative perspective to develop recommendations for reform.

The ideas and analyses contained in this report are intended to promote reflection on possible ways to improve protection of the personal information of citizens and permanent and foreign residents living and working in Canada, doing business here, or consuming goods and services produced by large, medium and small Canadian businesses. We hope that our analysis will generate debate and interaction among governments, industries, experts and

consumers. Given the complexity of federal, provincial and supranational regulations in this area, our analyses are not, and do not claim to be, the final authority on this issue.

For more information on this report, please contact:

France Houle
Full Professor
Faculty of Law
University of Montreal
P.O. Box 6128, Station Centre-ville
Montreal, Quebec H3C 3J7
514-343-6870
Email: france.houle@umontreal.ca

Lorne Sossin
Full Professor
Faculty of Law
University of Toronto
39 Queen's Park
Toronto, Ontario M5S 2C3
416-946-8229
Email: lorne.sossin@utoronto.ca

ACKNOWLEDGMENTS

The authors extend particular thanks to their research assistants: Mélissa Blaise, Nicolas Vermeys, Anne-Catherine Boucher, François Goyer, Kristen Rohr and Jeffrey Baggs, as well as all of those who agreed to participate in our empirical survey, whose names and institutional affiliations cannot be disclosed because of our commitment to preserve their full anonymity.

Finally, our special and most sincere thanks to the staff of the Office of the Privacy Commissioner, who assisted us in preparing this report by providing a vast amount of information and granting us the time necessary to answer our many questions.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

Objectives of the study 1

Research methodology 1

General conclusions 1

Context 5

Challenges 7

Strengths and weaknesses 7

Specific conclusions and recommendations 11

RESEARCH REPORT 17

General Introduction 17

PART I: PIPEDA: An act integrated with competition law 21

Part II: Approaches and alternatives in evaluating the Privacy Commissioner's PIPEDA jurisdiction 111

GENERAL CONCLUSIONS AND RECOMMENDATIONS 163

BIBLIOGRAPHY 173

APPENDIX A 193

PART III – Assessment of monetary penalties 193

APPENDIX B 197

Administrative monetary penalties 197

EXECUTIVE SUMMARY

Objectives of the study

In April 2009 the Office of the Privacy Commissioner mandated us to analyze the effectiveness of Part I of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). More specifically, we were asked to examine the effectiveness of the structure, mandate and powers assigned to the Privacy Commissioner, in order to answer the following general question: is the Ombuds model effective in regulating private-sector practices for the protection of personal information?

Research methodology

To conduct this analysis of the effectiveness of PIPEDA, we reviewed the literature, emphasizing analysis of the macro-economic, political and legal discourse of stakeholders who had a role in developing the Act. This mainly involved examining the public policies underlying the genesis of the statute and the history to date of the legal framework, and analyzing the functions and powers assigned to the Office of the Privacy Commissioner as well as their use by the commissioners appointed to that public office. In this regard, we were also required to examine other Canadian and foreign institutional models (also created to regulate the use of personal information by private-sector organizations) from a comparative perspective. For the review of use of legislative powers, we conducted interviews of private stakeholders to learn their views about the effectiveness of PIPEDA.

General conclusions

The Ombuds model and existing compliance activities have succeeded in achieving important goals. However, in light of these achievements, should more be accomplished and, if yes, how should it be done? Our research leads us to believe that there is a shift toward ensuring greater protection of consumers, which will need to be addressed by granting other specific powers to the

OPC. However, before modifying PIPEDA, we urge the OPC to consider conducting further research on several topics. Indeed, several pieces of the puzzle are missing to form a better picture of the actual environment in which PIPEDA actually operates and will have to operate in the future. In view of this statement, we recommend that further research be conducted:

- **Recommendation #1: Future research questions**

    1. The issues and challenges raised by Web 2.0 and the harmonization of national and supranational regulatory systems.
    2. The adaptability of the Ombuds model under PIPEDA for effective regulation of this new technological environment.
    3. The adaptability of the contemporary federal model (division of powers, human rights, federal-provincial cooperation) to meet these new issues and challenges. In particular, examine theories about functional interpretation of the constitution and the possibilities represented by the concept of networked federalism.

This being said, and starting from the hypothesis that there exists a shift toward ensuring greater protection of consumers, the question as to whether more powers should be given to the OPC to fulfill greater responsibilities in protecting consumers will need to be addressed. Should the OPC consider this option, we offer the following recommendations.

- **Recommendation #2: Extending the limits of the Ombuds Model to small and medium businesses**

The Ombuds model was particularly well suited to the first phase of regulating industry, where there was considerable concern about the impact of regulation on commercial enterprise. However, the current model does not appear to be as well suited to the small and medium business sector, where compliance rates are lower, and the risk to personal information is greater. The OPC should continue to use its existing leverage under the Ombuds model to achieve compliance with PIPEDA, especially from large businesses (e.g. banks, insurance companies, utilities, information technology and media); and to continue to target medium and small business sectors for outreach, education and incentives for compliance.

- **Recommendation #3: Granting limited order-making powers**

Ultimately, notwithstanding the important successes of the OPC, compliance levels with PIPEDA arguably remain too low, and the risk that consumers face with their personal information in the hands of small and medium sized businesses in Canada arguably is too high. While outreach, education and incentives for compliance targeted to small and medium business sectors are important, they may well be insufficient. Looking to the experience of provincial regulators in Canada, as well as to the American and European experience, the ability to levy fines and other order-making capabilities can lead to additional compliance and serve as an important deterrent even if not used often. The benefits to adopting this approach appear tangible while the risks

appear less compelling. The risk, for example, tends to focus on the anticipated negative reaction from businesses, increased adversarial tensions, litigiousness, as well as added cost and complexity both for the OPC and for businesses. The provincial experience with regulators who have order-making powers, however, suggests these risks may be overstated.

While we are certainly not the first to advocate greater order making, we do not believe the OPC at this point needs broad and intrusive powers, such as cessation orders. We believe that enhancing the order-making power of the OPC should be narrowly targeted to the kinds of enforcement activities appropriate to small and medium sized businesses (for example, fines and penalties). It is in these sectors where compliance appears to be the lowest, and where all the available data from provincial enforcement suggests that only the threat of penalties which affect the bottom-line can lead to a change in business behaviour, and ultimately, in business culture. While order-making may not be as necessary in the large business sectors, where the OPC already has made progress in enhancing compliance, it may have a salutary effects in this context as well. The order-making power may enhance the significance of privacy policies through these sectors and the profile of compliance officers. Further, given the positive experience with collaboration, consultation and engagement from this sector with the OPC, there is an important foundation of institutional knowledge, trust and credibility on which to build if additional regulatory tools are provided to the OPC.

The additional powers described are likely to lead to the OPC becoming a more efficient and more effective regulator under PIPEDA. Returning to the four criteria set out by Bennett and Raab and discussed in Part 2, these potential enhancements are apparent.

1) **Economy** - (e.g. the cost associated with setting up a regulatory regime). The shift to a hybrid model may well reduce the need for the existing separation of OPC operations into discrete PIPEDA and *Privacy Act* spheres. There may be a range of additional expenses associated with a hybrid model, but as a general approach, there is no clear justification for why either the budget or staffing of the OPC would need to change in any significant way if a hybrid model were adopted.

2) **Efficiency** (e.g. the cost of the regime measured against its results). The shift to a hybrid model would likely lead to greater efficiencies, particularly with respect to the small and medium sized business sectors. The combination of greater penetration in the sectors that are typically more sensitive to financial risk and penalties, and the deterrent effect of avoiding regulatory intervention, is likely to lead to more significant results for the same investment of effort and resources. Further, this model would address the current situation, where litigating a matter in Federal Court represents the only, and unfortunately inefficient, means by which the OPC now may have an order enforced.

3) **Effectiveness** (e.g. the extent to which the practical results of the regime fulfil its ultimate aims) The OPC and CIPPIC studies discussed in Part

2 show that non-compliance remains high. The shift to a hybrid model is likely to increase levels of compliance, particularly in the small and medium sized business sectors (effectiveness is impossible to measure without specific benchmarks and targets).

4) **Equity** (e.g. the extent to which the regime extends protection equitably across social groups). While consumers appear to enjoy greater protection as a result of the OPC's activities if they are customers of banks or insurance companies, social media or mainstream media, there is significantly less protection for consumers of small and medium sized businesses. A shift to a hybrid model would enhance equity and ensure consumer protection was not as dependent on the size and sophistication of the business as is the case now.

There is a compelling case for a limited enhancement to the OPC's regulatory powers, at least to include the power to levy fines for non-compliance.

- **Recommendation #4: Granting explicit guideline-making power**

Clear guidelines for the use of this order-making power, and safeguards to ensure fairness to those subject to it, will be essential accountability tools, and in our view, ought to accompany the additional regulatory authority. The development of guidelines also provides an opportunity for consultation with stakeholders, a scan of best practices among peer regulators and a context in which the OPC's values can be communicated clearly to those subject to PIPEDA.

- **Recommendation #5: Exploring other creative regulatory powers — Certification program**

The OPC could offer a certification program whereby the imprimatur of the OPC could be given to companies adopting "best practices," much like LEED certification can be earned by buildings with environmental best practices. Such certification or rating systems could then be used by municipal and provincial governments for other regulatory purposes or by companies for commercial benefit (e.g. as part of an advertising strategy). A related initiative could involve the creation of notices to the public about whether a company or business meets a set of standards, akin to the health inspection notices which are posted in restaurants and inform the public as to whether the establishment has "passed" or "failed" an inspection. These certification or standard setting initiatives rarely are successful on their own. Rather, their success depends on other regulators and industries to create the incentive for businesses to make the additional investment in compliance. For example, if a government, agency or large corporation agreed to limit its procurement to companies with a particular privacy rating, or if particular government permits or grants were tied to a particular privacy rating, this could create effective incentives.

While we are not suggesting that the OPC should be certifying, inspecting or imposing labels on the entire private sector, a pilot initiative in a particular industry with low compliance or where vulnerable members of the public

are particularly at risk (e.g. youth who share their personal information on-line) might well demonstrate whether this regulatory strategy is efficient and effective. Creating incentives and internal markets for higher compliance with PIPEDA is one example of an initiative consistent with the Ombuds model, with potential for raising compliance under PIPEDA, but which requires a proactive approach to the OPC's mandate.

- **Recommendation #6: Improving accountability mechanisms to ensure longer-term strategic planning and meaningful benchmarks**

The OPC is already using a number of accountability mechanisms that are helpful, but their impact is limited. What is lacking in the current accountability structure is a sense of longer-term strategic planning and meaningful benchmarks. While the OPC is hardly under-scrutinized, it is often difficult to discern the criteria by which the various reviews assess the OPC. More troubling, it is not clear by what standards the OPC evaluates its own performance. While the OPC collects data and notes trends in its activities, or the level of complaints or resolutions, the OPC has not identified benchmarks or targets by which its activities might be assessed. The FTC provides a helpful model in this regard. As we discuss in Part 2, the FTC publishes a five year strategic plan which highlights a number of overall goals (e.g. protect consumers), with each goal then including a set of objectives tied to performance measures, strategies to achieve the goal and method of evaluation.

Our final recommendation is that the OPC adopt a clearer strategic planning approach in relation to its activities under PIPEDA, involving:

- The establishment of benchmarks for compliance with PIPEDA;
- Monitoring and tracking compliance on an ongoing basis, at least in target or priority sectors such as small and medium sized businesses;
- Performance evaluation measures for OPC activities in this regard; and
- Short, medium and long-term strategic planning with established targets with specific timelines.

Context

To repeat, our research mandate was concerned with the functions and powers of the Ombudsman as set forth in PIPEDA. It did not extend to offering criticism of the scope and limitations of the principles of the Model Code for the Protection of Personal Information (Schedule 1 to PIPEDA). The limited nature of our study thus excludes certain fundamental issues, such as the transition from Web 1.0 to Web 2.0, which some specialists see as calling into question certain assumptions underlying the principles developed in the 1990s, which were approved by Parliament early in the new millennium and adopted in PIPEDA.

Nearly 10 years have passed since PIPEDA came into force. In that short span of time, major upheavals have occurred with the advent of Web 2.0. These changes have and will continue to have important, even radical, repercussions for the way that personal information is accessed, handled and used. Therefore,

all future considerations providing for the protection of personal information used by private-sector industries, especially in the course of electronic exchange and commerce, will have to incorporate these new dimensions. When reading the conclusions and recommendations of our study, then, account must be taken of the substantial limitations on our research mandate. For in 2010, it is quite clear that the public authorities will have to take this new technological environment into consideration when, as part of the upcoming PIPEDA review process, they are asked to evaluate whether the powers and functions of the Privacy Commissioner are appropriate for regulating the use, collection and retention of personal information by the private sector in the Web 2.0 environment.

That being said, PIPEDA seems to have had a positive impact over the 10 years of its existence. The recourse to the offices of an ombudsman – instead of an administrative tribunal, for example – has made possible significant advances in the education of the private actors subject to the Act. In spite of the many pitfalls created by the economic and political ideas in vogue in the 1990s, ideas that favoured a far more minimalist approach to government intervention in the marketplace and therefore imposed substantial legal constraints, recourse to the Ombuds institution has in the end yielded positive results. Indeed, it seems to have created greater awareness among private actors (natural and legal persons) of the importance of protecting the personal information of individuals and of implementing that protection internally in a more consistent and uniform manner.

However, does that institution have the tools it needs to intervene effectively in the modern-day context? Obviously, the answer to that question will vary according to normative perspective of the party concerned. But if changing the powers and functions of the Office of the Privacy Commissioner were to be an option, it would clearly be necessary to have a good understanding beforehand of the factual context but also of contemporary economic, political and legal discourse. On that subject, even though certain obstacles have been addressed, permitting the potential assignment of additional powers to the Office, the Ombuds institution is not a bottomless receptacle: one cannot pour everything into it without totally altering its nature. As a result, beyond assigning certain powers and functions specific to the institution of Ombudsman, it might be preferable to create another type of public agency, especially if the purpose of assigning other powers is to permit the exercise of constraints upon private actors. On this point, we have seen that when it comes to regulating the activities of civil society (of a class of individuals or industries), Canadian legislators normally prefer to create a decentralized organization, which may be an administrative tribunal (exercising decision-making functions only), or an economic regulatory agency (exercising economic or social regulatory functions, administrative functions and decision-making functions). In the past, it is the latter option that Parliament has used to regulate commercial activities.

It must be noted, however, that decentralized organizations have traditionally exercised oversight that is limited to a few very specific, targeted — rather than general — activities (hence the specialized character of these organizations). For the application of regulations of general scope, such as regulations on the

protection of personal information, one can question the feasibility of assigning general powers of constraint to a federal decentralized organization. At the very least, it would be necessary to carry out an analysis of costs, of advantages and disadvantages, and of the legal limitations of such an approach.

Challenges

Before commencing a legislative reform initiative in this vast field of privacy protection, there are many challenges to be met. They all relate to a better understanding of contemporary issues and to the interaction of the various factors underlying those issues. To cite the principal ones, the main stakeholders need to have common knowledge and understanding of the links between development of the knowledge-based economy and the protection of personal information, so that they can:

- better understand the scope and limitations of the guiding principles in the new technological environment of Web 2.0
    - should all or some of the corporate social obligations in this area be strengthened, modified or eliminated?

- better assess the risks of this new environment and better understand the needs of citizens and consumers in the area of privacy protection
    - are major generational changes observable in terms of general attitude toward expectations of privacy protection? If so, what is their nature and how are they affecting the underlying assumptions of PIPEDA?

- create methodological tools in order to better understand and evaluate national (federal and provincial) and supranational normative systems.
    - what are the strengths and weaknesses of these systems – not individually, but in relation to each other? Is it possible or desirable to make them more harmonious? If so, how?

Here we are only raising a few of the questions that seem to us central for future discussion. The responses to these questions will have repercussions for the assignment of powers and functions to the public institution that will be charged with implementation of PIPEDA. These few thoughts are enough to suggest that what is needed is an in-depth preliminary study involving wide-ranging consultation of all the stakeholders. In terms of public governance, the point is to ensure that all the stakeholders share a better understanding of the current issues – in short, to establish a broader consensus on the definition of those issues, for from them will follow clearer avenues of action for identifying solutions as to the instruments of administrative action, as well as the functions and powers assigned to the institution charged with enforcing the Act.

Strengths and weaknesses

Our review of the literature has allowed us to identify the following main strengths and weaknesses of PIPEDA.

The strengths identified relate to the assignment of powers for public education, research, investigations and audits. Many stakeholders consider the powers of investigation and audit to be among the most important functions that a privacy commissioner can perform. The main advantage is that the commissioner can use them to promote self-regulation by the actors subject to the Act. The main weaknesses identified by critics concerned matters of form (the consultative process), and of substance (choice of the ombudsman model rather than the administrative tribunal, the absence of order-making power, non-disclosure of results from investigations of complaints, and access to the Federal Court).

- **Consultative process**

When the policy was being developed and the bill studied, the critics argued that there had been too little public discussion to reach a broader consensus on the powers that ought to be assigned to the Privacy Commissioner. Many felt that the views of private business had dominated the debates, and hence the choice of public policies. And indeed, the review of the available literature shows that the concerns of citizens, especially from the perspective of consumer protection, were not well represented in the debates at the time, which is paradoxical given that the issue of those debates was the fundamental one of protection of personal information. And so the feeling emerged among critics that privacy protection was a background element of the bill, which was primarily intended as an instrument for promoting electronic commerce. In their view, the government (when developing the policy) and Parliament (when studying the bill) laid down certain principles from which they did not depart. One of the main principles to be remembered was that it was necessary to provide the public authority that would be charged with enforcing the Act with policy instruments that were as light, simple, flexible, efficacious and effective as possible.

- **The substantive issues**

Because the consultative process was inadequate, the critics feel that there was no real debate on the substantive issues, i.e. whether a power to issue binding judgments without appeal ought to be assigned to the public authority, and if so, whether a specialized tribunal should be created. Certain stakeholders felt that the commissioner's powers as Ombudsman were insufficient to guarantee effective implementation of the Act. A review of the parliamentary debates in fact shows that few dissenting voices were heard on the subject. The privacy commissioner of the time featured prominently in those debates, even though he was strongly opposed to any discussion of assigning binding powers to his Office. He preferred to function like a mediator and use his powers of persuasion and negotiation to settle complaints out of court. He also felt that the proper approach to problems of privacy protection was a process of education, discussion and examination of the information management system

of the company targeted by an individual's complaint, so that it was possible to identify its flaws and make systemic corrections to them.

After the passage of PIPEDA, the criticism of the effects of these legislative choices became more specific. Below is a very brief summary of three criticisms put forward by various authors concerning the Ombudsman's powers and functions and the Privacy Commissioner's responses to those criticisms.

1. The Ombuds model compared with the administrative tribunal — Criticism of the complaint resolution system

Authors' criticism: Doubt is cast on the effectiveness of the complaint resolution mechanism. It is felt that the costs involved, the delays and the uncertainty generated by this mechanism have become decisive considerations for parties wishing to file a complaint. One of the problems believed to be responsible for this ineffectiveness is that the Office of the Privacy Commissioner releases only brief summaries of its investigations. This is considered to have the effect of preventing complaints from being used as precedents, and hence as effective means of providing future information and guidance to parties.

Commissioner's response: The Office of the Privacy Commissioner is not an administrative tribunal, and therefore should not be assessed against the criteria of an administrative tribunal. The Privacy Commissioner acts as a neutral third party who has the mandate to communicate openly with both parties involved in a matter. The Commissioner has to work actively with the parties to settle the dispute and reach a fair solution. Her role is also educational, since she must endeavour to influence the privacy culture within a company not acting in compliance with the Act. The complaints-based model gives individuals the opportunity to be active in protecting their personal information and allows companies to be conscious of the practices they use to manage the personal information they hold. The Commissioner adds that it must not be forgotten that she can always take the initiative of filing a complaint under the Act when there are reasonable grounds to do so. Lastly, she considers that her vast powers of investigation constitute a kind of counterweight to the absence of an order-making power. During an investigation, the Commissioner's role is to gather all the facts and all of the necessary and useful considerations to find a lasting solution. The solutions that emerge are helpful not only in resolving the immediate complaint, but also in encouraging systemic changes toward a sustainable culture of respect for privacy. In her opinion, the adversarial process that would be imposed if she had order-making power would not necessarily allow her to resolve disputes in a more effective manner.

2. Disclosure of results of complaint investigations and openness

Authors' criticism: There is a lack of openness regarding the Commissioner's initiatives for ensuring compliance with the Act, and in particular the refusal to disclose the names of companies against which complaints have been filed. As there are no consequences to any finding of non-compliance, there is insufficient incentive to encourage companies in default to change their

behaviour. Furthermore, this lack of openness deprives the public and other companies of very useful knowledge about any best practices proposed by the Office to the company targeted by an individual's complaint. Finally, the lack of openness also makes it difficult to evaluate whether the regulatory system is functioning properly.

Commissioner's response: The nature and purpose of the Ombudsman institution is incompatible with the idea that the Commissioner should disclose more information on the processing and outcome of complaints with a view to establishing precedents. The Ombuds model is not intended to create normative precedents that would be binding on parties in similar situations in future. The parties involved in a complaint must be able to participate in the process in the knowledge that their personal situations will be taken into account, while remaining confident that they can play a role in negotiation of the solution to be adopted. If the parties knew from the outset that a predetermined solution would be imposed on them, the conciliation process would fail. While remaining ever conscious of her obligation of confidentiality, the Commissioner, on the other hand, has to the power to disclose the details of a complaint if those details are of public interest, as set forth in subsection 20(2) of PIPEDA.

3. Access to the Federal Court

Authors' criticism: The accessibility of recourse to the Federal Court must be placed in doubt in light of the costs generated by that procedure (over and above the costs of complaining to the Office of the Privacy Commissioner). The two-step process is long and expensive: it is liable to discourage complaints and to reduce the number of cases which might be heard by the Federal Court, permitting it to interpret the Act and so further develop the case law on the principles that underlie protection of personal information. These costs must also take into account the uncertainty created by the Federal Court procedure. On the one hand, until certain interpretation issues are addressed by the Federal Court or the Federal Court of Appeal, complainants are not in a position to assess their complaints' chances of success. On the other, the Commissioner cannot be certain that she has adopted the correct normative approach to settle a case, and this may create confusion among companies as to the nature and extent of their protection obligations. The authors furthermore underscore the Court's lack of expertise in privacy matters, as a result of which it is not the best forum for settling this type of dispute. Lastly, the authors feel that if the Federal Court were responsible for defining the provisions of the Act, the Commissioner's role would be marginal in spite of her expertise in privacy protection. In fact, the Court's decisions might also have the effect of undermining the Commissioner's authority with private companies.

Commissioner's response: Complainants are not seriously disadvantaged by the intervention of the Federal Court. To claim that they are is to overlook the fact that the Commissioner is able to refer a case to the Federal Court, either directly or on behalf of the complainant. Furthermore, since the Commissioner has no binding decision-making powers, she has a great deal of latitude to assist and advise complainants who wish to refer their complaint directly to the Court. The Ombudsman was chosen as the model for application of PIPEDA

with the intention of avoiding whenever possible the need to apply to a court, and hence of being able to propose reparation in an informal and inexpensive manner. In this way it is possible for the Commissioner to reach an out-of-court solution that is effective and satisfactory to the parties, thus reducing the burden on complainants.

*
* *

We have thus conducted our research and analyses upstream and downstream of passage and implementation of the Act within this general context of certain recurring criticisms of the Ombuds model and of the powers and functions that follow from it.

Specific conclusions and recommendations

In Part I we analyzed the economic, political and legal ideas that dominated the discourse underlying development of PIPEDA, as well as the ideas emerging in the contemporary context, so as to highlight as clearly as possible the points of convergence and divergence between the principal elements of that past and current discourse.

The economic discourse

- It continues to favour the imposition of a minimum of constraints on companies, with the aim of guaranteeing access to national and international markets.
    - However, reflection on the role of social regulations (the category into which PIPEDA falls) has progressed toward greater sensitivity to consumer protection.
    - The State's objective of protecting its citizens (consumers) against abuses of corporate power is seen as a contemporary role that is entirely legitimate.

- The idea of consumer protection must be thought out at the domestic level but also the international level, since States are obliged to harmonize their social regulations so far as possible, so as to guarantee effective protection against inter-State exchanges of information.

- The latter objective is the more important in that the technological developments of Web 2.0 indicate a looming need for this sort of harmonization: to be effective, the Act must take its place within a network of standards. The idea of consolidating the integrity system at the national and international levels assumes its full significance when these new technological developments are taken into account. In this regard, additional targeted research concerning the impact of these technological changes on the capacity of public agencies to implement their privacy protection mission is essential for assessing the effectiveness of PIPEDA.

The political/administrative discourse

- Although there have been no radical changes in political/administrative discourse on the organization and powers of public agencies charged with implementing legislation, the dogmatism of the ideas prevalent in the 1980s which actively opposed the setting up of new public agencies seems to have softened. This is especially true when one goes down the list of parliamentary agencies providing oversight of the administration's activities that were created to consolidate our national integrity system. One can in fact see a real enthusiasm for these oversight agencies among politicians over the last four years.
    - o It would be helpful to better understand the foundations and jurisdictional limitations that may be assigned to this type of organization, especially when they are required to take action in the private sector. Such reflection would be particularly relevant if Parliament were to contemplate adding new powers (e.g. regulatory and criminal) to the Office of the Privacy Commissioner, powers not normally associated with those of an ombudsman, whether that ombudsman reports to Parliament or not.

- Finally, it would seem that replacing the Office of the Privacy Commissioner with an agency in the decentralized organizations category, and more specifically, a social regulatory agency ('social' and not 'economic', since PIPEDA is social and not economic regulation) endowed with administrative powers (e.g. power of investigation), decision-making powers (e.g. power to issue orders and impose penalties) and regulatory powers, is an option which could be considered.

The legal context

- It should be noted that the right to privacy has reached quasi-constitutional status. This status would favour the implementation of better privacy protection to citizens and consumers.
    - o It should also be noted that preserving individual autonomy and the ability to decide for oneself as to the use of one's personal information is of importance. Do individuals want more protection? Are distinct generational trends at play? Should the OPC be conceived as a place where the public is educated but also where one learns from the public? In that regard, would it be appropriate for the OPC to receive the necessary funding (and authority) to hold regular public forums with the intent of better understanding the expectations of the general public, as well as those of industry and interest groups?

- It should be noted that construction of the Global Administrative Law on privacy protection has been ongoing for more than 20 years. It is continuing and becoming more complex. There are a number of initiatives in this respect: the Spanish initiative and the Galway project, with the goal of harmonization; the GPEN, aimed at improving enforcement of standards; the World Anti-Doping Agency's initiative regarding privacy protection for athletes; and, lastly, APEC's normative framework with

its Pathfinder projects and Cross-Border Privacy Rules system. All these initiatives provide a wealth of lessons to consider when assessing reform options.
  - Additional research will be necessary to better identify and understand the strengths and weaknesses of our Canadian system for protecting information relative to this network of standards that is part of Global Administrative Law.
  - It might also be useful to consider assigning powers to the Office of the Privacy Commissioner so that it can clearly participate in debates at the supranational level, and possibly even form a cooperation committee (composed of the federal commissioner and provincial commissioners, federal and provincial public servants, representatives of small, medium-sized and large industries, representatives of interest groups (especially in consumer protection) and citizens' representatives. In a way, this would be like creating a Canadian delegation (in the form of an advisory board) with sufficient authority to discuss privacy issues and intervene on the creation of global administrative law standards and mechanisms in this area.

- It should be noted that the constitutional problems raised by the passage of PIPEDA in 2000 have still not been resolved. Any consideration of granting the Commissioner order-making powers that could be applicable to all Canadian businesses would generate stormy federal-provincial debate. It will be necessary to monitor the debates in the courts of law, particularly debate on the validity of harmonization processes. On this point, the reference to the Supreme Court regarding the establishment of a federal regulatory agency for securities should be monitored. The Court's reasons could support a more functional interpretation of the division of legislative powers, paving the way for implementation of a form of networked federalism including all the entities of the federation (federal, provincial and municipal). For example, a functional interpretation could lead the entities of the federation to reach one or more federal-provincial (and municipal) agreements to ensure better enforcement of the legislation in view of contemporary problems. It would also be worthwhile to look into the possibility of establishing a federal secretariat, within the OPC, with the function of coordinating reflection and research at all levels of government (including municipal governments). These activities would be focused on reform, with the objectives of supplying the necessary analyses and data to find the best administrative practices and solutions for addressing the issues raised by today's new uses of information technologies.

- Regarding the possible assignment of criminal powers, it should be noted that, for the moment within the federal government, it appears that only the CRTC (an economic regulatory agency) has such powers.
  - In Quebec, the Human Rights Tribunal can assess punitive damages to natural and legal persons who knowingly violate the Charter of Human Rights and Freedoms. It is useful to note here that the Human Rights Tribunal considers the infringement of rights of a quasi-constitutional nature. Since it is likely that privacy protection has acquired this same

legal status, certain analogies could be made to justify the assignment of such powers to the Office of the Privacy Commissioner.

In Part II, we have explored in greater detail the operational environment of the OPC in relation to PIPEDA. In order to highlight appropriate evaluative criteria, we analysed empirical, comparative and normative perspectives on the OPC's Ombuds model.

- **From an empirical perspective**
  - A review of data on the OPC's outputs alone is unsatisfactory. Whether the number of inquiries or complaints has gone up or down does not disclose whether the OPC's model for assuring compliance with PIPEDA is successful.
    - The data alone can support any number of arguments about the OPC's effectiveness or ineffectiveness. The qualitative data about stakeholder and academic assessments of the OPC enriches the quantitative data.
    - Especially striking is the widely shared perception that the OPC's model is far more effective in established industries such as banking and insurance, than in the small business context, where personal information is likely to be most vulnerable.

- **From a comparative perspective**
  - The evaluation of PIPEDA and the OPC to date may be enhanced by incorporating the lessons learned from other Canadian jurisdictions (notably Quebec, Alberta and B.C.), as well as in the U.S. and U.K.
  - From other Canadian jurisdictions, for example, we noted that the Quebec experience highlights that independence and impartiality, as core administrative law norms, provide the backdrop against which institutional design and the search for the optimal model take place. The Alberta and B.C. examples demonstrate that an Ombuds model may coexist with and complement a range of enforcement and compliance measures, including order-making powers.
  - U.S. examples such as the FCC and the FTC reflect the move away from ad-hoc, politicized regulation toward evidence-based, strategic regulation. This approach to regulation emphasizes planning, benchmarks and performance evaluation.
  - From Europe, we observed that cooperative legalism represents a helpful framework to understand how a greater role for the state and a greater role for the market may be complementary aims for a privacy regulator. The European example, like that of other Canadian privacy regulators, suggests a complex and complementary mix between Ombuds and order making models.

- **From a normative perspective**
  - Any choice of evaluative criteria is an expression of particular values. For example, Bennett and Raab's prioritizing of economy, efficiency, effectiveness and equity, which resonate in the privacy sphere, suggest that measuring distributive justice in privacy regulation (who has

more of their data protected than others?) is as important as ensuring compliance by industry.

Whether viewed from an empirical, comparative or normative point of view, there is a basis both to confirm that the OPC's Ombuds model is a success, which has had a concrete and significant impact on the goals set out in PIPEDA, and to suggest that the OPC remains constrained from fulfilling its mandate under PIPEDA. There is strong support, for example, for the argument that a shift toward a consumer protection orientation of PIPEDA, or a push to ensure small business compliance with PIPEDA, requires greater order making power to complement the existing Ombuds responsibilities.

RESEARCH REPORT

GENERAL INTRODUCTION

Evaluating the effectiveness of legislation passed by our elected officials is a growing concern for countries around the world. Over the past 30 years, Canada, the United States, Australia, New Zealand and the member states of the European Union, including England, (just to name a few) have allocated considerable human and financial resources to the implementation of such evaluations. Now better known as "smart regulation" in Canada and the United States, "better regulation" in England and "quality regulation" in the European Union, this widespread initiative has affected the design of regulatory systems as well as the development and implementation of the regulations prescribed by these states. For the Canadian federal government, this initiative has taken a more structured and more definitive form with the approval by Cabinet of the *Directive on Streamlining Regulation*.[1]

This initiative to streamline regulation involves an ongoing evaluation process extending from the birth to death of statutes and regulations prescribed by public authorities. Many laws enacted in the last 10 to 15 years frequently contain clauses requiring a five-year review. This review is intended to verify whether, and to what extent, the legislative objectives were achieved, and if they were not, whether it would be desirable to amend the legislation to realize this goal.

1 In Canada, the concept of smart regulation was formally adopted by the federal Cabinet in 2007: CANADA, GOVERNMENT OF CANADA, *Cabinet Directive on Streamlining Regulation* (Ottawa: Her Majesty the Queen in Right of Canada, 2007), 14 p. The Directive is available in electronic format on the Government of Canada website at http://www.tbs-sct.gc.ca/ri-qr/directive/directive00-eng.asp (last visit: August 23, 2008). This directive came into force on April 1, 2007.

Such a provision was included in Part I of the *Personal Information Protection and Electronic Documents Act*[2] (PIPEDA). The first review was conducted in 2006; the second will be done in 2011. It is in preparation for this second review that we were asked to prepare this research report. The specific project that we were assigned was to evaluate the effectiveness of the Ombuds institution as the administrative authority in charge of the implementation of PIPEDA. The general question we were asked is this: Is this model able to protect the personal information of individuals that is held by the private sector? Does it have sufficient and appropriate powers to meet today's challenges in Canada, and internationally?

To answer these questions, we have conducted an evaluation to measure the successes and failures in the enforcement of the Act. However, our mandate is not concerned with quantitative measurement of those successes and failures (measuring *efficiency*), but rather qualitative evaluation (which can be a study of *efficacy* or *effectiveness*). Before further explaining the terms of this mandate, we first wish to clarify what is meant by *efficiency,* differentiating it from the concept of *efficacy* and *effectiveness*.

- ***Analytic framework***

The concept of efficiency derives from economics.[3] A system is described as economically efficient when "[*translation*] allocation and use of rare resources among the various producers result in the production of a group of goods such that there are no other groups containing more than each of the goods produced".[4] The general idea behind the concept of efficiency is that nothing more can be produced given the resources available (the system will then be said to be optimal). An economic system is considered more efficient than another if it can provide society with goods and services without using more resources in terms of labour and capital.

Efficacy and effectiveness, on the other hand, are two concepts that belong to the sociology of law.[5] Efficacy is a concept that evaluates the *implementation* of legal standards. A law is described as effective when it achieves the effect desired (intended or sought) by the legislature. At the very least, it must be an effect that is in the direction desired by the legislature and not in contradiction

2 *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5, s. 29(1)).

3 Claude JESSUA, Christian LABROUSSE and Daniel VITRY (eds.), *Dictionnaire des sciences économiques* (Paris: PUF, 2001), p. 345. In this dictionary, the authors use the term *efficacité* [efficacy] rather than *efficience* [efficiency]. In the present report, however, we will be using the term economic efficiency to avoid confusion between the concepts used in the two disciplines.

4 *Id.*, p. 345.

5 Pierre LASCOUMES and Évelyne SERVERIN, "Théories et pratiques de l'effectivité du droit," (1986) 2 *Droit et Soc.* 101.

with that direction.[6] In its primary sense, the efficacy of law designates the measure, in terms of distance, between the legal standard and the behaviour it is supposed to govern.[7] In short, efficacy studies look only downstream from the law. That is why this type of evaluation is criticized by certain researchers as being too reductive, and why they have replaced it with the broader concept of effectiveness.[8]

Like efficacy, effectiveness also evaluates legal standards, looking not only at their implementation, but also how they are produced and adopted by social stakeholders. To better capture the richness of a legal framework in all of its physical and temporal dimensions, effectiveness studies serve to evaluate all of the effects liable to be generated by that framework. Effectiveness studies can address all or part of the life cycle of a legal framework, from its emergence to its decline and, ultimately, its demise. So the concept of effectiveness includes that of efficacy, but is not confined to the review of the effects desired, intended or sought by the legislature; it also extends to the other effects of a law. Through this evaluation, researchers examine what is happening upstream and downstream from the law so that they can understand and explain the multiple effects of a law beyond those explicitly contained within it. For example, in the context of PIPEDA, we are interested not only in whether personal information is better protected as a result of this legislation but also what other effects a culture of privacy protection may lead to, such as the development of professionalized privacy officers in corporations, or the enhancement of compliance through information provided at the municipal level to support small business start-ups.

- ***Terms of the mandate***

This brief overview of the three evaluation concepts serves to more clearly define the research mandate that we were assigned. That mandate is indeed to evaluate the effectiveness of PIPEDA. However, it does not involve producing a complete study of PIPEDA's effectiveness, with an analysis of all of the intended and unintended, immediate and deferred, concrete or symbolic effects of the production, adoption and implementation of this Act. Our mandate, rather, is more modest. It has two main components: a study of the desired effectiveness and a study of the observed effectiveness. These two components give rise to the structure of this report.

More specifically, we were first asked to examine the context in which the Act emerged, including the public policies underlying its origin and the history of

6 Guy ROCHER, "L'effectiveness du droit," in Andrée LAJOIE, Roderick A. MACDONALD, Richard JANDA and Guy ROCHER (eds.), *Théories et émergence du droit: pluralisme, surdétermination et effectivité* (Montreal: Éditions Thémis, 1998), p. 133-149.

7 Luzius MADER, *L'évaluation législative. Pour une étude empirique des effets de la législation* (Lausanne: Payot, 1985), p. 57.

8 P. LASCOUMES and É. SERVERIN, *supra,* note 5.

the legal framework to date, as well as the current context. The objective here is to identify the significant changes that have occurred since the Act came into force, which can be used to identify new avenues of research into possible changes to the public policies underlying the Act. Next, we were asked to examine the functions and powers of the Office of the Privacy Commissioner (the Ombudsman) and their use by the commissioners appointed to that public office since the Act was passed. The objective of these analyses is to assess the impact of that model on compliance by the organizations subject to the Act. Finally, we were asked to examine other Canadian and foreign institutional models (also created to regulate use of personal information by private-sector organizations) from a comparative perspective to determine whether there are any practices elsewhere that might be better suited to the current context.

- ***Research limitations***

Two important limitations to this research should be noted from the outset. First, the authors of this report are not specialists in privacy laws. As professors of administrative law, the authors have particular expertise in the regulatory systems, organization and functions and powers of organizations that make up the public administration. Our mandate and our report should be read and considered from this perspective. The Privacy Commissioner has retained our services because her main concern is to determine whether the Ombuds institution is an adequate model for guaranteeing the effective application of PIPEDA. Second, our research mandate was to analyze what Parliament has done (descriptive position) and not what it should have done (normative position) or what it should do (prescriptive position). Furthermore, this is exploratory research, and its main objective is to identify deficiencies in knowledge. Therefore, it is not our role to draw generalizable conclusions, but simply to identify future research proposals and hypotheses as well as avenues of legislative reform.

- ***Plan of the report***

This report is divided into two parts. Part I concerns the effectiveness desired by the various public and social stakeholders involved in developing the new public policy aimed at protecting personal information in the private sector. The discussions that led to the passage of PIPEDA took place in an economic, political and legal context specific to the 1990s. In 2010, that context has changed. To identify the current problems and guide future discussions during the next round of the parliamentary review of the effectiveness of PIPEDA, Part 1 will also look at a few emerging trends in the contemporary context. Part II is an evaluative assessment of the observed effectiveness of the Act. We begin with a description of the choices made by Parliament in PIPEDA and then propose a comparative study of other institutional models in Canada and elsewhere, concluding with a review of certain issues surrounding the evaluation of the Office of the Privacy Commissioner.

PART I: PIPEDA: An act integrated with competition law

The desired effectiveness of a law is traced by analyzing the context in which it emerged to identify the various questions and problems that the legislature had to take into account before the bill could be proposed. We will examine the discourse of public and private actors concerning the economic, political and legal constraints that influenced the directions of the public policy that became PIPEDA. Since desired effectiveness involves events that occurred in the past, the most effective method of analyzing the discourse of the public and private actors who took part in the process is to review the relevant documentation available at that time. However, given that our objective is also to identify avenues of future research concerning PIPEDA, it is also important to determine whether and to what extent the constraints identified during the development of the Act are the same as those that exist today. If they are different, government authorities will have to look at the impact that these new constraints might have on any reform proposals being considered.

Section 1: General context of the emergence of PIPEDA

Although there had been calls since the late 1980s for federal privacy legislation applicable to the private sector,[9] it was not until 1996 that the Minister of Industry Canada promised an umbrella privacy act. In April 1997, the Standing Committee on Human Rights and the Status of Persons with Disabilities tabled a report entitled *Privacy: Where Do We Draw the Line?*[10] The Committee proposed replacing the *Privacy Act* with another statute that would apply to Parliament and all government agencies, as well as to the private sector under federal jurisdiction. In January 1998, the departments of Industry and Justice published a discussion paper entitled *The Protection of Personal Information: Building Canada's Information Economy and Society.*

Apart from these documents, there are very few scholarly articles that specifically discuss the organization and operation of the future legal framework. The available documentation was basically produced by or for the government. At the request of Industry Canada, certain privacy experts produced studies in preparation for the development of a legal framework for the protection of personal information in the private sector. The most influential studies written for the government were those by Lawson[11] and Bennett (particularly the one on mechanisms for implementing the law).[12] But the most

9 Nancy HOLMES, *Canada's Federal Privacy Laws* (Ottawa: Library of Parliament, Parliamentary Information and Research Service, 2008), p. 2.

10 CANADA, PARLIAMENT, STANDING COMMITTEE ON HUMAN RIGHTS AND THE STATUS OF DISABLED PERSONS, *Privacy: Where Do We Draw the Line?* (Ottawa: Supply and Services Canada, 1997).

11 Ian LAWSON, *Privacy and the Information Highway: Regulatory Options for Canada* (Ottawa: Industry Canada, 1996).

12 Colin BENNETT, *Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector* (Ottawa: Industry Canada, 1996).

important document is the discussion paper prepared at the request of Industry Canada and Justice Canada by the Task Force on Electronic Commerce.[13] The government solicited comments on this discussion paper through a notice published in the Canada Gazette. Briefs had to be submitted by March 27, 1998.[14]

In short, discussions regarding a future public policy on protection of personal information in the private sector began about 20 years ago in Canada. At that time, i.e. around the end of the 1980s,[15] three main factors had a fundamental impact on the Government of Canada's public policy statement, which was used to develop the future Bill.

First of all, the huge economic potential of the Internet was opening a new chapter in global economic history: the information age and knowledge-based economy. Given this economic potential, the ramifications of which were only partially known, it was difficult for a government to impose excessive constraints on this new environment if it could not explain the economic justifications for them. Prematurely forceful intervention would have been seen as a risk of damaging the development of Canadian businesses. This concern was part and parcel of the trend of prevailing economic ideas of the time, which will be our first consideration.

These economic ideas had a decisive political influence. While bringing an end to the dominance of the founding notions of the welfare state, the economic theories which were gradually imposed from the 1970s onward also ushered in a new age of public governance. In the early 1980s, regulatory programs were no longer seen as efficient instruments for remedying weaknesses in the market: they were now considered pathogenic in themselves. So creating new regulatory programs had to be avoided as much as possible, but if they were necessary, a new set of values and principles had to be taken into account. This is the second issue we will examine.

Finally, the national and international legal context also had a role in guiding the future Bill in certain directions. Current knowledge of the division of jurisdictions between the federal, provincial and territorial governments argued in favour of prudent intervention by the federal government in the privacy field. Furthermore, a normative approach regarding the protection of personal

---

13 GOVERNMENT OF CANADA, DEPARTMENTS OF INDUSTRY AND JUSTICE, TASK FORCE ON ELECTRONIC COMMERCE, *The Protection of Personal Information: Building Canada's Information Economy and Society* (Distribution Services, Communications Branch, 1998), p. 28.

14 *Canada Gazette*, Part I, Vol. 132, No. 4 — January 24, 1998, Notice No. IPPB-002-98 — Release of public discussion paper on the Protection of Personal Information in the Marketplace.

15 CANADA, PARLIAMENT, HOUSE OF COMMONS, STANDING COMMITTEE ON JUSTICE AND SOLICITOR GENERAL, *Open and Shut: Enhancing the Right to Know and the Right to Privacy; Access and Privacy: The Steps Ahead* (Ottawa: Government of Canada, 1987), p. 57.

information had already emerged both within and outside Canada, and given the new political imperative to coordinate actions and harmonize norms, the pressure for legislation that was compatible with commercial goals was high. This will be our third topic of discussion.

1.1 The economic context: At the crossroads of economic models

A market economy implies private ownership of the means of production and a regulatory system to coordinate the marketplace. The pricing mechanism and the action of competition are the two key elements of the coordination mechanism.[16] Therefore, according to classic economic theory,[17] the State must not intervene directly in the operation of the laws of the marketplace in order to regulate demand.

In the 1930s, Keynes challenged the merits of this idea born of classic economic theory. The Keynesian model, which was applied in western countries including Canada between 1945 and 1974, was, as we know, severely criticized in the wake of the two oil shocks that shook the economy during the 1970s. It was this criticism that marked a return to the foundations of classic economic theory for many researchers, who assembled under the banner of the neoclassical school. These researchers had substantial influence on the economic policies of governments, particularly in the OECD member countries, starting in the 1970s. In Canada, this trend became stronger in the early 1980s, and it still exists today. However, certain positions of the neoclassical theorists concerning limited State intervention in the economy were modified in the early 1990s by the theory of endogenous economic growth. This theory was particularly influential on account of the new challenges posed by the establishment of the knowledge-based economy.

Hence it was at the crossroads of established and emerging trends in economic theory that reflection began on the protection of personal information, especially within the OECD, in Canada, the United States, and the European community. At least three principal economic ideas emerge from the literature. First, it is recognized that tension exists between the free circulation of information and the ownership of personal information. Second, the general rules of competition law seemed ineffective in countering the misuse of personal information. And third, there had to be a balance between open competition and consumer protection in order to encourage the establishment of an environment conducive to technological innovation. So the economic choices that influenced the development of PIPEDA are based on the convergence of ideas about what constituted healthy competition in the course of developing the new knowledge economy.

16 *Dictionnaire des sciences économiques*, *supra*, note 3, p. 544.

17 Adam SMITH, *Inquiry into the Nature and Causes of the Wealth of Nations,* (Edinburgh: A. & C. Black, and W. Tait, 1863); Pierre ROSANVALLON, *Le libéralisme économique: histoire de l'idée de marché* (Paris: Seuil, 1989), p. 237.

1.1.1. Free circulation of information and ownership of personal information

In the early 1950s, the neoclassical school became the main school of thought in the United States. Its influence grew substantially during the 1970s, extending beyond American borders,[18] and it became a central part of the programs of major political parties in the United States, Europe (especially England), Australia, New Zealand and Canada in the early 1980s.

The neoclassical economic model is that of the economy of supply. According to this model, the most effective way to sustain economic growth is to help businesses produce more goods and services, encourage them to enter new markets and remove, as much as possible, the fiscal and regulatory impediments to their development. From this perspective, state intervention is considered legitimate when its objective is to regulate practices that distort the free play of competition. Any regulation of economic practices that was not found to be anti-competitive by competition law was usually strongly contested, as it was considered to be economically inefficient. The theorists felt that such regulation generated high costs, meaning that it did not offer the optimum combination of desired inputs to achieve economic efficiency. This line of thought was decisive in its influence on the implementation of deregulation policies.

In Canada, it was mainly economic regulation that was the target of vigorous attacks by economists and business people. However social regulation, which is the category under which PIPEDA falls (PIPEDA is not designed to erect barriers to market entry, but rather to protect consumers), has not been affected as much by this wave of deregulation as it has in the United States. This is one of the reasons why the creation of this sort of federal public policy could be considered in Canada, while such general legislation has yet to see the light of day in the United States.[19] The question therefore is: what is the economic function of a law such as PIPEDA?

Government documents from the 1990s suggest that the public authorities had a twofold objective in mind: foster the circulation of information, while protecting ownership of consumers' personal information. In the paper produced in 1998 by the Task Force on Electronic Commerce (the "Task Force"), formed jointly by Industry Canada and Justice Canada,[20] these parameters formed the framework for discussions on the contours of the future public policy. On the objective of circulation of information, the paper states: "It also requires […] rules where citizens, institutions and businesses can easily exchange information" and "guard[ing] against the creation of 'data havens' or

18 Bernard GUERRIEN, *L'Économie néo-classique* (Paris: La Découverte, 1989), p. 128.

19 Paul M. SCHWARTZ, "Privacy and Pre-emption," (2009) 118 *Yale L. J.* 902, 912. The author explains that the United States has instead taken a sectoral approach and has not passed general legislation covering the private sector.

20 TASK FORCE ON ELECTRONIC COMMERCE, *supra,* note 13.

barriers to the free flow of information".[21] Regarding the objective of protecting personal information, the paper explains that this involves protecting the "right of individuals to determine when, how and to what extent they will share personal information about themselves with others".[22]

This paper also points out the role of personal information in the economy, noting that it is "creating mounting pressure to collect and use personal information more broadly than ever before". But at the same time, it mentions the need to "create a level playing field where the misuse of personal information cannot result in a competitive advantage."[23]

1.1.2 Misuse of personal information

In another document produced for Industry Canada, lawyer Rick Shields lists the different forms of personal information available to the public and explains how just these sources, together, are fertile ground for private organizations, allowing them to compile personal information on the residents of an area.[24] At the time, it was already well known that certain private companies held huge amounts of personal information on their clients: banks, insurance, telecommunications and transportation companies, etc. Businesses and consumers raised a number of concerns about the potential misuse of this information. One of the fears expressed by businesses was that these information holdings could lead to anti-competitive practices that might encourage, for example, abuse of authority by the private organizations with these databanks containing personal information.

In this context, certain questions were raised about the efficacy of the general rules of competition law in countering such practices. Competition law sets up the basic legal structure whereby behaviours resulting in the creation of market imbalances are prohibited. The competition law of the 1990s was therefore built around such prohibitions, which fell within the sphere of criminal law. As we know, the standard of proof required in criminal law is very high, hence the difficulty of ensuring compliance with that law by economic actors. While this observation was made about numerous sectors of economic activity, the experts found the inadequacies of competition law in regulating the play of open competition in the virtual informational space of electronic commerce to be even more glaring. Unlike the industrial economy, where appropriation of resources and production of goods are dominant, development of the knowledge-based economy is tied to the appropriation of knowledge and

21 *Id.*, p. 2 and 12.

22 *Id.*, p. 5.

23 *Id.*, p. 6.

24 Rick SHIELDS, *Publicly Available Personal Information and Canada's Personal Information Protection and Electronic Documents Act* (Ottawa, October 12, 2000) (document written for McCarthy Tétrault, bearing number DMS-Ottawa #5574162/v.2).

continual innovation. Unlike resources and goods, knowledge is *not rare*. It exists in sufficient quantities (to meet our needs and desires), and one of its characteristics is that it can be shared. As a result, competition for knowledge is very stiff, and this has considerable effect on the efficacy of the prohibitions made by competition law.

This initial observation makes clear the importance of certain regulatory regimes designed to protect very specific economic niches, while affording sufficient legal guarantees to prevent anti-competitive situations and maintain competitive balance in a given economic sector. In a knowledge-based economy, this role is played, for example, by legislation governing protection of intellectual property, copyright and personal information. Such legislation compensates in a way for the inadequacies of competition law in effectively protecting the conditions of the exchange of information commonly used in the knowledge economy. PIPEDA and these other laws were deemed essential for building the basic legal infrastructure for harmonious establishment of the knowledge-based economy.

In short, PIPEDA's regulation of the uses of personal information is to be understood by understanding the limitations of competition law and the additions to the legal infrastructure of competition law that have as their aim the fostering of the growth of the knowledge economy. As many commentators on PIPEDA (and some of its critics) have pointed out, the primary function of PIPEDA is not the protection of citizens' right to privacy. Rather, it is, on the one hand, to regulate commercial conduct to promote the exchange and trading of personal information while preventing abuses detrimental to the exercise of open competition, and on the other hand, to protect consumers while creating a climate of consumer confidence that fosters an environment conducive to technological innovation.

1.1.3 Creation of an environment conducive to technological innovation

Creating an environment that fosters technological innovation was a concern that gradually gained importance starting in the 1990s. Economic theories that argued for state intervention in this area also became more predominant in government discourse during this time. In the 1990s, neoclassical orthodoxy began to give way to the views of theorists defending mixed economy models. These models accept that certain economic sectors may be more or less regulated by the State, depending on the competitive context in which trade is operating. Since electronic commerce was seen by many as the way of the future in terms of trade, the security of transactions was the issue of the day. If Canada wanted to develop these new technologies, then consumers needed to have confidence in these new systems of trade. As the Task Force concludes, "In an environment where over half of Canadians agree that the information highway is reducing the level of privacy in Canada, ensuring consumer confidence is key to securing growth in the Canadian information economy. Legislation that establishes a set of common rules for the protection of personal information

will help to build consumer confidence […]".[25] In this context, social regulation that promotes technological innovation is considered acceptable state action.

Within the general neoclassical economic model, various specific and more interventionist theories — that is, more interventionist than those that flourished in the 1980s — took shape. One of these economic theories concerned endogenous growth. It proposed a mixed economy model with strong emphasis on state interventions in the economy to increase technological innovation (including electronic commerce), thus supporting economic growth. Solow was the first theorist who, in the 1950s, established the importance of technological development as a factor in explaining the sustained economic growth of "The Glorious Thirty." Romer contributed to Solow's theory by demonstrating that technical progress, also known as innovation,[26] constituted an endogenous variable, i.e. it was the result of deliberate actions by economic actors. This theory has had a major impact on the renewal of the role of the State in the economy since the 1990s. Generally speaking, this renewal has facilitated the transition from the paradigm of pathogenic regulation to the paradigm of smart regulation, which we will return to in the next section. For the time being, let it suffice to say that when the government wants to implement the economic model of endogenous growth, it has to assume that the deliberate actions of economic actors — designed in particular to increase technological capital and the store of knowledge — will further the development of the knowledge economy, and hence economic growth.[27]

These economic concerns were very present in the discussions surrounding PIPEDA. The section of the paper prepared by the Task Force explaining why the protection of personal information that existed at the time was no longer adequate states that:

> New technologies, increasing data collection in the private sector, changing market trends and the new global marketplace for electronic commerce are contributing to the increasingly important role of information in the global economy. In the new global economy, information is a valuable commodity that can bring jobs, prosperity, and higher levels of customer service. This, along with a number of other key factors, is creating mounting pressure to collect and use personal information more broadly than ever before.[28]

25 TASK FORCE ON ELECTRONIC COMMERCE, *supra*, note 13, p. 6.

26 On the concept of innovation, see the *Dictionnaire des sciences économiques*, *supra*, note 3, p. 474-476.

27 Pierre-Yves HÉNIN and Pierre RALLE, "Les nouvelles théories de la croissance. Quelques apports pour la politique économique," *Revue économique – Hors série* 82, p. 82-86.

28 TASK FORCE ON ELECTRONIC COMMERCE, *supra*, note 13, p. 6.

Hence, in permitting the exchange and trading of personal information, PIPEDA would occupy a place in Canada's economic strategy in which development of the knowledge-based economy, competitive balance and privacy protection would be designed to be inextricably linked elements of a policy.

1.2 The political context: Impact of theories regarding government organization

Based on the criticisms of regulatory programs by neoclassical economists, a thorough review of the operation and organization of public administration was undertaken by researchers in the economic and administrative sciences who were interested in political science. Starting in the late 1960s, the theorists of the Chicago School, particularly those assembled under the banner of public choice theory,[29] contributed significantly to understanding the process by which the public administration makes its decisions. This work and others led to a fundamental reflection on the organization of administrative institutions. It also inspired the work of theorists in the administrative sciences, who proposed a new management philosophy for governments that they christened the New Public Management.

This philosophy had an impact on the way that administrative organizations function by recommending that public administration adopt the organizational model of the marketplace. In Canada, this model won the support of the federal and provincial governments in the 1980s as a way to modernize their public administration. The influence of these two theoretical trends on the organization and operation of public administration is significant because they led governments to reconsider the relationships between public and private organizations in terms of deciding which government institutions should be created to oversee the application of regulatory programs and the instruments of state intervention.

1.2.1 Choice of government institution

In the government documents concerning the development PIPEDA, there is no mention of discussions on the most appropriate institutional model for guaranteeing the effective application of PIPEDA. The Ombudsman at the time, Privacy Commissioner Phillips, suggested that the Office of the Privacy Commissioner, created under the *Privacy Act*, could be responsible for the implementation of the new law, although his justifications for this decision were not well developed. The absence or quasi-absence of debate about the institution responsible for applying the Act is surprising, since there were many persuasive reasons that could have been raised in favour of this choice.

29 The founding document of public choice theory was written by James M. BUCHANAN and Gordon TULLOCK: *The Calculus of Consent* (Ann Arbor: University of Michigan Press, 1962), p. 361.

The first and most obvious reason had to do with the context of the public finance crisis. In the 1980s, politicians were not inclined to propose the creation of another public agency. The mood was instead to reduce and reorganize the public administration to cut back public spending. However, if the creation of a new regulatory program was on the horizon, a public agency had to be entrusted with its oversight, and that required more public spending. From the standpoint of the politician who has to defend such an initiative, it is easier to conceal the spending by adding another jurisdiction to an existing agency than to create a completely new public agency. As the Privacy Commissioner at the time argued in his brief in response to the paper produced by the Task Force: "Equally important in this approach (extending the jurisdiction of the Commissioner) is the avoidance of proliferating bureaucracies and excessive and unnecessary costs".[30]

In addition to these financial considerations, two other reasons supported the choices that were made at the time PIPEDA was developed. First, important discussions were taking place on such issues as the uniform application of the law and the avoidance of overlap and proliferation of rules of law, especially within the federal system. Commissioner Phillips was mindful of these issues and wrote that the Ombuds model "offers the advantages of sensitivity to particular organizational problems coupled with commitment to uniform application of privacy principles".[31]

Second, another important idea influencing public discourse had to do with criticism of the concept of public interest. Public choice theorists felt that there was really no difference between public interest and private interest, since the public interest was essentially nothing but the aggregate of private interests. From this point of view, the role of the State had to be reconsidered. It was no longer up to the State to manage civil society, instead it had to arbitrate the interests at play and balance public action accordingly. In the 1990s it was relatively easy for a government to adopt this theoretical position because the arbitration role of the State had been recognized by the Supreme Court in 1992 in *Nova Scotia Pharmaceutical Society*.[32] From that perspective, Commissioner Phillips' discourse was also in keeping with the prevailing ideas of the time, since he was arguing that the Ombuds model was adapted to the modern context. By relying on consultation, conciliation and negotiation, the Ombudsman could, among other things, be "cognizant of the complexities of business" and more sensitive to the particular organization problems of the private sector.[33]

30 TASK FORCE ON ELECTRONIC COMMERCE, *supra,* note 13, p. 8.

31 *Ibid*.

32 *R.* v. *Nova Scotia Pharmaceutical Society*, [1992] 2 S.C.R. 606, at p. 42 of the PDF version available at LexUM: http://scc.lexum.umontreal.ca/en/1992/1992rcs2-606/1992rcs2-606.pdf (last visit: July 12, 2009).

33 TASK FORCE ON ELECTRONIC COMMERCE, note 13, p. 8.

It was after reflecting on all of these concerns that some new organizational ideas emerged, including the assigning of crosscutting jurisdictions to certain agencies of the public administration.

1.2.1.1 Assigning crosscutting jurisdictions

Public choice is an economic theory that examines problems that generally fall within the field of political science. It was Niskanen's work in the 1970s that clearly distinguished the study of the behaviour of public servants and the operation of bureaucracy in particular as a specific field of public choice theory.[34] One of the first problems identified by public choice theorists was the compartmentalization of organizations' jurisdictions, which raised questions about the vertical and hierarchical organizational model of public administration. Public choice theorists felt that assigning every government agency a specific and exclusive field of social and economic action did not facilitate communication and coordination among the member organizations of a given public administration (e.g. federal administration) and members of other public administrations (provincial or other states). They argued that this kind of silo organization creates unhealthy competition among state organizations because public administrators tend to create more regulatory standards in order to maximize their budgets and spheres of jurisdiction.

Based on this criticism, there was a prevailing feeling during this time that the public sector was ineffective: public administration was too rigid in the way it operated, too centralized in its organization, too expensive, too focused on its own development and incapable of innovation. The triple-E objective (economy, effectiveness, efficiency) emerged as the new credo of politicians.[35] This mentality led to some new ideas about the foundations of future administrative organizations. Flexibility and more thorough decentralization became key organizational concepts, leading to the proliferation of a new type of organization in the Canadian public administration: the agency. What is interesting about this new type of organization is the relationship between the agency and the Ombudsman, as noted by Daniel Mockle.[36] He explains that the proliferation of this model in contemporary Canadian administrative law is "[*translation*] the structural expression of the requirements of new public management,"[37] since the agency model has at least five characteristics: (1) clear definition of the missions of the agency; (2) broad decentralization of responsibilities and methods; (3) the central role of use; (4) evaluation of the concrete results of the agency's activities; and (5) functions limited to

34 William NISKANEN, *Bureaucracy and Representative Government* (Chicago: Aldine Atherton, 1971), p. 241.

35 Paolo URIO, "La gestion publique au service du marché," in Marc Hufty (ed.), *La pensée comptable: État, néolibéralisme, nouvelle gestion publique* (Paris and Geneva: PUF and Les nouveaux Cahiers de l'IUED, 1998), p. 91–124.

36 Daniel MOCKLE, *La gouvernance, l'État et le droit* (Éd. Bruylant, 2007), p. 233.

37 *Id*., p. 232.

implementation of the law.[38] We would add a sixth characteristic to this list, namely the frequent assignment of crosscutting jurisdictions to these agencies.

Our focus here, of course, is the protection of information in the public sector (*Privacy Act*) and the private sector (PIPEDA). Given that the private sector includes all private organizations under federal, provincial and territorial jurisdiction,[39] it is clear that the field of privacy requires a crosscutting regulatory program. In this context, the central issue is the capacity of a public institution to act as impartially as possible in its obligation to balance the interests of all stakeholders.

1.2.1.2 Balancing the interests of stakeholders

A second problem identified by public choice theorists was the implementation of the principle of the public interest. As previously mentioned, these theorists believed that the idea that public and private interest was distinct was false. They argued that both public and private actors are motivated by the maximization of their personal interests (income, power, altruism, etc.).[40] By showing that the public authorities were acting only to optimize their own well-being, public choice theorists also showed that the general interest was basically nothing but the aggregate of private interests.[41] To prevent these authorities from acting unfairly and prejudicially, the administrative mechanisms that neutralized or inhibited fair and impartial implementation of regulatory programs had to be identified. At least two mechanisms were singled out: (1) the rigidity of the regulations, which had to be replaced by more flexible regulations; and (2) a process that permits greater informational openness, so that all stakeholders are able to present their opinions on the development and application of the legislation. In the discussion paper on electronic commerce, the Task Force emphasizes the adoption of flexible standards to protect personal information: "Canada's new legislation should […] provide light but effective guidance for protecting enforceable rights and a level playing field in the marketplace".[42] Further on, the Task Force recommends the adoption of the standard approved by the Canadian Standards

38 *Id.*, p. 233.

39 *Personal Information Protection and Electronic Documents Act*, *supra*, note 2, s. 23 ff. Refer to CANADA, PRIVACY COMMISSIONER, *Report to Parliament Concerning Substantially Similar Provincial Legislation* (Ottawa: Public Works and Government Services, 2002). This publication is available on the OPC site: www.priv.gc.ca (last visit: July 10, 2009).

40 On this point, these theorists would say that this is why Commissioner Phillips proposed that the Office of the Privacy Commissioner also be responsible for the application of the new legislation.

41 Ejan MACKAAY and Stéphane ROUSSEAU, *Analyse économique du droit,* 2nd ed. (Montreal: Éditions Thémis, 2008), para. 144: "[*translation*] Society's collective choices have to be analyzed as resulting from the composition of individual choices."

42 TASK FORCE ON ELECTRONIC COMMERCE, *supra*, note 13, p. 11.

Association (the CSA Model Code) because it "has a number of advantages as a starting point for legislation", including the fact that it "provides flexibility".[43] The Commissioner did not object to the adoption of this standard, although he did recommend a number of improvements to it.[44]

On the subject of informational openness, public choice theorists believed that the information held by public authorities during decision making was fundamentally biased because the authorities' conception of public interest was based solely on what bureaucrats understood that public interest to be. If the concept of public interest is viewed as constituting an aggregate of private interests, the importance of the public choice theorists' idea to include all stakeholders in discussions on the development and/or implementation of the law is immediately clear. They believed that it was important for appropriate mechanisms to be implemented to fill in the information gaps of public organizations. These mechanisms would serve as a kind of guarantee of greater procedural fairness.

This was a key issue during the development of PIPEDA. Adoption of the Canadian Standards Association's standard was also based on the fact that it "represents a consensus among key stakeholders from the private sector, consumer and other public interest organizations, and some government bodies".[45] It was important for the basic standards applicable to private organizations to reflect their interests. It was also important for the mechanisms for implementing the Act to allow as much informational openness as possible. In this regard, the solution was to promote investigation mechanisms that were broad and comprehensive enough to provide the Commissioner with the maximum relevant information before making recommendations or proceeding with the conciliation or mediation of a consumer complaint. The confidentiality of the investigation process was also considered and subsequently adopted in PIPEDA to promote frank and full discussions between the Commissioner and the private organization involved in the complaint.

1.2.2 Choice of instruments of intervention

According to New Public Management, the public sector shares some common traits with the private sector. Because of these similarities, certain management tools used by the private sector can be used by the public sector. One of these tools is the cost-effectiveness study, which establishes a relationship between the cost and the effectiveness of an instrument of state intervention to determine the tool that is most economically efficient. The 1980s saw new

43 *Id.*, p. 13.

44 Bruce Phillips, Privacy Commissioner of Canada, *Response to the Government of Canada Discussion Paper "The Protection of Personal Information: Building Canada's Information Economy and Society"* (Ottawa: Office of the Privacy Commissioner of Canada, 1998), *supra,* note 30 [hereafter, "Commissioner Phillips' Response].

45 TASK FORCE ON ELECTRONIC COMMERCE, *supra*, note 13, p. 13.

social and economic problems requiring state intervention that called on the State to consider alternatives to the classic regulations.[46] In the 1990s, these alternatives focused on the concept of smart regulation, and further to discussions on the matter, the OECD countries came to an agreement on the objective of producing "better", "quality" or "smart" regulation.[47] Cooperation between the State and its public and private partners is central to the regulatory reform strategy, which is based largely on the harmonization of standards. Accountability implies that the bodies governed by the State may exercise their free will. It is therefore a matter of promoting regulatory approaches that serve to make social and economic actors more accountable.

1.2.2.1 Cooperation between public and private actors

Rethinking the quality of regulations and the management of the regulatory process involves a change in the role of the State. With the end of the age of the welfare state, the State is no longer required to direct the social and economic actors, but rather to facilitate commerce and join forces with its partners in civil society. It is in this context that public actors (national and foreign states) and private actors strive for greater cooperation among themselves.[48] Two objectives are central to this vast initiative: harmonizing standards and changing the organizational culture.

It is because of the globalization of commerce that the harmonization of state and other standards is imperative. It is necessary to avoid the "tyranny of [normative] differences"[49] that imposes barriers on domestic and international trade that are considered unnecessary. Industry put forward an argument that carried a lot of weight with governments: Canadian businesses should be able to access the markets at the lowest cost. It follows that any regulation that imposes requirements on these businesses that are stiffer than those of their competitors has the effect of reducing their competitive capacity. This concern is stated clearly in the paper produced by the Task Force on Electronic Commerce: "The ability to provide effective protection for personal information may be crucial to Canada's ability to remain competitive internationally in the global information

46 Concerning the choice of the State's instruments of intervention, refer to Lester M. SALAMON (ed.), *The Tools of Government: A Guide to the New Governance* (Oxford: Oxford University Press, 2002), p. 669; and Pearl F. ELIADIS, Margaret M. HILL and Michael P. HOWLETT, *Designing Government: from Instruments to Governance* (Montreal: McGill-Queen's University Press, 2005), p. 454.

47 On Canada's adoption of the smart regulation concept, see note 1.

48 QUÉBEC, MINISTÈRE DU CONSEIL EXÉCUTIF, *La Réglementation par objectifs, Propositions du Groupe de travail Justice – Secrétariat à l'allégement réglementaire* (Quebec City: Ministère du Conseil exécutif, 2001), p. 5, accessible online at: http://www.mce.gouv.qc.ca/allegement/documents/reglementation_objectifs.pdf (last visit: July 14, 2009).

49 This expression was used by the External Advisory Committee on Smart Regulation in its document *Smart Regulation: A Regulatory Strategy for Canada, supra*, note 47.

economy".[50] In its *Regulatory Policy, 1992*, the federal government explicitly asks its public administration to prove that " steps have been taken to ensure that the regulatory activity impedes Canada's competitiveness as little as possible " and that the "the regulatory burden on Canadians has been minimized through such methods as cooperation with other governments".[51] From this point forward, strengthening cooperation at the national and international levels by harmonizing standards became a priority for federal administrative management.[52] This requirement is also stated in the paper produced by the Task Force:

> If truly comprehensive privacy protection for all Canadians is to be achieved, then the federal, provincial and territorial governments will have to work closely and cooperatively to ensure a harmonized approach in all jurisdictions. This is vital for interprovincial trade, as well as for international trade.[53]

Commissioner Phillips also agreed with the objective to harmonize standards,[54] and this thinking was supported by other civil society groups as well, such as the Uniform Law Conference of Canada. In fact, the Law Conference had begun thinking about uniform data protection in the private sector as early as 1995[55] and had drafted a bill in 1998.[56] Thus, there was already a strong consensus on this issue when discussions on the development of PIPEDA were taking place.

However, to achieve cooperation through the harmonization of standards, the organizational culture between the public and private actors had to change. An environment had to be created in which there would be a spirit of collaboration between governments, industry, NGOs and citizens concerned or affected by the regulatory measures being considered. Various mechanisms could facilitate dialogue between the political, economic and social stakeholders, including consultation, negotiation, conciliation and mediation. In the paper prepared by the Task Force, the discussion of mechanisms for implementing the

---

50 TASK FORCE ON ELECTRONIC COMMERCE, *supra*, note 13, p. 7.

51 CANADA, TREASURY BOARD SECRETARIAT, *Regulatory Policy* (Ottawa: Treasury Board of Canada, 1992), pp. 4 and 5.

52 In 2007, these requirements would become even more specific and imperative with the *Cabinet Directive on Streamlining Regulation*, *supra*, note 47.

53 TASK FORCE ON ELECTRONIC COMMERCE, *supra*, note 13, p. 12.

54 Commissioner Phillips' Response, *supra*, note 30, p. 13.

55 See the Proceedings of Annual Meetings of the Conference (1995: Quebec City, QC, Appendix M: *Personal Information and the Protection of Privacy*), available at this address: http://www.ulcc.ca/en/poam2/index.cfm?sec=1995&sub=1995ac (last visit: July 13, 2009).

56 See the Proceedings of Annual Meetings of the Conference (1998: Halifax, N.S., #Appendix A: *Uniform Electronic Commerce Act*), available at this address:http://www.ulcc.ca/en/poam2/index.cfm?sec=1998&sub=1998ja (last visit: July 13, 2009).

future law stresses the out-of-court settlement of disputes between consumers and industry.[57] This was also the route preferred by Commissioner Phillips.[58] Although the Task Force left the door open to the possibility of creating an administrative tribunal, this was mentioned only in passing and was not a really important component of the discussions.[59] Commissioner Phillips was silent on the matter, but the mere fact that he felt that his Office should be responsible for the application of the new Act was an implicit rejection of the option of an administrative tribunal. In any case, he wrote that oversight had to be exercised in the least coercive manner possible: "The Privacy Commissioner believes, and has put into practice, the view that the essence of successful oversight is the maximum possible reliance on consultation, conciliation and negotiation, and the absolute minimum necessary resort to coercion and compulsion."[60]

1.2.2.2 Accountability of actors governed by the State

The theme of accountability of economic and social actors derives from a broader consideration on the exercise of state authority and the freedom of citizens, which was launched by Hayek in 1944 with the publication of his seminal work *The Road to Serfdom*.[61] Hayek's central thesis is that socialization of the economy[62] and massive state intervention in the marketplace result in the suppression of individual freedoms. This criticism, which was accepted by public choice theorists, had a major impact on methods of regulating in the eighties and nineties. Based on regulation of means model, states experimented more with alternatives such as regulation of objectives, self-regulation, and even non-regulation. These experiments were carried out primarily in the economic sectors, because this was the industry that criticized the regulation of means, condemning its harmful effects on industry's capacity to make economically efficient decisions, that is, decisions that allowed it to be truly competitive in the marketplace. Industry argued that the lack of flexibility in the regulation of means was detrimental to its competitiveness since it was an obstacle to technological innovation.[63]

Closer to home, Rod MacDonald, then President of the Law Commission of Canada, at a conference in 2000 organized by government legal officers, advocated an approach to public and private governance that was based on respect for individual free will and the search for a new legal balance that gave

57 TASK FORCE ON ELECTRONIC COMMERCE, *supra*, note 13, p. 20.

58 Commissioner Phillips' Response, *supra*, note 30, p. 11.

59 TASK FORCE ON ELECTRONIC COMMERCE, *supra*, note 13, p. 25.

60 Commissioner Phillips' Response, *supra*, note 30, p. 8.

61 Friedrich A. von HAYEK, *The Road to Serfdom* (Chicago: University of Chicago Press, 1962), p. 24-31; First published in 1944.

62 Socialization of the economy is a concept related to the notion of social justice or distributive justice: *Dictionnaire des sciences économiques*, *supra*, note 3, p. 496–498.

63 *La Réglementation par objectifs, supra,* note 48.

citizens maximum freedom of action. He proposed that the State abandon "[*translation*] so far as possible the idea that the law is a mechanism of social control governing a population that is incapable of acting in a fair and just manner toward others in the absence of rigid guidelines (regulatory law)". MacDonald felt that regulatory law had to be replaced by law that facilitates human interaction "and lays guideposts which indicate to us our values and encourage us to respect them".[64]

In this intellectual context, the State now leaned toward flexible regulatory programs ("soft law") rather than rigid ones ("hard law"), where appropriate.[65] As a result, when discussions on the development of PIPEDA began, soft law was already one of the underlying premises of the creation of new public policy. This is why the option of regulating means rather than objectives was not even a topic of discussion in the paper produced by the Task Force on Electronic Commerce. Only the objectives to be achieved by private organizations are discussed in the paper. It also gives broad consideration to self-regulation. The Task Force discusses in detail the content of voluntary standards already approved by the Canadian Standards Association (the CSA Model Code) and the option of allowing each industrial sector to adopt its own sectoral code. When this type of regulation is adopted (regulation by objectives and self-regulation), the public authority responsible for its application is automatically given a wider margin of appraisal as to the scope of the standard and the assessment of compliant and non-compliant behaviours.[66]

1.3 The legal context: Internal and external normative constraints

In proposing to legislate on the protection of personal information, the federal government wanted to address two urgent issues. First, the European Union had adopted a directive enabling it to impose non-tariff barriers on any private organization, of Canadian or any other nationality, whose business involved the exchange of personal information, if the state where the business was located did not have a personal information protection regime in place that was considered adequate by the European Union.[67]

---

64 Roderick A. MACDONALD, "La réforme du droit et ses organismes," in *Actes de la XIVe conférence des juristes de l'État* (Cowansville: Les Éditions Yvon Blais Inc., 2000), p. 377–397.

65 On the transformation of the roles of the State, see: Charles-Albert MORAND, *Le droit néo-moderne des politiques publiques* (Paris: L.G.D.J., 1998), p. 71 ff.

66 *R.* v. *Nova Scotia Pharmaceutical Society*, [1992] 2 S.C.R. 606.

67 THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L 281, 23/11/1995, pp. 31-50. Accessible online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (accessed on May 11, 2010).

To avoid becoming subject to such barriers, Canada had to establish a protection regime, and, to comply with the European requirements, the regime had to include uniform enforcement standards for all bodies exchanging personal information, whether intraprovincially, interprovincially or internationally. The federal government felt that there was not enough time to wait for each of the provinces and territories to act before the European directive would begin affecting trade between Canadian and European companies. It therefore decided to establish a national regime. Second, even if the provinces and territories had acted quickly, there was a concern that they would implement different regimes, and that certain provinces or territories would attempt to carve out a competitive advantage to the detriment of their partners in the Canadian federation. To avoid these undesirable outcomes, the federal government decided to begin developing what eventually became PIPEDA. However, while these objectives were laudable, there remained uncertainty as to the federal government's constitutional authority to legislate in this area.

In fact, both the federal and provincial governments could claim legislative jurisdiction over the protection of personal information under sections 91 and 92 of the *Constitution Act, 1867*.[68] The provincial governments, for example, could rely on their power to legislate with respect to property (personal information) and civil rights (the right to privacy) [s. 92.13] as well as all matters of a merely local or private nature in the province [s. 92.16]; under the latter provision, a provincial legislature "within its own field of legislative power can regulate, in the Province, a particular business or activity."[69] The federal government, on the other hand, could rely on its power to regulate trade and commerce, as set out in s. 91.2. However, this ground was less certain, as the scope and limits of this federal power had yet to be fully defined. The parameters for applying s. 91.2 remained somewhat fluid.

In the third section, we will describe the national and international normative principles that grounded the reflection in the 1990s on what was to become PIPEDA.[70] Then we will explore the state of constitutional law during the period in which discussions were being undertaken to illustrate the parameters within which the federal Parliament had to operate to ensure that the bill would rest on the strongest constitutional foundation possible. Our purpose here is not so much to provide a legal opinion on the division of powers as to point out some of the challenges faced at the time.

68 *Constitution Act, 1867*, 30 & 31 Vict., c. 3 (U.K.).

69 *Canadian Indemnity Co. et al.* v. *Attorney General of British Columbia*, [1977] 2 S.C.R. 504, 512 and 519; *Attorney General (Que.)* v. *Kellogg's Co. of Canada et al*, [1978] 2 S.C.R. 211, 225.

70 TASK FORCE ON ELECTRONIC COMMERCE, *supra*, note 13, p. 8.

1.3.1 The emergence of norms for the protection of personal information

In the early 1980s, the international community became aware of the potential for emerging information and communications technologies to be highly intrusive with respect to individual privacy. This awareness also extended to individuals, who, whether as consumers, clients or patients, began demanding greater respect for their privacy. First the OECD and later the European Union issued directives on the protection of personal information. As we will see in the first stage, these directives had a domino effect, which eventually led to a proposal by the federal government to legislate in this area.

However, Canadian and Quebec businesses had not waited for federal government action, already having implemented systems of standards with varying contents and constraints. The idea of having several regional or sectoral systems was not without its critics. Large federally regulated companies, for example, were likely in favour of adopting national standards. The idea of implementing minimum national standards began to emerge. In the second section, we will briefly describe the standards established by Quebec and the Canadian Standards Association to illustrate the normative differences between the two regimes and the resulting constraints for companies operating in several Canadian provinces, including Quebec.

1.3.1.1 The development of extraterritorial standards

On September 23, 1980, the OECD adopted the first international document on privacy and personal information. The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[71] include recommendations on the broad areas that should be covered by any regulatory privacy protection regime. This directive represented an attempt to reconcile the distinct understandings of the notion of privacy that could be found among the OECD member states.[72] It was designed to promote respect for privacy and awareness of the issues raised by the exchange of individuals' personal information.[73]

The OECD Guidelines are significant because they formed the foundation on which several personal information protection regimes were later built. For instance, Bennett reports that many European states adopted legislation based on the eight principles set out in Part Two of the Annex to the OECD

71 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted September 23, 1980. Accessible online at: http://www.oecd.org/document/57/0,3343, en_2649_34255_1815186_1_1_1_1,00.html (accessed on May 11, 2010).

72 Richard BECKER, "Recent Developments: Transborder Data Flows: Personal Data", (1981) 22 Harv. Int'l. L. J. 241, 246.

73 *Id*., 244.

Guidelines.[74] The eight basic principles are the following: (1) the collection limitation principle; (2) the data quality principle; (3) the purpose specification principle; (4) the use limitation principle; (5) the security safeguards principle; (6) the openness principle; (7) the individual participation principle; and (8) the accountability principle.[75] According to section 6 of the OECD Guidelines, these eight basic principles constitute minimum standards.[76] Moreover, the OECD merely recommended that member states adopt these standards. There were no legal sanctions for failure to comply. The OECD relied on the moral authority of its directives; if a member state refused to comply with the principles or to incorporate them into its domestic law, its reputation would suffer, as would that of its national undertakings. According to Becker, the moral pressure sufficed to encourage members to strive to work together cooperatively.[77] The directives were also used by nationals of member states to pressure their governments to provide adequate protection.

In 1985, the OECD signalled its commitment to protecting personal information by approving the *Declaration on Transborder Data Flows*.[78] The member states declared that, "considering . . . the significant progress that has been achieved in the area of privacy protection at national and international levels", they intended to continue their work in the area of privacy and personal information protection. Thirteen years later, in 1998, the member states reaffirmed their commitment to respecting the guidelines approved in 1980, as well as the *OECD Cryptography Policy Guidelines* (1997) and those included in the *Declaration on the Protection of Privacy on Global Networks*.[79] Despite these statements of intent, the content of the specific obligations imposed on member states remained relatively vague. The one obligation that seemed more restrictive than the others was the commitment by member states to assess their progress within two years of the declaration.[80]

The most important fact that emerges from this brief overview of the OECD's efforts to develop standards for the protection of personal information is that the member states reached a consensus on the eight basic principles contained

74 Colin BENNETT and Charles RAAB, *The Governance of Privacy: Policy Instruments in Global Perspective*, Aldershot, Ashgate, 2003, p. 75.

75 See Annex A for a more detailed description of these principles.

76 *Id.* (Annex A), s. 6.

77 R. BECKER, *supra*, note 72, p. 247.

78 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Declaration on Transborder Data Flows*, April 11, 1985. Accessible online at: http://www.oecd.org/document/32/0,3343,en_2649_34255_1888153_1_1_1_1,00.html (accessed on May 11, 2010).

79 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Declaration on the Protection of Privacy on Global Networks*, October 19, 1998. Accessible online at: http://www.oecd.org/dataoecd/39/13/1840065.pdf (accessed on May 11, 2010).

80 *Id.*, see the last paragraph of the declaration.

in the 1980 guidelines.[81] These principles did not have a direct impact on the Canadian authorities, but they have stimulated discussion among economic, social and political actors.

In 1995, the Canadian authorities began to be subject to real pressure. By signing off on the *Data Protection Directive*,[82] the European Union marked a shift away from the soft law approach. It was this Directive that led the United States to adopt the "safe harbour" rule[83] and the Canadian and Australian governments to legislate on the subject.[84] Most of the standards contained in the Directive apply only to Union member states, creating privacy protection obligations applicable to the exchange of personal information.[85] However, the key article for foreign countries such as Canada is Article 25 of Chapter IV (Transfer of Personal Data to Third Countries), which gives Union member states the power to refuse to exchange data with countries that do not ensure an "adequate" level of protection.[86]

The directive does not specify what constitutes an "adequate level of protection", so to define its scope, the European Commission produced a report in 1998 proposing a methodology for evaluating whether a state has established an adequate level of protection.[87] According to the Commission, to be considered adequate, the regime adopted by a third country must be functionally similar to those in place in Union member states.[88] The Commission also emphasizes that this is not an imposition of European mechanisms, which are not the sole models for the adequate protection of personal information. To the contrary, the Commission has stated that it prefers to avoid normative imperialism. To this end, the Commission specifies that a third country regime will be judged adequate if it effectively provides the same protection as the European regimes.

---

81 C. BENNETT and C. RAAB, *supra*, note 74, p. 74.

82 *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, supra*, note 67.

83 C. BENNETT and C. RAAB, *supra*, note 74, p. 132. The safe harbour rule comprises seven principles related to the protection of personal information. It is a list of voluntary norms developed by the corporate sector. When companies register with the Department of Commerce, they provide the information that they have received about Europeans in order to give them the opportunity to verify the accuracy of the information. They may also seek a remedy in cases where companies violate the principles.

84 C. BENNETT and C. RAAB, *supra*, note 74, p. 166.

85 *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, note 67, art. 34.

86 *Id*., art. 25.1. The text of article 25 is reproduced in Annex B.

87 EUROPEAN COMMISSION, INTERNAL MARKET AND SERVICES DIRECTORATE GENERAL, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data: annex to the annual report 1998 (XV D/5047/98) of the working party established by article 29 of directive 95/46/EC*, Luxembourg: Office for the Official Publications of the European Communities, 1998.

88 *Id*., art. 7.

In other words, a demonstration that the implementation of the principles set out in the Directive has generated the desired results will suffice.[89] The European Union evaluates the effectiveness of the regimes on two levels. Generally, an adequate regime promotes the advancement of knowledge of the basic principles that must underlie the protection of personal information. More specifically, the system must provide a mechanism for the resolution of complaints by individuals who feel that their right to have their personal information protected has been violated.[90] The complaints must also be heard by an independent authority, and appropriate security measures must be implemented to prevent a company from transmitting or providing unwanted access to the personal information it holds on individuals.

1.3.1.2 The development of intraterritorial standards

When the federal government began working on a bill to protect personal information in the private sector, two major initiatives had already been implemented in Canada: one in Quebec and one by the Canadian Standards Association. Thus, in the mid-1990s, there was a sense that a national standard was necessary to avoid having a patchwork of provincial, territorial and even sectoral legislation, which could have created major normative gaps, upsetting the competitive balance between the various economic actors.[91] This was one of the arguments put forward by Mr. Manley when he presented his bill:

> Right now, personal information is a commodity that can be bought, sold and traded. We have, in Canada, what the federal Privacy Commissioner has described as a «patchwork» of laws, regulations and codes. Personal information crosses all boundaries: provincial, territorial and national. Most industries are not subject to any rules concerning the collection, use and disclosure of personal information. Only Quebec has broad legislation for the private sector operating within the province.[92]

89 *Id.*, art. 12. The principles are the following (1) the principle of individual participation; (2) the principle of purpose-specification, (3) the principle of proportionality and (4) the principle of quality.

90 *Id.*, art. 16. More substantively, the Commission recommends in its report that the analysis focus on three facets. An adequate regime must include: (1) an explicit protection mechanism (such as a statute); (2) a monitoring mechanism; (3) a mechanism providing a recourse by which sanctions may be imposed if a violation of the standards governing the protection of personal information is identified.

91 Colin BENNETT, *Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector*, Ottawa, Industry Canada, 1996, p. 6.

92 GOVERNMENT OF CANADA, MINISTER OF INDUSTRY, "Speaking Notes: For the Honourable John Manley, Minister of Industry, Presentation to the Senate Committee Studying Bill C-6", Ottawa, December 2, 1999. Online: http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00217.html (accessed on May 11, 2010).

In this section, we will compare the contents of the *Model Code for the Protection of Personal Information*,[93] approved by the Association in 1996, and *An Act Respecting the Protection of Personal Information in the Private Sector*,[94] passed in 1994 by the Quebec National Assembly, in order to highlight the major disparities that already existed when the federal government set out to create what was to become PIPEDA.

The Model Code was adopted two years after the Province of Quebec passed its own legislation governing all undertakings involved in exchanging personal information. The Quebec act was inspired by articles 35 to 41 of the *Civil Code of Québec*, which set out the principle of respect of privacy. The Model Code and Quebec statute also draw on the 1981 OECD Guidelines. The Model Code is a voluntary code establishing minimum standards for the protection of personal information. The Code sets out ten principles;[95] the Quebec act does not prescribe principles as such, but nevertheless establishes standards related to each of the principles contained in the Model Code. To illustrate the differences between these two normative regimes, we will compare the two texts as they relate to two of the principles set out in the Code.

With respect to the Principle of Accountability (the first principle), the Model Code explains that an organization is responsible for personal information under its control. It must designate an individual or individuals who are accountable for the organization's compliance with the nine other principles in the Model Code. The Quebec act provides that organizations must designate an individual responsible for personal information, even though other individuals in the organization deal with the information.[96] Moreover, the identity of the individual designated must be made available upon request by a member of the public.[97] The Quebec act also provides that the individuals responsible for personal information in an organization must be registered with the government.[98] The obligations in the Quebec act are thus stricter than those in the Model Code with respect to the principle of accountability, facilitating access to the data by the persons concerned.

With respect to the consent of an individual to the collection of personal information (the third principle), the Model Code explains that the individual

93 CANADIAN STANDARDS ASSOCIATION (CSA), *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, Rexdale, CSA, 1996 [hereafter the "Model Code"].

94 *An Act respecting the Protection of personal information in the private sector*, R.S.Q., c. P-39.1 [hereafter the "Quebec act"].

95 (1) Accountability; (2) Identifying Purposes; (3) Consent; (4) Limiting Collection; (5) Limiting Use, Disclosure, and Retention; (6) Accuracy; (7) Safeguards; (8) Openness; (9) Individual Access and (10) Challenging Compliance.

96 Model Code, *supra*, note 93, s. 4.1.1.

97 *Id.*, s. 4.1.2.

98 Quebec act, *supra*, note 94, s. 70.

must be informed of the use that will be made of his or her personal information. The individual must also consent thereto, unless this is not possible. The Model Code suggests that it is also possible to obtain implied consent.[99] Several sections of the Quebec act relate to consent. While the Model Code seems more focused on the methods used to collect personal information,[100] sections 6 and 9 of the Quebec act establish an obligation to obtain the valid consent of an individual before collecting his or her personal information. Section 13 of the Quebec act provides that personal information cannot be transmitted to a third party without the valid consent of the person in question. Thus there is a notable difference between the Model Code and the Quebec act when it comes to the quality of the consent required.[101] In comparison to the Model Code, the standards are higher in the Quebec act. The Code refers to "reasonable understanding"[102] of the level of consent, which can vary depending on the type of information collected,[103] and implied consent "when the information is less sensitive".[104] Thus, the degree of consent required from individuals is clearly greater under the Quebec act than under the Model Code.

This comparison of two standards contained in the Model Code and the Quebec act shows that significant distinctions already existed between the two normative regimes in place at the time of the discussions leading to PIPEDA. This partly explains the federal government's desire to intervene to achieve a degree of harmonization among present and future legal and quasi-legal regimes. However, this does not mean that there were no issues relating to the constitutional validity of the federal initiative.

1.3.2 Federal power to regulate trade and commerce

There are two stages involved in analyzing the constitutional validity of a statute or provision from the perspective of the division of powers under the *Constitution Act, 1867*. First, the pith and substance, or dominant characteristic, of the impugned statute or provision must be determined in order to identify the head of power to which that characteristic is most closely related.[105] To determine the pith and substance of a statute or provision, the purpose and

99 Model Code, *supra*, note 93, s. 4.3.6.

100 *Id.*, ss. 4.3.4 and 4.3.7. Section 14 of the Quebec act reads as follows: "Consent to the collection, communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested."

101 Quebec act, *supra*, note 94, s. 14.

102 Model Code, *supra*, note 93, s. 4.3.2.

103 *Id.*, ss. 4.3.4 and 4.3.6.

104 *Id.*, s. 4.3.6.

105 *Reference re* Employment Insurance Act *(Can.), ss. 22 and 23*, [2005] 2 S.C.R. 669, para. 8.

effect of the impugned statute or legislative provision must be examined.[106] The purpose of this first stage of the analysis is to determine whether the impugned statute or provision comes within the jurisdiction of the enacting government.[107]

Sections 3 and 4 of PIPEDA indicate that the purpose relates to the exchange of personal information: primarily commercial exchanges by private organizations, but also non-commercial exchanges in connection with the employer-employee relationship in a federal work, undertaking or business.[108] Non-commercial public sector uses are governed by the *Privacy Act* adopted by the federal Parliament.[109] The dominant characteristic of PIPEDA is therefore the exchange of personal information, and the exchange of personal information is under the exclusive jurisdiction of the provinces. The provinces' legislative power to legislate in relation to the use and protection of private information by the private sector operating within the province, whether under the head of property and civil rights [including privacy protection] (92.13)[110] or health (92.16), was never in question from a constitutional perspective.[111] Minister Manley even explicitly recognized that fact in his presentation on Bill C-6 (PIPEDA):

> But the basis of the trade and commerce power is commercial activity and we need the provinces to act because they have jurisdiction over some of the most sensitive information Canadians want protected, including most health, education and employee records.[112]

With respect to the effect of the Act, one of the major difficulties relates to its scope, which extends to intraprovincial trade and commerce, another clear encroachment on exclusive provincial jurisdiction. Only provinces may legislate on matters of a local nature [s. 92(16)].

---

106 *Reference* re Firearms Act *(Can.)*, [2000] 1 S.C.R. 783, para. 16; *Reference re Validity of Section 5(*a*)* Dairy Industry Act, [1949] S.C.R. 1.

107 *Reference re* Employment Insurance Act *(Can.), ss. 22 and 23, supra*, note 105, para. 8; *Reference re Same-Sex Marriage*, [2004] 3 S.C.R. 698, para. 13; *Reference re* Firearms Act *(Can.)*, *supra*, note 106, para. 15; *Reference by the Government of Quebec pursuant to the* Court of Appeal Reference Act*, R.S.Q., c. R-23, concerning the constitutional validity of sections 8 to 19, 40 to 53, 60, 61 and 68 of the* Assisted Human Reproduction Act*, S.C. 2004, c. 2 (In the matter of a)*, 2008 QCCA 1167 [Unofficial English Translation], para. 49.

108 *Personal Information Protection and Electronic Documents Act*, *supra*, note 2, s. 3.

109 *Privacy Act*, R.S.C. 1985, c. P-21.

110 Note in particular s. 1 of *An Act respecting the Protection of personal information in the private sector*, *supra*, note 94.

111 *Canadian Indemnity Co. et al., supra*, note 69, 519; *Kellogg's Co. of Canada et al.*, *supra*, note 69, 225.

112 GOVERNMENT OF CANADA, MINISTER OF INDUSTRY, "Speaking Notes: For the Honourable John Manley, Minister of Industry, Presentation to the Senate Committee Studying Bill C-6", *supra*, note 92.

Thus, the federal government through PIPEDA addresses subject matter in two areas of exclusive provincial jurisdiction. However, as the Supreme Court often reiterates, the heads of power are not static: their content evolves to reflect Canadian society so that "Confederation can be adapted to new social realities."[113] However, progressive interpretation cannot be used to justify an encroachment by one level of government on an exclusive field of jurisdiction of the other. This is why the Court sets limits on this evolution, because of [translation] "certain principles related to the very essence of Canadian federalism, particularly with regard to the sharing of powers between the federal government and the provinces."[114]

In an attempt to strike a balance between these interpretive principles and federal-provincial relations, the Supreme Court described a second aspect of the federal power to regulate trade and commerce in *City National Leasing*,[115] based on *Parsons*.[116] We now know that section 91(2) has two aspects: (1) the power over international and interprovincial trade and commerce, and (2) the power over general trade and commerce affecting Canada as a whole.[117] In this case, when the government tabled its bill, it clearly intended to rely on its power over general trade and commerce. The then Minister of Industry said the following in his presentation:

> Bill C-6 shows leadership. It uses the trade and commerce powers to create a framework for coast-to-coast protection of personal information that aims at a harmonized approach for all provincial private-sector privacy legislation. [118]

However, the federal Parliament may only validly rely on this power if it can successfully (1) demonstrate that the act is valid (or that the impugned provision forms part of a valid statutory scheme), and (2) demonstrate that the

113 *Reference re* Employment Insurance Act *(Can.), ss. 22 and 23, supra*, note 105, para. 9; *Reference by the Government of Quebec pursuant to the* Court of Appeal Reference Act*, R.S.Q., c. R 23, concerning the constitutional validity of sections 8 to 19, 40 to 53, 60, 61 and 68 of the* Assisted Human Reproduction Act *(In the matter of a)*, *supra*, note 107, para. 54.

114 *Reference by the Government of Quebec pursuant to the* Court of Appeal Reference Act*, R.S.Q., c. R 23, concerning the constitutional validity of sections 8 to 19, 40 to 53, 60, 61 and 68 of the* Assisted Human Reproduction Act *(In the matter of a), supra,* note 107, para. 57; *Reference re Secession of Quebec*, [1998] 2 S.C.R. 217, paras. 43 *et seq.*

115 *General Motors of Canada Ltd.* v. *City National Leasing*, [1989] 1 S.C.R. 641. PDF version accessible online at LexUM: http://scc.lexum.umontreal.ca/en/1989/1989scr1-641/1989scr1-641.pdf (accessed on May 11, 2010).

116 *Id.*, p. 19 of the PDF version; *Citizens' Insurance Company of Canada* v. *Parsons*, (1881) 7 App. Cas. 96.

117 *Id.*, p. 20 of the PDF version.

118 GOVERNMENT OF CANADA, MINISTER OF INDUSTRY, "Speaking Notes: For the Honourable John Manley, Minister of Industry, Presentation to the Senate Committee Studying Bill C-6", *supra*, note 112.

impugned provision is sufficiently integrated with the statutory scheme. In this case, the public policy objectives that the federal government was preparing to present to Parliament posed problems at both stages of the test.

1.3.2.1 The existence of a valid statutory scheme

As the Supreme Court wrote in *City National Leasing*, finding whether the federal act is valid ". . . will normally involve finding the presence of a regulatory scheme and then ascertaining whether that scheme meets the requirements articulated in *Vapor Canada* . . . and in *Canadian National Transportation*."[119] These conditions correspond to the first three of the five factors set out in *City National Leasing*. The purpose of these factors is to assess correctly "the balance to be struck between ss. 91(2) and 92(13)."[120] The first three factors are the following:

1. the impugned legislation must be part of a general regulatory scheme;
2. the scheme must be monitored by the continuing oversight of a regulatory agency; and
3. the legislation must be concerned with trade as a whole rather than a particular industry.

In this case, the federal government announced that the purpose of PIPEDA would be to establish a general regulatory scheme (1st factor).[121] It also announced that the scheme would be monitored by a regulatory agency, in this case the Office of the Privacy Commissioner (2nd factor).[122] These two criteria were therefore satisfied, so any problems with the bill were not related to these factors, but rather the third: the legislation must be concerned with trade *as a whole* rather than a particular industry. Here, the federal government's purpose was to regulate the use of or trade in personal information, i.e. a particular industry or segment of trade[123] and not trade as a whole (as does the *Competition Act*, for example[124]).[125] This was therefore a constitutional

---

119 *General Motors of Canada Ltd.* v. *City National Leasing*, *supra*, note 115, p. 35 of the PDF version.

120 *Id.*, p. 23 of the PDF version. In 1998, the test still involved the analysis of five factors by way of a three-step method. For simpler formulations, see: *Kitkatla Band* v. *British Columbia (Minister of Small Business, Tourism and Culture)*, [2002] 2 S.C.R. 146, para. 58; *Kirkbi AG* v. *Ritvik Holdings Inc.*, [2005] 3 S.C.R. 302, para. 20.

121 Josh NISKER, "PIPEDA: A Constitutional Analysis", 85 *Canadian Bar Review* 317, contains a brief analysis of the factors at pages 331 *et seq*.

122 *Id*.

123 Colin McNAIRN and Alexander SCOTT, *A Guide to the Personal Information Protection and Electronic Documents Act*, Markham, LexisNexis Canada Inc., Ontario, 2007, p. 14.

124 As in *City National Leasing*, *supra*, note 115.

125 J. NISKER, *supra*, note 121. As previously mentioned, Minister Manley made a similar observation in his remarks, *supra*, note 112.

weakness that could not be ignored. It is probably partly for this reason that the federal government opted, in response to challenges from the provinces, to have PIPEDA apply to intraprovincial trade only until that province passed legislation of its own. As then Minister Manley explained, "After coming into effect, this Bill will apply until provinces act to protect personal information within their own borders. It will continue to apply where there is no privacy protection, and it will apply to transborder flows of information."[126] The federal government was therefore banking on having the provincial and territorial governments regulate personal information in the private sector in order to guarantee the constitutional validity of its own legislation in the longer term. Today, however, we remain far from attaining that objective.

These were not the only obstacles to constitutional validity, as there remained the second branch of the test to satisfy. Even taking for granted that the legislation was valid (1st branch), according to the method elaborated by the Supreme Court, it was necessary to determine whether the "impugned provision is sufficiently integrated with the scheme that it can be upheld by virtue of that relationship." At this stage, the fifth factor set out in *City National Leasing* becomes particularly relevant: "the failure to include one or more provinces or localities in a legislative scheme would jeopardize the successful operation of the scheme in other parts of the country."[127] To analyze this issue, the Supreme Court established the following test in *City National Leasing*:

> This requires considering the seriousness of the encroachment on provincial powers, in order to decide on the proper standard for such a relationship. If the provision passes this integration test, it is *intra vires* Parliament as an exercise of the general trade and commerce power. If the provision is not sufficiently integrated into the scheme of regulation, it cannot be sustained under the second branch of s. 91(2).[128]

In short, the Court must determine whether there is a rational, functional connection between the statute that has been declared valid and the impugned provision. According to the Court, the more serious the encroachment, the more strictly the rational, functional connection test must be applied; the less serious the encroachment, the more flexibly the test may be applied.

126 Remarks by Minister Manley, *supra*, note 112.

127 *General Motors of Canada Ltd.* v. *City National Leasing*, *supra*, note 115, p. 26 of the PDF version.

128 *Id.,* at pp. 35-36 of the PDF version.

1.3.2.2 The integration of the impugned provisions with the legislative scheme

It is very difficult to predict whether a provision will be considered sufficiently integrated, as the Supreme Court jurisprudence is vague on this issue. The Court has granted judges significant discretion:

> The same test will not be appropriate in all circumstances. In arriving at the correct standard the court must consider the degree to which the provision intrudes on provincial powers. The case law, to which I turn below, shows that in certain circumstances a stricter requirement is in order, while in others, a looser test is acceptable. For example, if the impugned provision only encroaches marginally on provincial powers, then a «functional» relationship may be sufficient to justify the provision. Alternatively, if the impugned provision is highly intrusive *vis-à-vis* provincial powers then a stricter test is appropriate. A careful case-by-case assessment of the proper test is the best approach.[129]

Therefore, identifying the applicable standard for establishing the relationship of constitutional validity between the valid statute and the impugned provision requires an *a priori* assessment of the degree of encroachment on exclusively provincial powers. It is noteworthy that the Court recommends a degree of judicial restraint in proposing strict tests that would result in striking down such legislation. It explains:

> In determining the proper test it should be remembered that in a federal system it is inevitable that, in pursuing valid objectives, the legislation of each level of government will impact occasionally on the sphere of power of the other level of government; overlap of legislation is to be expected and accommodated in a federal state.[130]

In this case, one of the most controversial mechanisms in the federal legislation is that enabling the federal government to force the provinces to adopt minimum protection standards. As we are all aware, PIPEDA applies to any private sector organization exchanging personal information, whether intraprovincially, interprovincially or internationally. In order to "recover its jurisdiction" over intraprovincial trade and commerce, a province must adopt legislation substantially similar to that of the federal government. The evaluation of whether the provincial legislation is substantially similar is

129 *General Motors of Canada Ltd.* v. *City National Leasing*, *supra*, note 115, p. 32 of the PDF version.

130 *Id.*, p. 33 of the PDF version.

carried out by the Privacy Commissioner,[131] but it is the Governor in Council who must officially recognize this fact through an order.[132] The content of the protection and the procedures form part of the Commissioner's evaluation.[133] Only when this process is complete does PIPEDA cease to apply to intraprovincial trade in personal information and the provincial legislation take its place.[134]

The federal government employs a mechanism of statutory harmonization to impose its standards on the provinces. Both in 1998 and today, the issue is whether this type of mechanism (or any other harmonization mechanism whose purpose is to establish national standards) is valid. That question may well be answered in the next few years. In 1996, the Attorney General of Quebec filed an application for judicial reference challenging the validity of PIPEDA with the Court of Appeal of Quebec. The Attorney General of Quebec has not yet filed any arguments, given that the Supreme Court of Canada has not yet decided another case in which a similar mechanism for harmonizing provincial and national standards is at issue.[135]

* *
*

Our objective in this section was to identify some of the economic, political and legal factors that have influenced the adoption of PIPEDA's legislative policies. As we have seen, PIPEDA has several objectives, not all of which can necessarily be reconciled, but that, as with all legislation, represent all of the compromises required in order for the statute to be adopted.

In developing an evaluation process, it is very important to understand the ideas that substantially influenced the legislative goals eventually entrenched in PIPEDA ten years ago. In reviewing a statute's effectiveness, one must determine whether the assumptions underlying past legislative choices remain

131 *Personal Information Protection and Electronic Documents Act, supra,* note 2, ss. 23(1).

132 *Id*., ss. 26(2).

133 CANADA, PRIVACY COMMISSIONER OF CANADA, *Report to Parliament Concerning Substantially Similar Provincial Legislation*, Ottawa, Department of Public Works and Government Services, 2002, p. 2. This publication is available at the Commissioner's website: www.priv.gc.ca (accessed on May 11, 2010).

134 *Id.*

135 The mechanism in question is that described in ss. 68(1) of *An Act respecting assisted human reproduction and related research*, L.C. 2004, c. 2. *Reference by the Government of Quebec pursuant to the* Court of Appeal Reference Act, *R.S.Q., c. R 23, concerning the constitutional validity of sections 8 to 19, 40 to 53, 60, 61 and 68 of the* Assisted Human Reproduction Act *(In the matter of a)*, *supra,* note 107, para. 34. The case was heard by the Supreme Court on April 25, 2009. The docket number is 32750.

valid. If not, it becomes crucial to identify the changes that have taken place over time to understand the events at the root of the identified problems. In this respect, quantitative evaluations may be useful. However, these are often based on an analysis of the parts rather than the whole. For this reason, it is important not to neglect qualitative studies. Obviously, neither the numbers nor the facts can provide a complete picture, but when they point in the same direction, quantitative and qualitative analyses are powerful tools in the search for potential solutions. The purpose of the second section was to identify which aspects of the modern context had changed so as to influence the selection and adoption of new legislative policies. Once this analysis is complete, we will be able to identify avenues for future research that will help establish more specific objectives for an assessment of PIPEDA'S effectiveness.

Section 2: New contemporary concerns

Should PIPEDA require amendments, bridges between past and future will have to be built. What has changed in the economic, political and legal context since the Act was passed? Are there any new openings or new constraints that would allow for discussion about possible reforms to the Act to be conducted on the basis of other assumptions? In this section we propose a few avenues for consideration.

Without question, the first significant change is in the technological environment that PIPEDA is required to govern. A second important point is the transformations in the organization of the federal government, which must be considered in order to better understand the role that can be played by an ombudsman, such as the Privacy Commissioner, in providing oversight of private activities. Finally, the evolution of the national and supranational legal contexts is another unavoidable factor that must be examined when thinking about possible reforms.

2.1 The technology dimension: Emergence of Web 2.0[136]

What Internet-related changes and innovations have taken place since the passage of PIPEDA? In this section, we look at Internet use that has had a major impact on the management and protection of personal information that was not considered by Parliament at the time PIPEDA was drafted. There are many such uses, but they all follow from one phenomenon: the emergence of Web 2.0.

136 The authors extend particular thanks to Mr. Nicolas Vermeys, LL.D. for his invaluable assistance with the writing of this section of the report. Mr. Vermeys is coordinator of the cyberjustice projects of the Centre de recherche en droit public at the Université de Montréal. On the issue of Web 2.0 and protection of personal information, one can also read the brand new work by professors Vincent GAUTRAIS and Pierre TRUDEL, *Circulation des renseignements personnels et le Web 2.0* (Montreal: Les Éditions Thémis, 2010), 231 p.

The term "Web 2.0" is attributed to Tim O'Reilly,[137] president of O'Reilly Media.[138] Making its first appearance in 2004,[139] this concept refers to the tendency observed in certain Web enterprises to publish user-generated content (UGC) instead of using the traditional business model to put proprietary media content online. Mr. O'Reilly sees Web 2.0 as being based on the following seven principles:

- Services, not packaged software, with cost-effective scalability
- Control over unique, hard-to-recreate data sources that get richer as more people use them
- Trusting users as co-developers
- Harnessing collective intelligence
- Leveraging the long tail [i.e. reaching out to the edges and not just the centre of the Web] through customer self-service
- Software above the level of a single device
- Lightweight user interfaces, development models, and business models.

In short, Web 2.0 is not a re-engineering of the Internet, but rather a business model based on the collective contribution and convergence of services that is better adapted to the new realities of the Web, as evidenced by today's Wikipedias,[140] YouTubes[141] and MySpaces.[142]

What we have today, then, are collegial, if not symbiotic, relationships between the various service providers, as well as between service providers and users — relationships that have a marked impact on the notions of privacy and protection of personal information. For greater contribution of content by Internet users carries the risk of disclosure, either deliberately or inadvertently, of a certain amount of personal information. Furthermore, the convergence of

137 See Tim O'REILLY, "What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software" (2005), available at: http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1. A French version entitled "Qu'est-ce que le web 2.0: modèles de conception et d'affaires pour la prochaine génération de logiciels" (2006), is available from: http://www.eutech-ssii.com/ressources/1 (last visit: March 23, 2010).

138 *Id.*

139 *Id.*

140 www.wikipedia.org: "Wikipedia is a multilingual, web-based, free-content encyclopedia project based on an openly-editable model."

141 www.youtube.com: "YouTube is the leader in online video, and the premier destination to watch and share original videos worldwide through a Web experience. YouTube allows people to easily upload and share video clips on www.YouTube.com and across the Internet through websites, mobile devices, blogs, and email."

142 www.myspace.com: "MySpace is an online community that lets you meet your friends' friends. Create a community on MySpace and you can share photos, journals and interests with your growing network of mutual friends! See who knows who, or how you are connected. Find out if you really are six people away from Kevin Bacon."

services is generating increased circulation, and even unauthorized sharing, of information about the users of those services.

To better circumscribe the various privacy-related problems in the Web 2.0 context, we have grouped them into three subsections: (1) the emergence of social networking sites; (2) the refinement and increased versatility of search engines; and (3) the convergence of Web tools and services. Note, however that given this convergence, this sort of division is artificial, and its sole purpose is to facilitate the reading of this report. It cannot constitute an "official" classification of the impact of Web 2.0 on the concepts of privacy and protection of personal information.

2.1.1 Social networking sites

Social networking sites can be defined as Web-based interpersonal relationship networks that permit users to build and expand their circle of acquaintances through friends and the friends of friends who make up the network.[143] These sites, the most famous being Facebook[144] and MySpace,[145] are the element of Web 2.0 that is prompting the most fears regarding privacy. A report prepared by the Office of the Privacy Commissioner called *Social Network Site Privacy: A Comparative Analysis of Six Sites*[146] has looked into the main problems related to these sites. Without repeating the content of the report, it is important to note that these problems are caused by three things: (a) use by the sites of the personal information of Internet users; (b) use by third parties of the personal information of Internet users; and (c) unlawful dissemination by Internet users of the personal information of third parties.

2.1.1.1 Use of Internet users' personal information

The main fear about social networking sites is how the information collected by those sites is used. For example, despite the fact that Facebook has agreed to respond to the Privacy Commissioner's concerns about its use of the personal information it holds about its subscribers,[147] the site's Privacy Policy, which was updated on December 9, 2009,[148] still permits the service to track its users' activities and to collect information without their knowledge, notably through third-party or other site accounts, which is contrary to the requirements of PIPEDA (s. 4.3 of Schedule 1 to the Act). This information is then used for

143 www.granddictionnaire.com.

144 http://www.facebook.com.

145 http://www.myspace.com.

146 See OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Social Network Site Privacy: A Comparative Analysis of Six Sites* (Ottawa: Office of the Privacy Commissioner of Canada, 2009), available at: http://www.priv.gc.ca/information/pub/sub_comp_200901_e.cfm (last visit: March 23, 2010).

147 *Id.*

148 See: http://www.facebook.com/policy.php.

statistical, advertising and commercial purposes, which appear to exceed the "reasonable expectations" (s. 4.3.5 of Schedule 1 to PIPEDA) of certain users.

Furthermore, the site's "Statement of Rights and Responsibilities"[149] provides for the granting of "a non-exclusive, transferable, sub-licensable, royalty-free, worldwide licence to use any IP content that you post on or in connection with Facebook". Since any image or text containing personal information can be legally deemed "intellectual property", this licence seems to overstep the limits set by PIPEDA (s. 4.5 of Schedule 1) relating to the use of data.

2.1.1.2 Use of Internet users' personal information by third parties

The use of Internet users' personal information by third parties is not due to some evil intention on the part of social networking sites, but to those users' carelessness or ignorance. For they themselves publicize a certain amount of personal information about them with no fear for the consequences that such transparency could entail.[150] As demonstrated in an article published in the French bimonthly newsletter *Le Tigre*[151] in January 2009, the amount of information made available on such sites can sometimes be alarming:

> [*translation*]
> Happy birthday, Mark. On December 5, 2008, you will be 29. Mind if I treat you like a buddy, Marc? True, you don't know me. But I know you real well. You had the fortune, or misfortune, to be the first Google profile in *Le Tigre*. It's a very simple idea for a column: we take an anonymous person and tell his life using all the tracks he has left on the Web, whether deliberately or not. What's that you say? Is there some message behind this column? Of course: the idea that we don't really pay attention to the private information available on the Internet, and that once it is all brought together, it suddenly makes for a very worrying picture […]

The article goes on to explain that, using Mark's Facebook profile, the journalist was able to find out many details about his private life. Obviously, the private life of an individual belongs to him, and it is up to each person to decide what he or she wants to make public. It is therefore important not to take a paternalistic attitude and impose a collective sense of modesty via legislation or some other route. Although most social networking sites offer an option

149 http://www.facebook.com/terms.php?ref=pf.

150 Excessive disclosure of personal information via these sorts of sites could augment the risks of identity theft. However, it is important to note that such risks are just as high when we put personal information in our household garbage or recycling bins. See: http://www.cisc.gc.ca/annual_reports/annual_report_2008/feature_focus_2008_e.html.

151 http://www.le-tigre.net/Marc-L.html (last visit: March 23, 2010).

whereby you can limit access to your profile, this option is not always activated by default, in spite of what users might think.[152] Therefore it is a matter of informing and educating Internet users about the consequences of putting personal information online, and in particular the relative perpetuity of this data once it is posted on the network.

It is important to note that the collection of such information by a third party is prohibited by Principle 3 of Schedule 1 to PIPEDA regarding consent, and specifically section 4.3.1 which states: "Consent is required for the collection of personal information and the subsequent use or disclosure of this information." However, a company could argue that an Internet user who has a public profile on Facebook must have a reasonable expectation that this information will be collected by third parties (s. 4.3.5 of Schedule 1 to PIPEDA) and that there is implied consent to such use of Facebook (s. 4.3.7(*d*) of Schedule 1 to PIPEDA).

2.1.1.3 Unlawful dissemination a third party's personal information by Internet users

Social networks facilitate, if not encourage, the unlawful dissemination of a third party's personal information. For example, a television ad by Rogers, broadcast in 2008, advertised a young person photographing a friend and then sending that image directly to his or her Facebook album to share it with third parties. Yet such publication of an individual's image without obtaining his or her prior permission is contrary to the directions of the Supreme Court.[153]

While they are not social networking sites as such, sites that permit the sharing of images, such as Flickr,[154] or videos, such as YouTube,[155] are participants in this publicization of private life. Once again, this is not a matter of making a value judgment on the desire of Internet users to share their images with third parties. It is simply a matter of ensuring that they fully understand the consequences of such sharing. What is more, like all the social networking sites, these sites reserve certain rights to redistribute and reuse user-posted content, which could have harmful repercussions for a possible "*droit à l'oubli numérique*" or "right to forget".[156] For example, the YouTube "Terms of Use" stipulate that:

---

152 See *Social Network Site Privacy: A Comparative Analysis of Six Sites*, *supra,* note 146.

153 See *Aubry v. Éditions Vice-Versa inc.*, [1998] 1 S.C.R. 591.

154 http://www.flickr.com/.

155 http://www.youtube.com.

156 A bill that would recognize such a right was tabled in France on November 6, 2009. See: http://www.senat.fr/leg/ppl09-093.html. Note that the concept of "*droit à l'oubli*" has been recognized by Quebec case law. See *Bombardier c. Bouchard*, 1996 CanLII 6356 (QC C.A.).

> … by submitting User Submissions to YouTube, you hereby grant YouTube a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the User Submissions in connection with the YouTube Website and YouTube's (and its successors' and affiliates') business, including without limitation for promoting and redistributing part or all of the YouTube Website (and derivative works thereof) in any media formats and through any media channels.[157]

This indirectly implies that personal information contained in videos uploaded to YouTube may be exploited by the company for purposes not foreseen by the user. This is particularly problematic when the uploaded content contains information concerning a third party who did not consent to such distribution (such as a friend featured in the video).

2.1.2 Refinement and increased versatility of search engines

At the time that PIPEDA was passed, most search engines indexed Web sites based on their meta tags, which are HTML tags inserted in the <head> area of a Web page, after the title, whereby the content of the page can be described for correct and easier referencing in search engines.[158] In concrete terms, they are keywords found in a page's HTML code that are supposed to describe its content. Site administrators thus had some degree of control over their classification according to the tags selected. However, although a judicious choice of the keywords used to index a Web page still assists in its classification,[159] modern search engines employ a combination of criteria to index sites. In fact, Google, which is used for 65% of Internet searches,[160] does not use meta tags as a classification criterion.[161]

> Modern search engines now use complex algorithms and hundreds of different ranking criteria to produce their results. Among the data sources is the feedback loop generated by the frequency of search terms, the number of user clicks on search results, and our own personal search and browsing history. For example, if a majority of users

157 http://www.youtube.com/t/terms.

158 www.granddictionnaire.com.

159 See in particular *Netbored v. Avery Holdings Inc.*, 2005 FC 1405 (CanLII), para. 4.

160 "comScore Releases June 2009 U.S. Search Engine Rankings" (2009), available at this address: http://www.comscore.com/Press_Events/Press_Releases/2009/7/comScore_Releases_June_2009_U.S._Search_Engine_Rankings.

161 See: http://googlewebmastercentral.blogspot.com/2009/09/google-does-not-use-keywords-meta-tag.html.

> start clicking on the fifth item on a particular search results page more often than the first, Google's algorithms take this as a signal that the fifth result may well be better than the first, and eventually adjust the results accordingly.[162]

In other words, personal information that used to be lost in cyberspace is now becoming easily accessible. What is more, the addition of image search tools such as Google Images[163] makes it possible to link a name to a face in a few clicks, an operation made that much easier by the presence of public profiles on the various social networking sites. Certain search engines also allow users to search for addresses: for example, Google Maps[164] and Yahoo! Maps.[165]

The Google Maps engine recently generated a flood of comment following the introduction of the "Google Street View" service, which allows one to "zoom, rotate and pan through street level photos of cities around the world".[166] Since being launched in Canada, the site has provided access to images of a Montreal citizen leaving a sex shop on Ste-Catherine Street[167] and two female University of Ottawa students sunbathing.[168] Although this service has "[translation:] developed a very sophisticated technology that can blur faces and licence plates",[169] the fact is that this technology is not flawless. Even when a face is blurred, it may still be possible to identify the individual using other criteria such as his or her geographic location, appearance and dress.[170] Although it is possible to ask that an image be removed,[171] the fact remains that this technology is contrary to the position adopted by the Supreme Court in *Aubry v. Éditions Vice-versa,*[172] to the effect that "a photographer [must] obtain the consent of all those he or she photographs in public places before publishing their photographs".[173] Eventually this inconsistency will therefore have to be corrected, either by legislation or by the closure of the service.

---

162 Tim O'REILLY and John BATTELLE, "Web Squared: Web 2.0 Five Years On" (2009), available at this address: http://www.web2summit.com/web2009/public/schedule/detail/10194.

163 http://images.google.ca/.

164 http://maps.google.ca/.

165 http://ca.maps.yahoo.com/.

166 See: http://maps.google.ca/help/maps/streetview/.

167 See: http://www.infinit.net/techno/nouvelles/archives/2009/10/20091008-073509.html.

168 Ian KERR, "Soft Surveillance, Hard Consent," lecture given on December 1, 2009 at the Université de Montréal.

169 http://maps.google.ca/help/maps/streetview/privacy.html.

170 I. KERR, *supra,* note 168.

171 http://maps.google.ca/help/maps/streetview/privacy.html.

172 *Aubry v. Éditions Vice-Versa inc.*, *supra*, note 153.

173 *Id.*, para. 65.

2.1.3 Convergence of Web tools and services

As Tim O'Reilly explains:

> When commodity components are abundant, you can create value simply by assembling them in novel or effective ways. Much as the PC revolution provided many opportunities for innovation in assembly of commodity hardware, with companies like Dell making a science out of such assembly, thereby defeating companies whose business model required innovation in product development, we believe that Web 2.0 will provide opportunities for companies to beat the competition by getting better at harnessing and integrating services provided by others.[174]

This principle of "innovation in assembly"[175] involves a certain amount of information sharing between departments of the same company, and even between different companies. For example, the toolbar of the Firefox browser includes a Google search window, while Facebook allows the incorporation of videos from the YouTube site. In some cases, third parties will combine the content of different suppliers to offer a new service. This is the case, for example, with the site http://www.housingmaps.com/, which combines information from Craigslist.com and Googlemaps.com to permit a housing search by geographic region.[176]

This collaboration between different services necessarily entails substantial sharing of data about the said services, but also about users. This is why Google's "Privacy Center"[177] warns users: "We offer some of our services on or through other web sites. Personal information that you provide to those sites may be sent to Google in order to deliver the service". Google is in fact a typical example of service convergence, since its Privacy Policy "applies to all of the products, services and websites offered by Google Inc. or its subsidiaries or affiliated companies except DoubleClick and Postini,"[178] which includes Gmail, Google Maps, YouTube, Blogger, etc.[179]

Similarly, Facebook's Privacy Policy states: "We may provide services jointly with other companies, such as the classifieds service in the Facebook Marketplace. If you use these services, we may share your information to facilitate that service". While such sharing may be necessary to establish

174 See T. O'REILLY, *supra,* note 137.

175 *Id.*

176 *Id.*

177 http://www.google.ca/privacypolicy.html.

178 *Id.*

179 See: http://www.google.ca/options/.

gateways between services, and hence for the overall user-friendliness of the Web, the fact remains that it is contrary to the principles of *identifying purposes*, *consent* and *limiting use, disclosure and retention* cited in sections 4.2, 4.3 and 4.5 of Schedule 1 to PIPEDA.

According to the experts, the current trend is pointing to the eventual creation of a "network-wide identity database"[180] (a project which has already been initiated by Google),[181] and hence wider sharing of the personal information of Internet users. This trend has similarities to the concept of "cloud computing", which refers to a "[translation:] computing model which, through distant servers interconnected by the Internet, permits on-demand network access to a shared pool of configurable, externalized and non-locatable computer resources, in the form of services which are evolving, dynamically customizable, and billed upon use".[182]

> Any information stored locally on a computer could be stored in a cloud, including email, word processing documents, spreadsheets, videos, health records, photographs, tax or other financial information, business plans, PowerPoint presentations, accounting information, advertising campaigns, sales numbers, appointment calendars, address books, and more. The entire contents of a user's storage device may be stored with a single cloud provider or with many cloud providers.[183]

The fact that this information is available in a "cloud" means that it can be stored on different sites offering variable levels of security, and also in different countries where the privacy legislation is not always on a par with Canadian law.[184] What's more, the service provider has access to *all* of the information on a user, information that it may, depending on the context, choose to share with other companies.[185] Obviously, if the personal information deposited in the cloud is controlled by the person it identifies, the issue is not the same as when the information is deposited in the cloud by a third party.

* *
*

180 See T. O'REILLY, *supra,* note 137.

181 *Id*.

182 See: http://www.granddictionnaire.com.

183 See WORLD PRIVACY FORUM, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing" (2009), available at: http://www.worldprivacyforum.org/cloudprivacy.html.

184 *Id*.

185 *Id.*

In short, it must be emphasized that to conceive of the Internet simply as a computer network is to hold an outdated view of technology. Smart phones, AppleTV and VoIP (Voice over IP) technology are all examples which demonstrate that interconnectedness and media pairing are forcing us to redefine our concept of media:

> … more and more devices are [being] connected to the new platform [of the Web]. What applications become possible when our phones and our cars are not consuming data but reporting it?[186]

Where management and protection of personal information are concerned, the repercussions of this paradigm shift are many. The reporting of data regarding our position, our activities and our routine, all of which constitute personal information within the meaning of section 2 of PIPEDA, implies a constant circulation of information about us, and hence a greater need for safeguards for all of these communications (section 4.7 of Schedule 1 to PIPEDA). This exponential proliferation of information concerning us also demands a collective realization of the fact that the advantages offered by this technology are difficult to reconcile with current legislative requirements for the collection, retention and destruction of information (sections 4.2 and 4.5 of Schedule 1 to PIPEDA).

2.2. The organizational dimension: Emergence of other types of state institutions

With the advent of the welfare state, the executive branch, as we know, underwent substantial expansion, through the creation of not only multiple new departments, but also a great many decentralized organizations (administrative tribunals, administrative commissions and economic regulatory agencies).

In the 1970s and 1980s, governments questioned the effectiveness and efficiency of the welfare state, leading to major reorganizations of services and the dismantling of many decentralized organizations. What was particularly notable in this overhaul, however, was the emergence of another type of organization: the agencies that provide oversight for the activities of the administration. This type of agency was not completely unknown to legislatures before the 1970s, but from that decade forward, more were to be created.

There are a number of distinguishing traits of these oversight agencies, traits that some authors see as heralding the advent of a national integrity system, which, organizationally, is a component of the parliamentary rather than governmental apparatus. First of all, we will explore the intellectual origins of the concept of the integrity system. It should be noted that this new integrity system is designed as a mechanism to oversee government activities as a whole,

186 See T. O'REILLY, *supra,* note 137.

and not the activities of the private sector. The Privacy Commissioner, however, oversees both public activities (*Privacy Act*) and private activities (PIPEDA).

Given the upsurge in the creation of this type of agency within the federal government, we have to question the extent to which the initial decision to assign jurisdiction to administer PIPEDA to the Privacy Commissioner is consistent with the transformations in the organization of the federal government. This is the second question we will be considering.

2.2.1 The integrity system

In an article published in 1999, Professor Bruce Ackerman argues for what he describes as "the integrity branch".[187] This American researcher is formally proposing that such a branch be created within the republican political system of the United States. He says that the agencies that would be part of this branch would act as "constitutional watchdogs".

Professor Ackerman feels that this branch must function separately from the other three branches of the State (the judiciary, the executive and the legislature). Its role would be focussed exclusively on oversight and monitoring risks of corruption. Many times in his text, he argues that we have to break free from the traditional design of the three branches of state.[188] Therefore he proposes constructing a new doctrine of the separation of powers, and encourages the framers of modern constitutions to consider incorporating an integrity branch. The author's main justification for the creation of an integrity branch is that, in his view, politicians cannot be trusted to get serious about corruption.[189]

The formation of an integrity branch has become a subject of interest for other legal scholars as well. The contribution of Justice Spigelman, who has proposed that this branch be introduced in the Australian parliamentary system, is largely concerned with extending the jurisdictions of the agencies that are part of this integrity system.

2.2.1.1 Extending the jurisdictions of public organizations

Ackerman's idea has drawn the interest of lawyers who work in a parliamentary system such as ours. In fact, a few years after Ackerman's text was published,

187 Bruce ACKERMAN, "The New Separation of Powers" (1999-2000) 113 *Harvard Law Review* 633, p. 694-696; See also a previous article by Bruce TOPPERWIEN, "Separation of Powers and the Status of Administrative Review," (1999) 20 *Australian Institute of Administrative Law Forum* 32.

188 B. ACKERMAN, *supra,* note 187, 691.

189 *Id*., 694.

the Honourable James Spigelman, a chief justice in Australia,[190] spoke out in favour of creating an "integrity branch" in his country. In so doing he transposed Ackerman's idea to a British parliamentary system:

> The parliament as an institution does more than legislate. It performs an important role in ensuring that powers conferred upon the executive and judges, given the authority of parliaments to remove judicial officers, are properly performed. The integrity function of parliament lies at the heart of legitimacy of our governmental process.[191]

The judge explains that the jurisdictions of such a branch should not be limited to problems of corruption (as Ackerman proposes), for he feels that so narrow a jurisdiction would be inadequate in itself to encompass all abuses of power. So he goes further, adding that the rationale of this branch must be expanded to include respect for "the rule of law" and "morality in law". These two ideas advanced by the judge are not new, for the philosopher Lon Fuller had presented them earlier in his writings.[192]

The integrity branch should have the function of overseeing public institutions to ensure they do not stray from either the functions for which they were created or the public values which they are obliged to observe:[193]

> A short definition is that the integrity branch or function of government is concerned to ensure that each governmental institution exercises the powers conferred on it in the manner in which it is expected and/or required to do so and for the purposes for which those powers were conferred, and for no other purpose.

In his analysis, Justice Spigelman emphasizes institutional integrity rather than personal integrity, while noting that the latter is directly related to the former. On the one hand, he explains that personal integrity can be described in terms of such personal qualities as honesty, absence of corruption, ethical conduct and compliance with proper practice. On the other, he says that institutional

---

190 The Honourable James SPIGELMAN, Chief Justice, "The Integrity Branch of Government – The First Lecture in the 2004 National Lecture Series," lecture given in the *National Lecture Series of the Australian Institute of Administrative Law* (Sydney, April 29, 2004), available online at this address: http://www.lawlink.nsw.gov.au/lawlink/supreme_court/ll_sc.nsf/pages/SCO_speech_spigelman_290404 (last visit: December 14, 2009). The judge has published a whole series of speeches on the same subject, which are available online.

191 The Honourable Chief Justice James SPIGELMAN, "The Integrity Branch of Government," *Quadrant,* XLVIII, **7 (**July-August 2004), p. 51.

192 See for example: Lon L. FULLER, "Positivism and Fidelity to Law — A Reply to Professor Hart," (1958) 71: 4 *Harvard Law Review* 630.

193 The Honourable Chief Justice Spigelman, *supra,* note 190, p. 52.

integrity breaks down into three main elements: the conduct of every government institution (1) must be authorized by law, (2) must be faithful to the public purposes for which a power was conferred or a duty imposed, and (3) must be in accordance with the values the institution is expected to obey.[194]

Using numerous examples, he notes that many existing institutions within the three recognized branches already collectively constitute an integrity system, but emphasizes the organizational limitations of the *status quo*.[195] For it is necessary to point out the limitations of such a system when the agencies that are part of it are at insufficient arm's length from the government whose actions they are supposed to be overseeing. Finally, he feels that traditional administrative law literature has already explored many themes analyzing the integrity system and that it is now time to propose a new unified assembly of them.[196] On this point, an examination of the Canadian "integrity system" at the federal level shows that there is already great consistency in terms of the institutional organization of this type of agency.

2.2.1.2 Institutional consistency of the federal integrity system

Within the Canadian federal government, there are already about a dozen public organizations with different jurisdictions, but all of them connected to a broader notion of integrity such as proposed by Justice Spigelman, and responsible for overseeing government activities, whether those activities are the product of central agencies or decentralized organizations.

As we mentioned in the introduction, this type of agency is not a totally new phenomenon. The first to be established, and the oldest, is without question the Auditor General's office, born in 1908. Next came the Office of the Chief Electoral Officer in 1920. For a period of 50 years, however, no other new organization of this type was created. It was not until the 1970s that such agencies emerged again on the federal scene. In 1970 the Office of the Commissioner of Official Languages was established. In 1983 came two more commissioners' offices: the offices of the Privacy Commissioner and the Access to Information Commissioner. The new millennium brought some real enthusiasm for this sort of agency, for five new ones were created: the Parliamentary Budget Officer (2006), the Office of the Commissioner for Public Appointments (created in 2006, but an incumbent has yet to be

194 The Honourable Chief Justice James SPIGELMAN, "Judicial Review and the Integrity Branch of Government Address," given at the *World Jurist Association Congress* (Shanghai, September 8, 2005), available online at this address: http://www.lawlink.nsw.gov.au/lawlink/supreme_court/ll_sc.nsf/pages/SCO_spigelman080905 (last visit: December 14, 2009). See also: John McMILLAN, "The Ombudsman and the Rule of Law" (2005), 44 *Australian Institute of Administrative Law Forum* 1; Anita STUMCKE and Anne TRAN, "The Commonwealth Ombudsman: an Integrity Branch of Government?" (2007) 32: 4 *Alternative Law Journal* 233.

195 The Honourable Chief Justice SPIGELMAN, *supra*, note 190, p. 51.

196 *Id*., p. 57.

appointed[197]), the Office of the Conflict of Interest and Ethics Commissioner (House of Commons and Senate) (2007), the Office of the Public Sector Integrity Commissioner (2007) and the Office of the Commissioner of Lobbying (2008). Finally, note must be taken of Parliament's recognition of the importance of two other commissioners' offices, those of the Human Rights Commission and the Public Service Commission. These are two longstanding organizations, but only in the last few years have their executives been recognized as Officers of Parliament.[198] In summary, our national integrity system is a group of organizations responsible for ensuring that administration of the federal government is as upright as possible, in terms of:

- public accounts and budget management, the electoral system, the access to information system, and the system for hiring public servants and public office holders (in the latter case, no one has yet been appointed to this position);
- protection of the right to personal integrity (protection of personal information and human rights);
- oversight of measures to combat corruption among public servants and public office holders.

Our national integrity system shows a high level of coherence and consistency in at least two regards. First, there is very great consistency in the high degree of independence that these agencies are acknowledged to have, so that they can carry out their mission free from government pressure. Second, and relatedly, these agencies are offices of Parliament, and not part of the executive branch.

Regarding their degree of independence, it should be noted that the incorporating legislation of these agencies contains very clear differences from the statutes incorporating decentralized bodies such as administrative tribunals. One of the very significant distinctions is the fact that the executives of these agencies are appointed by a procedure that requires the participation of parliamentarians. Generally, both the House of Commons and the Senate have to be consulted by the government regarding the person that the government intends to appoint, who must receive the approval of both

197 *Salaries Act*, R.S.C. 1985, c. S-3, s. 1.1, Act amended by s. 227 of the *Federal Accountability Act*, S.C. 2006, c. 9, s. 109 ff.

198 http://www2.parl.gc.ca/Parlinfo/compilations/OfficersAndOfficials/OfficersOfParliament.aspx?Language=E

chambers.[199] This appointment procedure contrasts with those used to appoint members to decentralized bodies (such as administrative tribunals), whose appointment requires only the support of the government. The removal of members appointed to agencies in the national integrity system also requires the support of both chambers, as is not the case for the removal of members of decentralized organizations.

Two points are to be noted with regard to the attachment of these agencies to Parliament. First, all the executives of these agencies are now recognized as Officers of Parliament (of course, that status relates to the special procedures which have to be followed in order to appoint or remove these executives). The term "Officer of Parliament" designates various positions of persons who play key roles in the exercise of parliamentary functions:

1. Senators and MPs who are appointed to certain Parliament-related positions;
2. Procedural clerks and senior executives of the Senate, House of Commons and Library of Parliament;
3. Independent public servants entrusted with oversight who report to Parliament.[200]

The latter is the category containing the heads of the agencies we have listed, including the Office of the Privacy Commissioner, which is our focus. The designation of Officer of Parliament is used to:

> … [emphasize] that they carry out work for Parliament and are responsible to Parliament, and as a means of distinguishing them from other officers and officials of

199 It is important to note, however, that the procedures for appointing these Officers of Parliament are not uniform. Nonetheless, apart from the Canadian Human Rights Commissioner, all the executives of these agencies are appointed using a procedure that requires approval by at least the House of Commons. For example, the Auditor General is appointed by the Governor in Council by commission under the Great Seal, after consultation with the leader of every recognized party in the Senate and the House of Commons and approval by resolution of the Senate and the House of Commons: *Auditor General Act*, R.S.C. 1985, c. A-17, s. 3(1); a similar procedure is used to appoint the Commissioner of Official Languages: *Official Languages Act*, R.S.C. 1985, c. 31 (4th suppl.), s. 49(1); for the Privacy Commissioner: *Privacy Act*, RS..C. 1985, c. P-21, s. 53(1); the Information Commissioner: *Access to Information Act*, R.S.C. 1985, c. A-1, s. 54(1); the Conflict of Interest and Ethics Commissioner, *Parliament of Canada Act*, R.S.C. 1985, c. P-1, s. 81**(**1); the Commissioner of Lobbying: *Lobbying Act*, R.S.C. 1985, c. 44 (4th suppl.), s.4.1(1); and the Public Service Commissioner: *Public Service Employment Act*, S.C. 2003, c. 22, s. 4(5). The Chief Electoral Officer is appointed by resolution of the House of Commons: *Canada Elections Act*, S.C. 2000, c. 9, s. 13. Finally, the Human Rights Commissioner is appointed by the Governor in Council, and may be removed only by the Governor in Council on address of the Senate and the House of Commons: *Canadian Human Rights Act*, R.S.C. 1985, c. H-6, s. 26(1) and (4).

200 *Id*.

> Parliament. It also emphasizes their independence from the government of the day. These "Officers of Parliament" carry out duties assigned by statute, and report to one or both of the Senate and House of Commons. The individuals appointed to these offices perform work on behalf of Parliament, and report to the chambers, usually through the Speakers.[201]

Finally, to set their duties apart, which they must carry out independently from the executive, the Officers of Parliament of these oversight agencies report directly to Parliament on their annual activities (and not to a minister, as is the case for the decentralized organizations). Furthermore, they may inform Parliament (and thereby the media) at any time of any problem they consider to be urgent. This extraordinary power is fundamental, because thanks to it these executives can make a real contribution to the effective operation of the parliamentary system. As we know, the proper functioning of Parliament depends on a whole range of constitutional customs and conventions, which are effective only if the government respects them. Hence, in parliamentary tradition, Officers of Parliament work in "independent accountability agencies created to assist Parliament in holding ministers and the bureaucracy accountable and to protect various kinds of rights of individual Canadians, or to carry out certain functions independent of the executive". This is why the holders of these positions report to Parliament and not the government (or a particular minister).

However this institutional consistency is not perfect. The idea of instituting a national integrity system is intended to make it possible to exercise continuous oversight of government activities in certain very targeted sectors. Also, to assign the mission for this to agencies attached to Parliament makes sense in terms of the way the government is organized. These public offices are listed in Part II of the *Federal Accountability Act,* which is entitled "Supporting Parliament".[202] However it is also the mission of two of these "parliamentary oversight agencies", including the one with which we are concerned – the Office of the Privacy Commissioner (the other is the Canadian Human Rights Commission) – to oversee activities in the private sector in their sphere of jurisdiction. The issue that arises here is whether this choice made by Parliament ought to be called into question.

2.2.2 Oversight of private-sector activities

Was it institutionally consistent to assign the Privacy Commissioner responsibility for overseeing non-governmental activities? We will examine two arguments: one in favour, the other not in favour. Second, we will review the categories of decentralized organizations in order to shed some light on

201 *Id.*

202 *Federal Accountability Act*, *supra,* note 197, s. 109 ff.

the type of organization that might be entrusted with the administration of PIPEDA in the event that the Privacy Commissioner is relieved of that responsibility.

2.2.2.1 Two arguments for maintaining the OPC's jurisdiction with respect to PIPEDA

The question of whether the administration of PIPEDA should or should not remain under the auspices of the Office of the Privacy Commissioner is a topic of debate. Of course, many responses could be given to this question, depending on one's theoretical perspective. Our aim here is not to exhaust all possible arguments, but simply to examine a few of them, with a view to stimulating discussion.

For example, one might feel that the Office should remain in charge of overseeing the administration of PIPEDA. Certain pragmatic arguments can be made in support of this choice. A first one might be *institutional expertise*. There is no question that the Office has acquired considerable experience since being entrusted with oversight of PIPEDA. There is also no question that its previous experience in enforcing the *Privacy Act* has been of invaluable assistance in enforcing PIPEDA. Next, one could also argue the indivisibility of the subject being legislated. The protection of personal information raises similar problems in the public sector and the private sector. Lastly, the argument of the risk of normative inconsistency could also be made. If two different agencies are made responsible for overseeing the protection of personal information in each of the sectors, incompatible solutions could be the result.

On the other hand, if we perceive the role of a parliamentary ombudsman such as the Office of the Privacy Commissioner to be to act as Parliament's aid (to support parliamentary business, as mentioned in Part II of the *Federal Accountability Act*), it would seem inconsistent for it to be entrusted with overseeing activities that do not fall within the purview of Parliament. In fact, Parliament is in a way the perfect oversight body for the government's activities. It is at the top of the pyramid. When the Office of the Privacy Commissioner oversees the administration of the *Privacy Act*, it is clearly supporting Parliament in the execution of a task that Parliament itself cannot perform (for lack of time and expertise), but which nonetheless clearly falls within its institutional mission. However, when one asks the Office to monitor whether the private sector is protecting personal information as it ought to, the link between that private mission and the public mission of Parliament is not at all evident. Therefore, a division of tasks between two separate agencies would seem more coherent in terms of the organization of the functions and powers of government institutions.

However, whatever arguments may have been used in the past, or might be used in the present or future, to justify extending this mandate to the Privacy Commissioner, those arguments should still be given thorough examination, particularly since this type of question has yet to be dealt with in Canadian law. Even if there were real objections to assigning jurisdiction over privacy to two separate agencies, it would be necessary to explore every possible avenue

in order to avoid facile solutions. In the parliamentary and legal traditions of the common law, too often institutions are created as an ad hoc response to the emergence of problems. Solutions are proposed without giving serious consideration to such factors as the institutional coherence of the state, making any large-scale process of reform extremely difficult to carry out.

Keeping future reforms in mind, this seems to us a question that should not be ignored. Before taking legislative action, it would be very helpful, if not necessary, to carefully distinguish between what is feasible and what is desirable, especially if the final objective is to develop a genuine national integrity system. For example, it would be difficult to reconcile the idea that within a single agency – the Office of the Privacy Commissioner – there can co-exist within a single person an Ombudsman responsible for enforcing the *Privacy Act* and a decision maker responsible for ruling on violations of and ordering penalties under PIPEDA, without the legitimacy of the differing treatment being constantly challenged, thereby undermining the institution's credibility over the long term. This is particularly true if the statutory violations committed by the government and the private sector were to be essentially of the same nature.

An initial solution would be to treat statutory offences the same way whether they are committed by the public sector or the private sector, to merge the two legislative regimes into one, and to provide the Commissioner's office with the financial and human resources to implement this new mandate. However, this solution could be seen as creating additional difficulties. The resources that would have to be invested for the Canada-wide implementation of this new mandate could reach colossal proportions. A second solution would be to create two separate agencies. For example, if at the end of deliberations on possible amendments to PIPEDA it was concluded that criminal powers had to be assigned to the public agency charged with its implementation, would it not be preferable to detach that agency from the Office of the Privacy Commissioner? This solution would have the advantage of being more institutionally coherent. In fact, the way that our public administrations are presently organized in Canada, the task of overseeing the private sector normally falls to decentralized organizations.

2.2.2.2 Categories of decentralized organizations

To situate the discussion, a reminder of the three main categories of decentralized organizations will be helpful.

- **Administrative commissions**

These commissions differ from the other categories in that often they carry out only one type of function: administrative (such as inspection, investigation, price monitoring, public information and education, etc.). They may also exercise a few decision-making functions. The power they are most frequently assigned in this regard is the power to rule on complaints. Often the functions of administrative commissions and parliamentary agencies that oversee government activities are the same. What distinguish them are the subjects and entities monitored (private or public). In the case of implementation of

PIPEDA, no value would be added by creating an administrative commission distinct from the Office of the Privacy Commissioner yet with essentially the same powers as those now held by the Office. Hence this avenue is not particularly compelling in terms of either effectiveness or efficiency.

- **Administrative tribunals**

Strictly speaking, administrative tribunals have only one function: to make individual decisions (e.g. the IRB, Pension Tribunal, Veterans' Board). So far as we know, no serious consideration has been given to the option of assigning oversight of PIPEDA to an administrative tribunal in the sense used here. Of course, it would always be possible to create two integrated agencies (a commission and a tribunal), employing something like the structure created to implement the *Canadian Human Rights Act* (Human Rights Commission and Human Rights Tribunal). But this avenue would add a new batch of difficulties (some of them constitutional). In this context, the scope and limitations of PIPEDA would have to be thoroughly reconsidered.

- **(Economic or social) regulatory agencies**

These agencies are different because of the fact that they perform three functions: administrative (like the administrative commissions), decision-making (like the administrative tribunals), and lastly, regulatory. It is the regulatory function that justifies classifying an agency as a "regulatory agency". Some examples in the category of *economic* regulatory agency are the Canadian Grain Commission,[203] the CRTC,[204] and the National Energy Board.[205] An example of a *social* regulatory agency is the Industrial Relations Board.[206]

If the application of PIPEDA were to be assigned to a decentralized organization, there is no question that a *social* regulatory agency might be the most interesting option, as it would permit reflection on the protection of personal information on a much more comprehensive level. Since all of the powers can be assigned to it, it can act in a manner similar to an ombudsman (which is mainly conferred administrative functions, like the administrative commissions), an administrative tribunal (should one wish to assign it order-making powers) and a social regulatory agency (in that it could exercise powers of a regulatory nature, in the form of policies or regulations).

Finally, the appeal of this type of agency is that it can investigate and identify violations of the law or the regulations it prescribes. Furthermore, it

203 *Canadian Grains Act*, R.S.C. 1985, c. G-10.

204 *Canadian Radio-television and Telecommunications Commission Act*, R.S.C. 1985, c. C-22.

205 *National Energy Board Act*, R.S.C. 1985, c. N-7.

206 The Canada Industrial Relations Board is instituted by the *Canada Labour Code*, R.S.C. 1985, c. L-2.

is interesting to note that in federal administrative law (and also provincial law, particularly in Quebec with the creation of the Autorité des marchés financiers, or even at the federal level with the proposed establishment of a Canadian securities regulator), there is a trend toward the power to sanction contraventions of the law.

2.2.2.3 Choice of type of decentralized organization

Although current knowledge about the missions, powers and functions of decentralized organizations is rather limited, especially in federal administrative law, it may be helpful to mention that, to our knowledge, there are no decentralized organizations in categories 1 (administrative commissions) and 2 (administrative tribunals) on which Parliament has conferred powers to impose penalties (fines) upon a finding by an employee of such an organization that there has been a contravention of the law. The only exception to this principle that we have found in federal law is in the *Employment Equity Act*.[207] The mechanism works as follows: upon a finding of a violation of the Act, the minister may issue a notice of monetary penalty (constituting a violation of the Act but not an offence under the Criminal Code: s. 35(3)). The employer may contest this notice before the Human Rights Tribunal. Hence this is a procedure whereby an administrative tribunal is involved in the sanction process, but only after the minister has first found a violation of the Act and decided to impose a monetary penalty. Therefore we are still a long way from a sanction mechanism directly administered by a decentralized organization, which the minister himself may be in charge of (See Appendix A for the relevant clauses of the Act).

However, we note that the Quebec Human Rights Tribunal has the power under section 49(2) of the *Charter of Human Rights and Freedoms* to grant punitive damages for the unlawful and intentional interference with a quasi-constitutional right protected by that Charter.[208] It is interesting to note the existence of this power in the context of implementation of a quasi-constitutional statute because, as we will mention later on, the protection of personal information may now have achieved the status of a quasi-constitutional right.

Normally, the punitive regimes that one finds in incorporating legislation – which these two types of agencies are responsible for applying – are administered by judges upon finding *offences* under that legislation. The term "offence" in a law triggers the criminal law procedure (normally on summary conviction). At that point the protections of the criminal law are applicable, and it is judges in courts of law who have to make a finding of guilt and impose a sentence.

207 *Employment Equity Act*, S.C. 1995, c. 44, Part III (Monetary Penalties), s. 35 ff.

208 *Charter of Human Rights and Freedoms*, R.S.Q., c. C-12, s. 49.

On the other hand, certain criminal powers are conferred to the benefit of economic or social regulatory agencies (category 3). Such devolutions of power are not unknown in federal administrative law. For example, in 2005 Parliament passed an amendment to the *Telecommunications Act* authorizing the CRTC to impose administrative sanctions (see Appendix B for the clauses of the Act). It would be interesting to learn more about the justifications for this legislative change, which is a turning point, at least in federal legislation, for the punitive role that certain decentralized organizations, such as an economic regulatory agency like the CRTC, can play in the oversight process for public legislation. Granting criminal powers to decentralized organizations is in fact a relatively recent idea in federal administrative law, and it seems to have yet to pervade federal law on a large scale. Therefore, more thorough research should be conducted to better understand the emergence of this phenomenon.[209] For now, legal justifications could be offered to support the assignment of this type of power based on the emergence of other normative values and systems.

2.3 The legal dimension: Emergence of other normative values and systems

Since the passage of PIPEDA, developments in new information technologies have revolutionized and continue to revolutionize access to knowledge. Their potential uses are constantly growing, raising the question of the limits, particularly the legal and ethical limits, that should be put on their application.

All these changes profoundly alter our concept of the world, and the fundamental question that arises is whether previous models are still consistent with these new realities. Some believe that these changes require the Canadian government to intervene to offer more protection; others disagree.[210]

In this section, we examine the changes taking place in the legal sphere that result, at least in part, from these technological advances and impact the effectiveness of personal information protection legislation. These changes are of interest because they allow significant modifications to the design of the existing normative systems, particularly with a view to offering greater privacy protection to citizens.

First, we look at the evolution of ideas in Canadian constitutional law, which, if they were fully implemented, would profoundly alter the legislative design of personal information protection. Second, we examine the emergence of new supranational normative systems (known as global administrative law) for

209 Anne-Marie BOISVERT, Hélène DUMONT and Alexandre STYLIOS, "En marge de l'affaire Norbourg: les enjeux substantifs et punitifs suscités par le double aspect, réglementaire et criminel, de certains comportements frauduleux dans le domaine des valeurs mobilières," available online on the Papyrus site of the Université de Montréal, at this address: http://hdl.handle.net/1866/2913. This is an advance publication. The final text will be published in "Dérives et évolutions du droit pénal," *Les Cahiers de droit* – special issue to appear in 2010.

210 Gautrais and Trudel, *supra* note 136.

protection of this personal information. These normative systems have appeared in response to the problems created by the use of new information technologies, and with a view to offering more effective protection against abusive uses of personal information. In effect, it was observed that it was difficult to offer an adequate level of protection through national legislation exclusively. The construction of this global administrative law has made possible the emergence of a vast network of standards and institutions interconnected by the objective of "protection of personal information".[211]

2.3.1 The evolution of constitutional law

Canadian constitutional law is undergoing a transformation, in terms of organization as well as individual rights and the division of powers. Earlier, we discussed changes made on the organizational level through the establishment of a national integrity system (other changes in the legal landscape result from fundamental questioning with regard to the guarantees of independence that should be established for administrative judges, and so forth). In this section, we look more specifically at the changes in constitutional law pertaining to basic human rights and the division of legislative powers.

With regard to the first issue, the discussion will address the hierarchical status of the right to privacy. The argument here is as follows: if the right to privacy has higher status than a simple civil right, could that status be used to give a more solid constitutional foundation to federal government actions in this area and, consequently, to PIPEDA? As everyone knows, the two levels of government are obligated to protect a fundamental right, and this has necessarily had effects on the scope of existing powers, even if it cannot have the effect of modifying them.[212] Often times, legislative jurisdictions over a fundamental right cannot be exclusive to one level of government, since otherwise the protection may be totally or partially ineffective. In this context, it becomes important to fully understand the foundation of the right to the protection of personal information.

However, this discussion would be pointless were it not for another change in constitutional law. This is the shift from a formal interpretation of the division of powers to a functional one. Although this new interpretive theory has not been officially endorsed by the Supreme Court (in this regard, we must monitor

211 Key Centre for Ethics, Law, Justice and Governance, Griffith University et Transparency International Australia, *Chaos or Coherence? Strengths, Opportunities and Challenges for Australia's Integrity Systems: National Integrity Systems Assessment (NISA) Final Report*, 2005, accessible online at the following address: http://www.griffith.edu.au/arts-languages-criminology/key-centre-ethics-law-justice-governance/research/integrity-anti-corruption/projects/?a=37155 (last visit: January 20, 2010).

212 In principle, the Charter does not impact the division of powers, but this assumption is questionable. Nonetheless, the Supreme Court maintains that the adoption of the Canadian Charter has not changed federalism or the rules governing the division of powers: *R. c. Turpin*, [1989] 1 S.C.R. 1296.

the Court's decision with regard to the federal securities bill), it is being explored by Canadian theorists, at least in certain areas where the division of powers is unclear (the interaction between sections 91.2 (federal power over trade and commerce) and 92.13 (provincial authority over property and civil rights)) or explicitly shared (concurrent jurisdiction in the areas of immigration and agriculture).

2.3.1.1 The protection of personal information: a quasi-constitutional right

Human rights are divided into two categories: fundamental rights and private law rights (which are social and economic in nature). Private law rights are protected by private law, and in this regard it is clear and incontestable that protection of personal information, as a component of the right to respect for privacy, is a private law right that is protected under Quebec civil law[213] and the common law in the other provinces of Canada. However, the status of this right appears to have changed, possibly during the 1990s. From a simple private law right it has acquired a higher status -- that of a fundamental human right.

In Canada, fundamental rights and freedoms are protected by enactments of a constitutional and quasi-constitutional nature. Among the constitutional protections, we must note to begin with that the *Canadian Charter of Rights and Freedoms* contains no specific provision on the right to privacy of every individual. At the end of the 1990s, however, the Supreme Court recognized that right as being included in the "Legal Rights" segment, and more specifically, sections 7 and 8, of the Charter.[214] However, we know that these sections are of limited application.[215] On the other hand, might this right be protected under rules of a quasi-constitutional nature? Before launching into this debate, it should be pointed out straightaway that use of the term "laws of a quasi-constitutional nature" means laws that are closely tied to the values and rights covered in the Constitution. However, the status of quasi-constitutional law does not have the effect of changing the traditional approach to statutory interpretation. It is nothing but an indicator to be considered when interpreting statutes: it is not in itself decisive. This clarification having been made, we must emphasize that federal law has evolved in favour of recognizing the quasi-constitutional character of laws designed to protect personal information.

---

213 *Civil Code of Quebec*, Title Two, Chapter III: Respect of Reputation and Privacy, at articles 35 to 41.

214 S. 7 of the Charter: *R. v. O'Connor*, [1995] 4 S.C.R. 411, *Cheskes v. Ontario*, 2007 CanLII 38387 (ON S.C.); s. 8: *Hunter v. Southam*, [1984] 2 S.C.R. 145.

215 *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, para. 65-66. Under s. 7, a law may deprive a person of the right to life, liberty or security of the person provided that deprival is in accordance with the principles of fundamental justice. And section 8 permits Parliament to make laws governing searches, provided they are not unreasonable. That said, a law on the protection of personal information does not involve the application of s. 7 or s. 8. What is more, the protections guaranteed by the *Canadian Charter of Rights and Freedoms* do not apply to the private sector. As a result, individuals' right to have their privacy respected by private companies finds no foundation in the *Canadian Charter*.

First of all, the *Canadian Human Rights Act* has been recognized as having quasi-constitutional status.[216] Although it has never contained provisions that pertain to respect for privacy, Part IV of the Act once contained certain legal guarantees relating to the confidentiality of personal information. This part was repealed in 1983[217] and replaced by the *Privacy Act*.[218] It was because of this legislative history of the *Privacy Act* that Noël J. of the Federal Court decided in *Canada (Privacy Commissioner) v. Canada (Labour Relations Board)* that, by virtue of its roots, the *Privacy Act* too is of a quasi-constitutional nature.[219]

In short, the *Privacy Act* is recognized as a fundamental law of the Canadian legal system. It belongs to that privileged category of "legislation which reflects 'certain basic goals of our society' and must be so interpreted 'as to advance the broad policy considerations underlying it'."[220] As pointed out by La Forest J. (in *Dagg*), it is a reminder of the extent to which the protection of privacy is necessary to the preservation of a free and democratic society,[221] and of "'the privileged, foundational position of privacy interests in our social and legal culture' (para. 69)." Therefore, if the *Privacy Act* has this status, can PIPEDA also be described as a law of a quasi-constitutional nature? As the purposes of these two laws are similar, a negative response might seem unusual, even if their scope or their effects are different. This in fact was the interpretation accepted by the Federal Court in *Eastmond* where the judge wrote: "I have no hesitation in classifying *PIPEDA* as a fundamental law of Canada, just as the Supreme Court of Canada ruled the federal *Privacy Act* enjoyed quasi-constitutional status".[222]

This judicial interpretation is consistent with the evolution of Canadian domestic law, but it also raises the question of the division of legislative powers in this area. In fact, offering effective protection to citizens nationwide will take concerted action by all levels of government (federal, provincial and municipal) that draws on all their strengths (for example: the federal government's financial resources, the provinces' understanding of regional characteristics and the municipalities' proximity to citizens and businesses). A vertical or silo-based approach to public governance does not offer a broad enough perspective to

216 *Canadian Human Rights Act*, S.C. 1976-77, c. 33.

217 S.C. 1980-81-82-83, c. 111 (Schedule IV, s. 3).

218 S.C. 1980-81-82-83, c. 111, Schedule II.

219 [1996] 3 F.C. 609, 652.

220 *Lavigne v. Canada (Office of the Commissioner of Official Language)*, [2002] 2 S.C.R. 773, para. 24. See also: *Canada (Attorney General) v. Viola*, [1991] 1 F.C. 373, 386 (Federal Court of Appeal); *Rogers v. Canada (Correctional Service)*, [2001] 2 F.C. 586, 602-603 (Federal Court).

221 *Dagg v. Canada (Minister of Finance), supra*, note 214; *R. v. Dyment*, [1988] 2 S.C.R. 417, 427; see also Joel FEINBERG, "Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?" (1982) 58 *Notre Dame L. Rev.* 445.

222 *Eastmond v. Canadian Pacific Railway and Privacy Commissioner of Canada*, [2004] F.C. 852, para. 100.

resolve problems such as those pertaining to personal information protection. Moreover, this observation was made, at least in part, since PIPEDA – as explained above – does not constitute a legislative model reflecting a strictly formal interpretation of the division of powers, but a hybrid model combining elements of both formalism and functionalism.

The question today is whether PIPEDA's hybrid model is suited to the new realities and can therefore offer the protection considered necessary to deal with technological advances and their many uses. This paradigm shift, which we are postulating for purposes of analysis, and the effects of which we can measure more effectively today (both on our lifestyles and on our values and beliefs), provides a backdrop to the discussion that follows and helps better understand the evolution of Canadian federalism. In fact, Canadian federalism was already moving, at least with respect to the hybrid model used in the area of personal information protection, towards a more extended functional interpretation of the division of legislative powers.

2.3.1.2 Functional interpretation of the division of legislative powers

A reflection of its time and the political tensions and economic realities of that era, the *British North America Act, 1867*, gave rise to a long tradition of interpreting the division of federal and provincial powers vertically. Out of respect for the "spirit of federalism", the powers were divided among either level of government, avoiding to the extent possible overlapping or legal confusion on legislative matters. However, the question arises: does this approach to federalism, both as an interpretive method and a political project, allow resolution of problems as complex as those pertaining to personal information protection and transborder data flows?

According to some authors, this dominant formalist approach to Canadian constitutionalism is not suited to the new knowledge economy. To perform more effectively on the international level, Canada needs to change to an interpretive approach allowing greater overlap between its levels of government. Such overlapping would be an opportunity to implement a networked federalism more in line with contemporary organizational systems. Rather than being a source of inefficiency and tension, well-developed networks would be conducive to innovation and cooperation among all levels of government: federal, provincial and municipal. This interpretive approach was specifically developed to allow greater contributions from municipalities.

The combination of globalization and the information revolution, says Thomas J. Courchene,[223] has led to the creation of a knowledge-based economy. Creativity, pragmatism, accessibility of information and flexibility of organizations are the watchwords of this new global order. Based on services

223 Thomas J. COURCHENE, "Global Future for Canada's Global Cities," in *Transitions: Fiscal and Political Federalism in an Era of Change*, Kingston, McGill-Queen's University Press, 2009, p. 263.

rather than exploitation of natural resources, the knowledge (or post-industrial) economy is organized around global city regions acting as economic drivers for their environments. The heart of the economy is found in these large cities since they alone offer sufficient density of human resources, the primary resources of the tertiary sector. Competing on the international level to attract the best elements of this "creative class," their ability to attract remains the main comparative advantage of a nation in the eyes of transnational companies and investors. In Canada, our major cities do not have any constitutional status and suffer from a chronic lack of financial resources. Moreover, their status as "creatures of the provinces" limits federal intervention in their regard. These factors limit their ability to compete successfully with other major cities, particularly their main U.S. and European competitors. This constitutional design, combined with the strong "territorial" culture of the different levels of government in Canada, represents a threat to our prosperity, according to Courchene and Stein.

The strategic importance of cities in a tertiary economy clearly illustrates the need for greater cooperation among the different levels of government. Canadian federalism, Stein tells us, "needs to be less defined, not more; less concerned with jurisdictional rights, not more; and much more focussed on results, on what we need to get done and how we can get there."[224]

More specifically, this absence of municipalities from the most important tables is contrary to the phenomenon of "glocalization". Glocalization consists of dual trends. First, the democratization of information technologies has made citizens more aware of the environment surrounding them and interested in participating in it. The main political entry point is therefore the local level, especially since cities are becoming, as mentioned, veritable city-states in the new world order. Second, the speed with which a knowledge economy operates, and the lack of distance on which it is based, contributes to the establishment of international and national standards. Whereas certain powers are shifting downward as a result of the first trend, others are now shifting upward. In the Canadian context, this phenomenon is very clearly visible in the areas of securities and privacy protection (two areas of debate arising from interpretation of the same sections of the constitution).

This dual trend clearly demonstrates, according to advocates of a more functional constitutional approach, the inevitable interdependence of the different levels of government. It would therefore be futile, even counterproductive, to try to disentangle each level's powers. On the contrary, the speed with which this new dynamic operates demands that the authorities develop more effective mechanisms that work just as quickly. Networked federalism, according to its supporters, is the organizational model most likely to meet these challenges.

224 Janice Gross STEIN, "Networked Federalism," in *Transitions: Fiscal and Political Federalism in an Era of Change*, Kingston, McGill-Queen's University Press, 2009, p. 347.

A. Networked federalism

What is networked federalism? How can it respond to the new economic reality more effectively? A network differs from a hierarchical system in that it does not represent a pyramid, but is composed instead of links and points corresponding to contacts maintained by representatives of different organizations working in the same area. Particularly effective for transmitting large amounts of information, a network allows the participants to communicate their information, ideas, and so on, without impediment. A lack of response from one of the points in the network does not prevent the information from continuing to circulate, in contrast to a hierarchical system where information is transmitted as if through a series of "locks". A network offers many entry points and an abundance of contributions.

A networked organization is highly decentralized and is not concerned with having a monopoly over its area of jurisdiction and practice. On the contrary, a network supports a culture of cooperation and circulation of information in order to multiply the entry points open to network users (citizens, businesses or members of the network). This multiplication of entry points allows almost instantaneous access to the information sought. The speed with which harmonized information can be accessed represents the main advantage of a network for its users; this gives a comparative advantage to the State adopting it.

The networked organization already seems to have proven itself in the private and parapublic sector where there is more pressure on stakeholders to adapt to their environment. It is also, according to Ronfeldt in his historiography of organizations, the most evolved form of organizational schema.[225] In short, Canadians have everything to gain from embracing this model, which is highly suited to the contemporary environment. In concrete terms, Canadian networked federalism would be reflected in, for example, the opening of secretariats in various government agencies and departments. Desirable in areas where there is overlap,[226] these secretariats would represent sites for sharing information and coordinating the development of legislation and its application. Universities, as well as experts from the private and parapublic sectors, would also be integrated into the network, always with a view to obtaining multiple contributions to solving increasingly complex problems.

Finally, the many debates surrounding the interpretation of sections 91.2 and 92.13 of the Constitution should be addressed in a completely different manner. A "silo-based" approach to these powers (securities, privacy protection, etc.) would give way to a less linear approach, operating "on several planes".

---

225 D.F. RONFELDT, *Tribes, Institutions, Markets, Networks: A Framework about Societal Evolution*. 1996, Santa Monica, CA: Rand.

226 Some jurisdictions that are clearly defined, such as national defence, are not conducive to the establishment of a networked federalism. See STEIN, *supra* note 224, 360.

Rather than investing significant amounts of energy in legal debates, governments, including the municipal governments, would approach these issues in a spirit of cooperation.

B. An interpretive posture that does not require constitutional amendments

The establishment of networked federalism does not require constitutional amendments or significant institutional changes. On the contrary, the debates surrounding sections 91.2 and 92.13 demonstrate the existence of the constitutional uncertainty needed to establish networks in certain strategic areas. Ironically, what has been a constitutional bone of contention for many generations now looks like a predestined entry point. According to advocates of networked federalism, we should embrace this "legal messiness" and take advantage of it. The establishment of networked federalism is more a matter of administrative organization than constitutional amendments, therefore. It is an interpretative posture gradually shaping our practices.

Although this approach can sometimes be observed already (for example, the cooperation between the federal Privacy Commissioner and her counterpart in British Columbia), there appear to be some obstacles to its generalization. These obstacles are primarily cultural, according to the authors, and involve, first, government officials and, second, the political elites.

First, Stein deplores the lack of trust among officials from the different levels of government, noting that the most effective networks are those based on good social cohesion. Bonds of trust and friendship among government officials, experts and universities are essential to greater cooperation among our institutions. Yet, since the federal cuts of the 1990s, Stein tells us, and probably longer than that in the case of Quebec, provincial officials have shown a significant lack of trust in their federal counterparts.[227] This lack of trust hinders the sharing of information, values and common objectives essential to the establishment of networked federalism.

Second, Stein believes that the view of intergovernmental relations held by our political elites represents the most serious obstacle to a functional approach to the constitution.[228] Canadian politics has been based too long on a system of confrontation among governments, with the main Canadian conversations revolving around matters of jurisdiction. Our leaders, according to Stein, will have to move from this culture of territoriality and control and adopt a discourse based on problem-solving and innovation.[229] This "letting go" represents the greatest challenge for our political elites in the 21st century and is essential to maintaining our competitiveness. Our elites must learn

227 See STEIN, *supra* note 224, 364.

228 *Id.*, 365.

229 *Id.*, 365.

to navigate a less defined and less linear federal system that focuses more on finding solutions.

In short, networked federalism, according to its advocates, represents the constitutional approach that is best suited to the 21st century. According to Stein, "a global economy rewards those who move sideways as well as up and down along the grid, with a large tolerance for fluid structures that give a quick response".[230] This approach to interpreting the division of powers could make it possible to respond more quickly to contemporary problems but also to the world crises that occur. One of these crises began with the events of September 11, 2001. The terrorist threat that has hung over the West since that day has led to the overhaul of many national security laws here and elsewhere. The United States has been particularly active in this regard through the strengthening of its legal systems in the area of national security. The *Patriot Act* represents a good example[231] since this law has created very strong points of tension between the United States' security needs and the need to protect the personal information of citizens, including our Canadian citizens and businesses. This example clearly illustrates the complexity of contemporary problems (legal, but also political and diplomatic) in this area of state intervention and the value of exploring networked federalism.

2.3.1.3 National security and personal information protection: points of tension

The *Patriot Act* was adopted in the wake of the events of September 11, 2001, to give more investigative powers to the government agencies responsible for combatting terrorism. This legislation modifies the *Foreign Intelligence Surveillance Act* (*FISA*) and, among other things, makes it easier for the FBI to obtain personal information held by U.S. companies. Although the American government was able to obtain personal information on Canadian citizens before 2001, the *Patriot Act* eased the process for obtaining warrants and expanded the definition of terrorism (extending it to, among other things, domestic terrorism).

This new conceptualization of the war on terror has resulted, in general, in a lowering of investigative criteria. The criminal procedural guarantees have been replaced, through various pieces of legislation, by a new category of more flexible guarantees established specifically for the war on terror, which leave more openings for transfers of personal data. These cross-border transfers of personal data represent a good example of PIPEDA's limits in the face of

230 *Id.*, 348.

231 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (*USA PATRIOT ACT*) Act of 2001, Pub. L. No. 107-56, 272, Stat. 218, online: http://www.govtrack.us/congress/billtext.xpd?bill=h107-3162&version=enr (consulted July 13, 2010), hereinafter referred to as the *Patriot Act*.

national security legislation. We will begin by examining some legal conflicts between the *Patriot Act* and PIPEDA.

The start of the 21st century was, as mentioned above, marked by an explosion of on-line exchanges and, above all, by the private sector's accumulation of a significant amount of personal information on their clientele. Vast databases were created, capable of reconstructing the daily habits of a citizen (including Canadian citizens) in one click. The *Patriot Act*, as a post-September 11 legal innovation, combined with the new economic model based on the accumulation of personal information, paved the way for increased surveillance by government agencies whose actions raise ethical problems. These ethical problems will be the subject of the next section.

A. Some legal conflicts between the Patriot Act and PIPEDA

The mechanisms put in place by PIPEDA to regulate the transfer of sensitive data to third parties appear to be ineffective with regard to application of the provisions of the *Patriot Act*. For example, the FBI can use a secret order from the FISA Court to force a U.S. company to turn over personal information. Such an order is now easier to obtain because the *Patriot Act* lowers the criteria required.[232] This has had the effect of neutralizing the prohibition against "fishing expeditions" in the area of search and seizure.

Consequently, the U.S. government can obtain the personal information of Canadian citizens through a U.S. company with a branch in Canada or a Canadian company transferring personal information to a third-party U.S. organization. Although this is nothing new – FISA dates back to 1978 – the *Patriot Act* extended the powers of U.S. agencies and facilitated their use. The secrecy now surrounding the disclosure of data to the U.S. authorities also complicates application of PIPEDA.

The companies targeted by a secret order obtained under the *Patriot Act* are also kept secret.[233] Moreover, these orders may have extra-territorial effect. For example, a U.S. company receiving such an order from the FISA Court could give the FBI information from a database held by a Canadian subsidiary to which it has access without informing the latter. In fact, to comply with U.S. law, the company would not warn its Canadian partner nor, of course, the Canadian citizen whose personal information it is disclosing. This type of intrusion into the private life of Canadians is described by Assistant Privacy Commissioner Heather Black as a threat to our national sovereignty and a

232 *Id.*, The FISA now states, "that a *significant purpose* of the surveillance is to obtain foreign intelligence information," whereas the previous wording of the criteria was "*the purpose*."

233 *Id.*, s. 215.

violation of PIPEDA.[234] It is difficult, however, to punish these violations of the law since these secret initiatives fall between the cracks of a system based on consumer complaints. The secrecy surrounding government actions with respect to national security therefore represent an obstacle to PIPEDA's application.

PIPEDA also appears to suffer from a lack of effectiveness with respect to national security legislation in situations where data are voluntarily transferred outside the country. The mechanism established to ensure protection of data transferred to another jurisdiction, namely, a system of contractual clauses that places the responsibility on the Canadian company, does not seem to be effective here.

Principle 1 of the Canadian legislation, pertaining to accountability, states that a Canadian company is responsible for the security of personal information transferred to third parties, particularly those located in another jurisdiction. Since PIPEDA cannot be enforced outside Canada, this obligation represents the cornerstone of the Canadian system of supervising international transfers of data. To meet this obligation, Canadian companies bind their foreign partners through contractual clauses guaranteeing certain data protection measures. Although these clauses may be effective within the private sector, they cannot prevent the competent authorities from ordering a U.S. company to disclose personal information. The U.S. company is required to comply with the *Patriot Act*.

PIPEDA's effects end therefore at the Canadian border. Once the data of Canadian citizens is transferred to the United States, the Canadian government cannot offer them any protection, apart from this system of contractual clauses penalizing companies that are subject to its jurisdiction. And a contractual stipulation cannot prevent a disclosure order authorized under national security legislation.

However, as the Assistant Privacy Commissioner notes, a company located in Canada must comply first and foremost with the Canadian legislation.[235] There are certain obligations established under PIPEDA that may be more effective in protecting the privacy of Canadians dealing with intrusive practices by foreign authorities.

In the first scenario, the secrecy surrounding the actions of the U.S. authorities should not prevent compliance with Canadian law. Principle 7 of PIPEDA states that Canadian companies should establish security safeguards that are appropriate to the sensitivity of the information held. These technological, organizational or physical mechanisms should protect the information from unauthorized access. It stands to reason that a foreign subsidiary secretly trying

234 H. BLACK, *11th Annual Meeting on Regulatory Compliance for Financial Institutions*. 2005, online: http://www.priv.gc.ca/speech/2005/sp-d_051118_hb_e.cfm (consulted July 12, 2010)

235 *Id.*

to access a database that originated and is located in Canada in order to disclose the information to its authorities falls into this category. In this connection, the decision *BC Government and Services Employees' Union v. British Columbia (Minister of Health Services)*[236] suggests four measures to prevent this type of foreign intrusion more effectively. First, a company should restrict and control electronic access by employees. Second, confidentiality obligations should be associated with substantial penalties. Third, whistle blowers should be protected. Finally, employees should receive training in respect of their legal duties.

As for the ineffectiveness of a contractual provision regarding a requisition under national security legislation, it is worth referring to the CIBC case to inform this debate. In 2004, CIBC Visa notified its credit card holders of a change in its policy of use. As it was now doing business with a new service provider located in the United States, the company warned its clients that their information could be disclosed to the U.S. authorities. This change of policy prompted a number of consumer complaints to the Canadian Privacy Commissioner, who investigated the company's compliance with PIPEDA. Analysis of the contract showed that all appropriate measure had been taken by CIBC and that the subcontracting company had been contractually obliged to put data protection mechanisms in place. Since such contractual clauses do not prevent the potential disclosure of information to the relevant authorities, the Canadian Commissioner found that CIBC had acted correctly in warning its clients of the possibility of such a scenario. Through this measure, the company was, in fact, complying with Principle 8 of PIPEDA, stating that an organization must inform clients about its practices for managing their personal information.[237]

Finally, the Assistant Commissioner notes that companies should be more proactive with regard to their knowledge of personal information transferred out of the country. In fact, given the ease with which sensitive data travels today, many companies are not fully aware of the extent of the data transfers they carry out. Being more knowledgeable about their practices could allow these organizations to put in place corporate mechanisms that are more effective and consistent with PIPEDA.[238]

Looking beyond piecemeal solutions, however, this example demonstrates the complexity of the contemporary problems associated with information protection, examined here through the lens of a balance between this right and the issue of national security. Taking as a starting point the premise that the right to protection of personal information is of a constitutional nature, this tension must be resolved "in a way that respects the imperatives both of

236 *B.C. Govt. Serv. Empl. Union* v. *British Columbia (Minister of Health Services)*, (2005) B.C.S.C. 446, online: http://www.canlii.org/en/bc/bcsc/doc/2005/2005bcsc446/2005bcsc446.html (consulted July 15, 2010)

237 BLACK, *supra* note 234, p. 6.

238 *Id.*, p. 7.

security and of accountable constitutional governance".[239] The implementation of networked federalism could, in this connection, supply interesting and innovative possibilities for future action, especially with regard to the role of education that could be played by the various levels of government (including municipal governments). Strengthening the government's role could also have particularly beneficial effects with respect to ethical problems, such as those arising from the interaction of the war on terror and the accumulation of personal information by the private sector

B. Some ethical problems arising from the interaction of the war on terror and the accumulation of personal information by the private sector

Gunasekara identifies three ethical problems arising from the interaction of the new legal conceptualization of the war on terror and the accumulation of personal information by the private sector.[240] First, the author notes that the tendency of governments to make the private sector its "partner" in the application of laws conflicts with the right to privacy. Citizens transmit their personal information to the private sector in order to obtain a service. Yet the information initially transmitted for that purpose is then disclosed to government agencies responsible for maintaining order and good government. Practices that co-opt the private sector in this way, developed and applied without the public's knowledge, constitute, according to the Privacy Commissioner, violations of the "most basic fair information practices".[241]

This partnership with the private sector, capable of providing government agencies with significant amounts of personal information, is even more alarming given the emergence of new intrusive technologies, such as "data mining". This practice consists in applying statistical models to databases to look for correlations among consumption habits in order to derive a list of potential terrorists. For example, through data on credit card use, airline ticket purchases or car rentals, these statistical models "add" information on a citizen's likely future habits to his or her profile. The most ambitious data mining project was the *Terrorism Information Awareness* (TIA) project established by the

---

239 *Charkaoui* v. *Canada (Citizenship and Immigration)*, [2007] 1 S.C.R. 350, par. 1: "One of the most fundamental responsibilities of a government is to ensure the security of its citizens. This may require it to act on information that it cannot disclose and to detain people who threaten national security. Yet in a constitutional democracy, governments must act accountably and in conformity with the Constitution and the rights and liberties it guarantees. These two propositions describe a tension that lies at the heart of modern democratic governance. It is a tension that must be resolved in a way that respects the imperatives both of security and of accountable constitutional governance."

240 G. GUNASEKARA, "The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows," (2007) 17 *International Journal of Law and Information Technology* 147.

241 CANADA, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. *Annual Report to Parliament 2003–2004*, 2004, p. 29, online: http://www.priv.gc.ca/information/ar/200304/200304_e.pdf (consulted July 14, 2010).

Pentagon in 2002. The objective of this project was to create a giant database using information collected by the private sector. This database would then be used to identify patterns associated with planning terrorist attacks.[242] Although this program no longer exists, many U.S. agencies are still conducting research of this nature, research that would be impossible without co-opting the private sector.

Gunasekara also discusses the blurring of the distinction between the legislative standards applicable in criminal matters and the standards developed in the context of the war on terror, which are less restrictive. In addition to the concerns of criminal lawyers that these lower standards will be applied to "ordinary" crimes,[243] there is a risk that the powerful tools granted to security agencies will be used for ordinary criminal investigations. In this way, personal information obtained without the traditional guarantees could be used for investigations into crimes that are not directly related to terrorism.[244]

Finally, Gunasekara warns us about the private sector taking over technological tools used by government agencies to combat terror.[245] Recalling the origins of the Internet, GPS and microwave oven, the author notes that military technological innovation has often served as a research and development laboratory for the consumer economy. For example, Gunasekara fears the day when powerful data mining software falls into the hands of the private sector, such as the insurance companies. In fact, this is already happening; those of us with accounts on social networks such as Facebook have already noticed how the ads on these pages are geared specifically to our needs. The promise of these public sector tools is, in short, an irresistible lure to the private sector. Strict application of privacy standards in their regard should therefore be a priority, concludes Gunasekara, to prevent them becoming a "Trojan Horse which once allowed within the city proved fatal to its liberty".

* *
*

242 GUNASEKARA, *supra* note 240, 158.

243 For example, the concept of facilitation, a type of preliminary offence created to fight terrorism, has already been extended to pedophilia in Canadian law. See the relationship between section 83.19 (terrorism) and section 172.1 (sexual assault of a minor facilitated by Internet communications) of the Criminal Code.

244 For more information on the scope of these surveillance, search and seizure powers and their impact on citizens' privacy rights, refer to the 2009 report by the Privacy Commissioner comparing anti-terrorism legislation in Canada, Britain, France and the United States: CANADA, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Surveillance, Search or Seizure Powers Extended by Recent Legislation in Canada, Britain, France and the United States*, 2009, online: http://www.priv.gc.ca/parl/2009/parl_bg_090507_e.pdf (consulted July 13, 2010).

245 GUNASEKARA, *supra* note 240, 163.

To summarize these developments in constitutional law, it is important to note the significant intellectual activity deployed by universities and legal and government institutions (including the Office of the Privacy Commissioner). The results of this intellectual activity serve as a basis for legal innovation aimed at resolving contemporary problems associated with new information technologies that throw open the doors to transfers of personal information among companies, and between companies and governments. Recognizing personal information protection as a quasi-constitutional right has the positive effect of offering greater protection to citizens and consumers. Likewise, the evolution of federalism to a more functional interpretation of our constitution could make it possible to implement a form of networked federalism in the future.

Of course, these legal changes are still in the embryonic stage and, although at first glance they appear to offer appealing solutions, these must nevertheless be subject to critical evaluation. A better understanding of the long-term consequences of these theoretical policies both on Canadian federalism and on individual rights and freedoms is needed. However, there is a strong movement towards the development of normative systems intended to protect personal information. In this connection, construction of a global administrative law on privacy protection has been ongoing for some years.

2.3.2 Construction of a global administrative law for the protection of personal information

Global Administrative Law represents an emerging field of law, which has been subject to systematic theorizing since 2005.[246] Starting from the observation that global governance can be understood as including regulation and administration, researchers have noted the emergence of a global realm of administration in which the strict opposition between domestic law and international law is being erased.[247] This realm is described by the word "global" rather than "international" so as to reflect the interweaving of domestic and international regulations.[248]

Global Administrative Law encompasses mechanisms, principles and practices, as well as their associated social codes, and its study includes the study of formal intergovernmental regulatory institutions, informal intergovernmental regulatory networks, and arrangements for the coordination of regulatory systems, national regulatory institutions acting in reference to an international

246 See the Global Administrative Law site of the New York University School of Law: http://www.iilj.org/global_adlaw.

247 Nico KRISCH and Benedict KINGSBURY, "Introduction: Global Governance and Global Administrative Law in the International Legal Order" (2006) 17:1 E.J.I.L. 1-13, 1.

248 *Id.*, 5.

intergovernmental regime, etc.[249] In this section, we will briefly describe the emergence of a global administrative law relating to the protection of personal information.

In this section, we briefly describe some normative networks for privacy protection that have been constructed in the last ten years. Study of these networks offers a wealth of information to advance our understanding of global administrative law and inspire legislative reform.

The first system is composed of a number of normative networks and clearly illustrates the establishment of harmonization and coordination mechanisms with general goals. The objectives of the second system are similar to the first, but its focus is more specific. This is the network of standards developed by the World Anti-Doping Agency. Finally, the third system, developed by APEC, establishes a legislative framework giving rise to the Pathfinder projects and the Cross-Border Privacy Rules system as well as a unique certification system.

2.3.2.1 The establishment of general harmonization and coordination mechanisms

Although there is no major international convention on transborder data flows and privacy protection as of yet, the network of supranational standards is largely based on the 1981 OECD Guidelines, which remains the core text that has drawn international consensus on data protection. This comment is important, because the issue of flows of transborder data and protection of privacy is still largely perceived as something that mainly concerns trade and commerce. Evidence of this is to be found in the free trade agreements that incorporate stipulations on privacy. Canadian examples include NAFTA,[250] and more recently, the free trade agreements between Canada and Peru[251]

249 Benedict KINGSBURY, Nico KRISCH and Richard B. STEWART, "The Emergence of Global Administrative Law" (2005) 68:15 Law and Contemporary Problems 15, 17.

250 *North American Free Trade Agreement between the Government of Canada, the Government of the United Mexican States and the Government of the United States of America*, December 17, 1992, [1994] R.T. Can. No. 2, entered into force on January 1, 1994, accessible online at this address: http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/nafta-alena/texte/index.aspx?lang=eng (last visit: March 20, 2010). Article 2105 discusses personal information but this is still an exception to an obligation to disclose rather than a guarantee of protection for personal information.

251 *Free Trade Agreement between Canada and the Republic of Peru*, May 29, 2008, entered into force on August 1, 2009, at art. 1507, accessible online at this address: http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/peru-perou/peru-toc-perou-tdm.aspx?lang=eng (last visit: March 20, 2010).

and between Canada and Jordan.[252] Mention should also be made of the Agreement between Canada and the European Community on passenger name records.[253] This agreement makes reference to the *Directive on the protection of individuals with regard to the processing of personal data*.[254] More interesting still is the development of a multitude of agreements of the "soft law" type. These agreements concern preliminary work done with a view to the negotiation of future agreements. Here we will briefly describe a few initiatives: the Spanish initiative, the APEC Framework, and the Galway accountability project. The primary function of these initiatives is to promote the development of harmonizing principles for personal information protection among States. The most recent initiative, the establishment of a Global Privacy Enforcement Network, focuses more on the effective enforcement of protection standards.

A. The development of harmonizing principles: the Spanish initiative and the Galway project

The Spanish initiative is the product of the international conferences of data protection and privacy commissioners, one of the principles of which is that "[t]he recognition of these rights requires the adoption of a universal legally binding instrument establishing, drawing on and complementing the common data protection and privacy principles laid down in several existing instruments and strengthening the international cooperation between data protection authorities".[255] Hence the commissioners' conference will consider its work completed once an international convention protecting personal information is published. In the meantime, the commissioners are developing tools designed to

252 *Free Trade Agreement between Canada and the Hashemite Kingdom of Jordan*, June 28, 2009, art. 15.4, accessible online at this address: http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/jordan-jordanie/agreement-toc-tdm-accord.aspx?lang=eng (last visit: March 20, 2010)

253 *Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data*, October 3, 2005, *Official Journal of the European Union* L 82/15 21.3.2006, entered into force on March 22, 2006, accessible online at the following address: http://www.canadainternational.gc.ca/eu-ue/assets/pdfs/031005PNR_eng.pdf (last visit: March 20, 2010). The preamble states: "HAVING REGARD to the relevant Commission Decision, pursuant to Article 25(6) of Directive 95/46/EC, (hereinafter the Decision), whereby the relevant Canadian competent authority is considered as providing an adequate level of protection for API/PNR data transferred from the European Community (hereinafter the Community) concerning passenger flights to Canada, in accordance with the relevant Commitments, which are annexed to the respective Decision;…"

254 *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, supra*, note 67.

255 *Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection*, document adopted in Strasbourg, October 17, 2008, and available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/08-10-17_Strasbourg_international_standards_EN.pdf (last visit: January 20, 2010).

encourage *rapprochement* between the laws on flows of transborder data in their respective countries.

The last conference, held in Spain in 2009, was the thirty-first, and it produced a *Joint Proposal for Setting International Standards on Privacy and Personal Data Protection.*[256] This proposal contains certain basic principles, rights and obligations deemed necessary by the conference commissioners for the effective protection of personal information. They are: lawfulness, fairness, purpose specification, proportionality, data quality, openness and accountability.[257] Some of these principles derive from the OECD Guidelines,[258] others from the European Directive.[259]

The Galway project focuses its normative efforts on ways to improve and clarify current legislation affecting businesses, with the objective of facilitating commerce.[260] As the participants are directing their attention to business practices, they are focussing on implementation of the principle of corporate accountability. On that subject, the participants are using the accountability principle in the OECD Guidelines as a foundation, while developing it so as to make it possible to harmonize practices with the standards promulgated in the

256 INTERNATIONAL CONFERENCES OF DATA PROTECTION AND PRIVACY COMMISSIONERS, Madrid, November 5, 2009. See the site: http://www.edri.org/edri-gram/number7.2/international-standards-data-protection (last visit: January 20, 2010).

257 *Id.,* art. 6-12.

258 ORGANISATION FOR ECONOMIC CO-OPÉRATION AND DEVELOPMENT (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, supra,* note 71; see in particular articles 8, 9, 12 and 14.

259 EUROPEAN PARLIAMENT AND COUNCIL OF EUROPE, *Directive 95/46/EC of the European Parliament and of the Council of Europe of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, *supra*, note 67, art. 6.1 and 7. [*Directive*] and proportionality principle. See the report on the directive: EUROPEAN COMMISSION, INTERNAL MARKET AND FINANCIAL SERVICES DIRECTORATE GENERAL, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data: annex to the annual report 1998 (XV D/5047/98) of the working party established by article 29 of directive 95/46/EC* (Luxembourg: Office of Official Publications of the European Communities, 1998).

260 "Global Discussion on the Commonly-accepted Elements of Privacy Accountability," Galway, Ireland, April 29, 2009. (Summary on the Galway conference) "While policymakers have provided the market with guidance on the structure of binding corporate rules and cross-border privacy rules, and basic principles about how to meet consumer privacy expectations are well established, little guidance exists about how companies might demonstrate their accountable use and management of personal information. International resolution of the elements of privacy accountability issues is especially important as the evolution of modern distributed business increasingly enables processing and accessing of data around the globe."

various statutes.[261] The difference between the Galway project and the Spanish Initiative is that the goal of the Galway Project participants is not to draft an international convention, but to harmonize the various laws and ensure they are continually updated.

In addition to harmonization, the supranational actors, and particularly the privacy commissioners for the OECD member countries, have noted that the dramatic increase in cross-border exchanges of data over the past decade makes enforcement of the existing legislation more difficult. In order to deal with the many new challenges created by the multiplication of national standards and their effective enforcement, the privacy commissioners for the OECD member countries met in Paris in March 2010, where they laid the foundation for a *Global Privacy Enforcement Network* (GPEN).[262]

B. Implementation of protection standards: the GPEN

The GPEN represents a new form of supranational cooperation for controlling transborder flows of data. In this section, we will summarize the debates and documents that gave rise to this plan, as well as the principles underlying it. We will also examine the scope and nature of the mechanisms proposed for the GPEN by its creators. We will see that the GPEN is not intended to replace the OECD Privacy Guidelines or promote standardization of national regimes, but rather to establish an organization for cooperation among the different privacy enforcement authorities, in order to promote enforcement of the legislation already in place. Finally, we will look at the first demonstration of this cooperation mechanism's effectiveness in the context of the Google Buzz case.

The GPEN is rooted in Paragraph 21 of the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* which states that "[the] Member countries should establish procedures to facilitate information exchange related to these Guidelines, and mutual assistance in the procedural and investigative matters involved".[263] Unlike other guidelines that emphasize the harmonization of standards, Paragraph 21 focuses more on cooperation among the different authorities to enforce domestic laws. This distinction is important since the underlying objective of the GPEN action plan is to

261 The Galway project identifies five elements of accountability: (1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria; (2) Mechanisms to put privacy policies into effect, including tools, training and education; (3) Systems for internal, ongoing oversight and assurance reviews and external verification; (4) Transparency and mechanisms for individual participation; and (5) Means for remediation and external enforcement.

262 A cooperation mechanism developed at the conference "30 Years After: The Impact of the OECD Privacy Guidelines."

263 OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, online: http://www.oecd.org/document/18/0,3343, en_2649_34255_1815186_1_1_1_1,00.html (consulted May 31, 2010).

improve the effectiveness of domestic regimes in dealing with problems associated with transborder data flows. According to the GPEN member commissioners, this objective will not be achieved through reform of the OECD Guidelines (dating from 1980), but by implementing a cooperation mechanism for joint action by the various privacy enforcement authorities. The thrust of this paragraph is therefore a decisive factor in the scope of this new network.

In 2007, an important step was taken with the adoption of the *OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy*. This recommendation, developed under the leadership of Canadian Privacy Commissioner Jennifer Stoddart, arose from a consensus on "the need to promote closer cooperation among privacy law enforcement authorities to help them exchange information and carry out investigations with their foreign counterparts".[264]

Although issued by the OECD member countries, the objective of this recommendation is the creation of a new instrument with global scope, or "the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement cooperation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns".[265] This recommendation therefore begins from the position that "effective enforcement cooperation can be accomplished despite variations in domestic approaches".[266] Modeled on the *Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* [C(2003)116] and the *Recommendation on Cross-border Cooperation in the Enforcement of Laws against Spam* [C(2006)57], the 2007 text contains four recommendations:

1) Improve their domestic frameworks for privacy law enforcement to better enable their authorities to cooperate with foreign authorities.
2) Develop effective international mechanisms to facilitate cross-border privacy law enforcement cooperation.
3) Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.

264 OECD, *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, 2007, online: http://www.oecd.org/dataoecd/43/28/38770483.pdf (consulted May 31, 2010), p. 4.

265 *Id.,* p. 11.

266 *Id.*, p. 5.

4) Engage relevant stakeholders in discussion and activities aimed at furthering cooperation in the enforcement of laws protecting privacy.

This recommendation lays the foundations for the discussions that took place at the conference held in Paris (mentioned above) and these four principles were explicitly reviewed and incorporated into the GPEN Action Plan. A number of participants who have worked or are working within public and private organizations discussed the founding principles of the Privacy Guidelines and their effectiveness with regard to contemporary challenges. Pursuant to these discussions, the following consensus was reached:[267] despite the sustained technological innovation of the past thirty years, the guidelines adopted in 1980, by virtue of their flexibility and technologically neutral terms, do not require extensive reform. The challenge lies rather in improving the *enforcement* of the domestic regimes stemming from these guidelines. Since transborder data flows have increased significantly in recent years, authorities must now handle many cases whose effects extend beyond their borders. Improved enforcement of the legislation will therefore come through closer cooperation among the relevant authorities.

This cooperation, according to the action plan, consists in sharing information about privacy enforcement issues and the approaches used (effective investigative techniques and legislation, etc.) to deal with these issues. It also provides for a mechanism intended to facilitate dialogue with the private sector and facilitate effective cross-border privacy enforcement by creating a contact list of privacy enforcement authorities interested in bilateral cooperation in cross-border investigations.[268] More specifically, the GPEN seeks to establish a Secretariat responsible for operating a website, coordinating public education campaigns and making information on the different domestic regimes available to the member authorities. The establishment of this Secretariat is a noteworthy initiative since, with the exception of the working groups of such regional organizations as the OECD and the annual conferences of competent authorities, no international body for cooperation in this area exists at this time. Moreover, the GPEN members intend to take part in periodic conference

---

267 Jane HAMILTON, *30th Anniversary of the OECD Privacy Guidelines, Remarks by Jane Hamilton, Industry Canada*, online: http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html (consulted May 31, 2010); Peter HUSTINX, *Recent Developments in the European Union*, 2010, online: http://www.oecd.org/ findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html (consulted May 31, 2010); Michael KIRBY, *The History, Achievement and Future of the 1980 OECD Guidelines on Privacy*, 2010, online: http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_2_1,00.html (consulted May 31, 2010); Hugh G. STEVENSON, *30 Years After: The Impact of the OECD Privacy Guidelines, Remarks of Hugh G. Stevenson*, 2010, online: http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html (consulted May 31, 2010).

268 OECD, *Action Plan for the Global Privacy Enforcement Network (GPEN)*, 2010, p. 1 and 2

calls and meetings. This new network intends to concentrate its efforts on the challenges affecting the private sector, but does not exclude cooperation regarding personal information held by the public sector.[269]

The GPEN hopes to restrict itself to the practical aspects of international cooperation. Its mandate does not include taking a position on matters of public policy.[270] Furthermore, although it is an initiative of the OECD countries, the GPEN is open to any country that wishes to participate, and more than one privacy enforcement authority from each country may participate. Finally, the GPEN action plan does not create any legally binding obligations. However, joint action by its members has already shown its effectiveness in the Google Buzz case.

In April 2010, the GPEN took one of its first actions, initiated by Commissioner Stoddart. After the introduction of Google Buzz, an application infringing the privacy of Gmail users, a number of privacy enforcement authorities, including the commissioners from Canada, Germany, France, the United Kingdom and several other countries, wrote a public letter to Google's CEO, reminding him of his legal obligations.[271] Although Google itself quickly withdrew the service, this joint action clearly shows that these authorities can establish the balance of power and force large economic actors such as Google to retreat. Moreover, Michael Geist, Professor and Canada Research Chair in Internet and E-commerce Law at the University of Ottawa, saw this joint effort as a "major step forward toward the globalization of privacy enforcement".[272]

In short, it seems that the growing challenges arising from transborder data flows cannot be overcome solely through enforcement of the domestic regimes already in place, since these regimes end at their respective borders. However, the similarity of the standards established by many of these regimes, based on the OECD guidelines of 1980, enhance the potential for more effective cooperation among privacy enforcement authorities. The goal of the Global Privacy Enforcement Network, therefore, is to establish a system for more effective privacy law enforcement. Through a permanent agency coordinating efforts and increased cooperation among the member authorities, better protection of personal information transferred across borders now seems possible.

269 *Id.*, p.4

270 *Id.*

271 This letter can be read in full on the OPC Web site at: http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm (consulted May 31, 2010)

272 Michael GEIST, "Privacy Takes Step Towards Global Enforcement," 2010, online: http://www.michaelgeist.ca/content/view/4994/135/ (consulted May 31, 2010).

2.3.2.2 A normative network with a specific scope: the World Anti-Doping Agency

The World Anti-Doping Agency (WADA) represents a research subject in global administrative law that offers a wealth of lessons for the Office of the Privacy Commissioner. First for its institutional design, given its significant successes in the past few years, but also because of the methods used to protect the personal information of athletes in particular.

First, we will give a historical and institutional overview of WADA, as well as examining the mechanisms established to control and monitor doping practices in sport and exploring whether these mechanisms could serve as a model for improving PIPEDA's effectiveness. WADA and its founders have succeeded in achieving objectives that are collectively rational (and based on game theory) by strongly integrating the private stakeholders that they regulate. This integration into the framework of the anti-doping system is organized in the form of a pyramid. The national and international sports federations are the front-line actors and they must adhere to a clear and explicit normative framework, the *World Anti-Doping Code*, such that WADA can enforce a deterrence-based system of sanctions. This system seems to pay dividends. In addition, we will see that WADA's anti-doping successes are also attributable to its efforts at education. Second, we will explore the methods proposed by WADA to resolve the problem of personal information protection for athletes travelling outside their countries. Since the personal information collected for doping control is intimately linked to the athletes' most basic rights, WADA adopted international standards to ensure that no errors could occur.

A. Historical and institutional overview

The mission of the World Anti-Doping Agency is "to promote, coordinate and monitor the fight against doping in sport in all its forms".[273] This non-governmental organization stems from Paragraph 4 of the Lausanne Declaration of 1999[274] and represents a response to the Tour de France scandal of 1998. This declaration was signed by representatives of governments, non-governmental organizations, including many sports federations, and the athletes who participated in the conference. Initially financed entirely by the International Olympic Committee, WADA has been supported equally by governments and the IOC since 2002.

In 2004, to meet its international coordination objectives effectively, WADA adopted a *World Anti-Doping Code*, which was revised in 2009. All of the participating sports federations adopted this code at the 2004 Olympic Games in Athens. In 2005, the *UNESCO International Convention against Doping in*

273 WORLD ANTI-DOPING AGENCY, *About WADA*, 2010, online: http://www.wada-ama.org/en/About-WADA/ (consulted June 23, 2010).

274 This declaration can be read in full at: http://www.sportunterricht.de/lksport/Declaration_e.html (consulted June 23, 2010).

Sport was adopted to allow incorporation of the *World Anti-Doping Code* into domestic legislation.[275] To date, 141 countries have ratified this convention.[276]

The anti-doping system is therefore organized in the form of a pyramid, with WADA at the peak and the national sports federations at the base. The international federations are located in the middle of this pyramid. All are linked by the World Code. Article 20.3.2 states that national federations must adopt the code to be members of an international federation. Both the national and international sports federations are responsible for periodic testing and sanctions in case of violation of the Code (Articles 5 and 10). The decisions of these bodies may be appealed before the Court of Arbitration for Sport.[277] Sports federations are also responsible for promoting educational campaigns.

Governments, by signing the UNESCO Convention, undertake to respect the World Code's regulatory framework and model their legislation on its principles.[278] WADA, at the top of this pyramid, develops the regulatory framework and coordinates efforts to enforce the code (Article 20.7.1 of the World Code). These efforts may include establishing educational campaigns (Article 20.7.6), accrediting national laboratories (Article 20.7.4), promoting research and technological innovation in detection techniques (Article 20.7.6) and so on. The Agency may also take part in appeals of decisions by sports federations.

In short, WADA coordinates and provides resources to partners strongly integrated into the system. Their efforts make it possible to reach the athletes more effectively and explain the consequences of their actions to them. Moreover, the participation of the various stakeholders in development of the general principles underlying the fight against doping ensures their adherence and participation. Their commitment takes the form of the obligations set out in the *World Anti-Doping Code*.

- **The World Anti-Doping Code**

The *World Anti-Doping Code* is divided into three parts. The first part deals with doping control (Articles 1 to 17). It defines doping practices and the prohibited

275 UNESCO, *International Convention Against Doping in Sport* 2005, online: http://portal.unesco.org/en/ev.php-URL_ID=31037&URL_DO=DO_TOPIC&URL_SECTION=201.html (consulted June 23, 2010). Some countries are not able to ratify a document prepared by an independent NGO.

276 WORLD ANTI-DOPING AGENCY, *UNESCO Convention Reaches 140 Ratification Mark*, 2010, online: http://www.wada-ama.org/en/News-Center/Articles/UNESCO-Convention-Reaches-the-140-Ratification-Mark/ (consulted June 23, 2010).

277 COURT OF ARBITRATION FOR SPORT, *History of the CAS*, 2010, online: http://www.tas-cas.org/history (consulted June 23, 2010).

278 See, for example, *The Canadian Policy Against Doping in Sport* at: http://www.pch.gc.ca/pgm/sc/pol/dop/index-eng.cfm (consulted June 25, 2010).

substances. This section then puts in place procedures for testing and results management. The sanctions and administrative procedures (right of appeal, right to a fair hearing, etc.) are described next. It is in this section, specifically Article 14, that the confidentiality guarantees are explicitly set out.

The second part of the Code covers education and research (Articles 18 and 19). It is worth noting here that the Agency's anti-doping successes are explained in part by the effectiveness of the campaigns conducted by the various institutions linked by the Code. This effectiveness can be attributed to the involvement of private stakeholders in these campaigns. For example, at the last World Cup, FIFA joined WADA in its "Say NO! To Doping" campaign.[279] The pyramid shape described above can be seen here: a campaign is developed and coordinated by WADA, and a sports federation, in this case FIFA, carries out the campaign with the athletes. Article 19 sets objectives for anti-doping research to ensure compliance with the regulations. WADA is responsible for coordination among the different agencies and the dissemination of scientific findings (Article 19.3).

The third part of the Code sets out the obligations of all stakeholders, including private parties (Articles 20 to 23). One section is devoted to each type of stakeholder (the IOC, national sports federations, international federations, medical personnel, athletes, governments, etc.). In addition to allowing better coordination of efforts to fight doping, this normative framework serves as a basis for the deterrence-based system of sanctions instituted by the Code.

The issue of doping in sport may be analysed from the perspective of game theory: while it is individually rational for an athlete to practise doping, in order to improve his or her performance and gain a comparative advantage over his or her competitors, it is collectively irrational to tolerate these practices, insofar as the principle of fair play is an important value. It may even be considered to represent the spirit of sport.[280] However, it is difficult to prove subjective fault in disputed cases (since the athlete can easily plead ignorance of the treatments received). To fight doping as effectively as possible in this context, the authors of the Code chose to establish an objective standard of responsibility based on negligence and reversing the burden of proof (Article 10.5.1). It is therefore unusual for an athlete to escape his or her responsibility once the material elements have been proven (through a positive test result).[281] The athletes are therefore held personally responsible for any doping. They are the ones

279 WORLD ANTI-DOPING AGENCY, *FIFA Joins WADA's Say NO! to Doping Campaign during World Cup*, 2010, online: *http://www.wada-ama.org/en/News-Center/Articles/FIFA-Joins-WADAs-Say-NO-to-Doping-Campaign-during-World-Cup-1/* (consulted June 21, 2010).

280 This objection is explained in the section *Fundamental Rationale for the World Anti-Doping Code*. WORLD ANTI-DOPING AGENCY, *World Anti-Doping Code*, 2009, p. 14.

281 Olivier NIGGLI and Julien SIEVEKING, "Selected Case Law Rendered Under the World Anti-Doping Code," (2006) 20 *Jusletter*, p. 2.

who must "ensure that any medical treatment received in no way violates the applicable anti-doping rules".[282] This objective responsibility is accepted by the stakeholders, who think that too high a burden of proof with regard to guilty intent would make the fight against doping ineffective.

In addition to objective responsibility, the quasi-absent principle of proportionality of the sanction is one of the notable characteristics of this deterrence-based system. Suspensions, ranging from one year to a lifetime suspension, are generally automatic. Article 10.5 places strict limits on the consideration of specific circumstances in order to adjust a sanction. A violation of the Code therefore entails severe sanctions with the admitted intention of deterrence. Furthermore, the CAS states, in the Hondo decision, that "a more flexible interpretation of the said system that would, for example, allow for the mitigation of the sanction even in the absence of the specific circumstances provided for in Articles 264 and 265 RAD [Article 10.5 of the Code], could jeopardize the uniform application and effectiveness thereof".[283]

The voluntary adherence of international and national federations and athletes to the Code serves to support this punitive type of regulation. Judge Claude Rouiller notes, in his legal opinion on the compatibility of the Code with Swiss law and the proportionality principle, that an athlete who adheres to a federation that is a signatory to the Code "[translation] agrees, in a deliberate manner, that he or she may be the subject of an abrupt sanction".[284] This regulatory framework resembles a contractual obligation, where the contract constitutes the law of the parties. It is important to recognize this relationship, in the institutional design of the fight against doping, between a system of severe sanctions on one hand, and a legitimization of this system on the other hand through the voluntary adherence of private stakeholders to a clear and explicit regulatory framework. Judge Rouiller clearly summarizes the situation:

> [*translation*]
> The Code's aim is to completely eradicate doping, which is acknowledged as potentially fatal for the future of large sports competitions. Even if deterrence does not justify every means, the punitive system, which also takes on a general preventative role, must be in keeping with what is at stake. If the athletes themselves think, rightly, that this system is appropriate and necessary, that hardly leaves any room for criticizing it from

282 *Id.*, p. 4.

283 *UCI, WADA v. Hondo, Swiss Olympic*, CAS, January 10, 2006, par. 142, online: http://www.wada-ama.org/rtecontent/document/CASELAW_Hondo.pdf (consulted June 22, 2010).

284 Claude ROUILLER, *Legal Opinion on whether Article 10.2 of the World Anti-Doping Code is compatible with the Fundamental Principles of Swiss Domestic Law,* 2005, online: http://www.wada-ama.org/en/World-Anti-Doping-Program/Legal-articles-case-law-and-national-laws/Advisory-and-Legal-Opinions-on-the-Code/ (consulted June 22, 2010).

> the angle of proportionality as such, as ultimately embodied in Article 27 SCC."[285]

The problem of doping by athletes presents, to some extent, similarities with that of the protection of personal information held by the private sector. From the standpoint of game theory, there may not be enough incentives for a private company to comply with the regulatory provisions, while violations may have significant consequences for the free play of competition and consumer rights (the general interest). Effective regulation of the flow of data may therefore come through cooperation among the various stakeholders, to help identify the rational interests that should be pursued, and the implementation of more powerful systems of sanctions. However, some nuances are required with regard to WADA's system and its transposition to the context of PIPEDA.

A system based on deterrence is more likely to be accepted by private stakeholders when the collective objectives to be pursued are the subject of consensus. However, the consensus on the irrationality of the individual practice is much more significant in the case of anti-doping than with respect to personal information. In fact, the problem of doping in sport is viewed by most stakeholders in the very simple terms of "good" and "bad". It is easy to obtain the adherence of private stakeholders to a highly repressive system based on the principle of deterrence when such basic moral principles are involved. It is completely different in the case of PIPEDA, where various principles come into conflict (free enterprise, consumer confidence, a quasi-constitutional right, etc.).

Moreover, the sanctions applied under the *World Anti-Doping Code* do not involve economic consequences of the same order as in the case of companies subject to PIPEDA. Would a deterrence-based system for protection of personal information, involving severe sanctions, be accepted by the private stakeholders governed by PIPEDA? The answer to this question probably depends on the level of consensus reached on the collective objectives to be pursued.

In short, WADA's anti-doping successes may be attributed to an institutional design in which private stakeholders play an important role. Their integration into the system allows, in addition to a proximity essential to educating the members and applying the normative framework, the legitimization of a deterrence-based system of severe, but effective sanctions. Although some nuances are required for comparison with PIPEDA, it may be possible to transpose some of the practices of WADA and its institutional organization to that context.

B. Personal information protection initiatives

In this second section, our attention turns to WADA's personal information practices. WADA and its partners collect a significant amount of personal

285 *Id.*, p. 36–37.

information when conducting drug tests. Since these tests are often carried out at international events, the information gathered passes from one jurisdiction to another. Management of the results may also require the transfer of data across borders, as when, for example, results are transmitted from a national sports federation to WADA's headquarters in Canada. The fight against doping therefore involves constant transfers of personal data across borders.

At the urging of the European governments, WADA adopted the *International Standard for the Protection of Privacy and Personal Information* in order to set forth "a minimum, common set of rules to which *Anti-Doping Organizations* must conform when collecting and handling Personal Information pursuant to the Code".[286] This standard underlies the *World Anti-Doping Code* and the practices of its signatories. In accordance with the 1980 OECD Guidelines, its primary objective is to "ensure that organizations and persons involved in anti-doping in sport apply appropriate, sufficient and effective privacy protections to Personal Information that they Process, regardless of whether this is also required by applicable laws".[287] We will examine the rights and obligations set out in this international standard with a view to understanding the mechanisms established to handle the personal information of athletes in order to respect their privacy.

- **A security perimeter created by a minimum, common set of rules**

The International Standard establishes a minimum set of rules to guarantee protection of the personal information of athletes. Despite the legislative disparities between the States among which these data travel, all parties involved in handling these data are bound in some way by the rules set out in the International Standard.

According to its Article 4.1, an anti-doping organization acting in a State where the legislation is more flexible than the Standard must harmonize its practices with the standard (provided that such harmonization does not breach other applicable laws). An anti-doping organization that does not comply with these minimum restrictions may be prohibited from participating since the other organizations are required to report it to WADA and refuse to share personal information with it (Article 8.2). Furthermore, still with this objective of establishing an environment that provides harmonized guarantees of privacy protection for the athletes, anti-doping organizations must choose subcontractors (laboratories, IT service providers, etc.) that provide guarantees in respect of their technical security and organizational measures and ensure that such companies are contractually bound to protect the confidentiality of data (Articles 9.4 and 9.5). In all cases, the anti-doping organization

286 WORLD ANTI-DOPING AGENCY, *International Standard for the Protection of Privacy*, 2009, p. 1, online: http://www.wada-ama.org/en/News-Center/Articles/International-Standard-for-the-Protection-of-Privacy-Now-Online/ (consulted June 22, 2010).

287 *Id.*

remains responsible for protecting the personal information of the participants (including the athletes and the organization's employees). The International Standard thereby establishes a sort of security perimeter around the athletes, by binding all parties handling their personal information outside the sports federation.

To prevent the athletes' personal information from crossing this security perimeter, the Standard prohibits communication of data collected to third parties, unless the organization is required to do so by law, obtains consent from the relevant participant or is asked to do so by law enforcement authorities in the context of an investigation (Article 8.3). Since the International Standard represents a minimum set of rules, it does not conflict with more restrictive regional legislation. Anti-doping organizations operating in States with more stringent systems must comply with those higher standards (Article 4.2). This is the case, for example, for European anti-doping organizations. In fact, despite the initial fears of the Article 29 Working Group, it is now recognized by all that the Standard does not lower the legislative requirements of the European Union with respect to personal information protection.[288]

In short, the International Standard creates a sort of security perimeter around the athlete by establishing minimum standards for personal information protection and limiting the number of natural and legal persons that can access that information. Although the personal data collected by anti-doping organizations is transferred to different jurisdictions with varying, and sometimes divergent protection systems, ultimately it passes only into the hands of parties bound by the requirements of the International Standard.

- **Centralized information control**

The pyramidal structure of the anti-doping system is also seen with respect to personal information protection. Under Article 14.5 of the *World Anti-Doping Code*, national and international anti-doping organizations must submit all testing data and results to WADA. By centralizing the information, this measure helps to prevent duplication of tests and increase effectiveness, and to safeguard cross-border transfers of sensitive data. WADA has established a secure computerized system for access to its data, the *Anti-doping Administration and Management System* (ADAMS). This database is accessible to all signatories of the Code, from the national and international federations to the IOC, including the athletes themselves.

It goes without saying that access to data is limited by the type of stakeholder signing on. For example, an athlete can access his or her file on ADAMS in order to enter whereabouts information in case of surprise testing. A national

288 WORLD ANTI-DOPING AGENCY, *WADA Statement about the Opinion of European Working Party on Data Protection*, 2009, p.1, online: http://www.wada-ama.org/en/News-Center/Articles/WADA-Statement-about-the-Opinion-of-European-Working-Party-on-Data-Protection/ (consulted June 22, 2010).

anti-doping organization has access to data on athletes living within its jurisdiction. In the event that the organization wants information on a foreign athlete in order to plan testing at a sports event in its jurisdiction, it must obtain authorization from the athlete's national sports federation. The athlete will then be informed that his or her personal information is available – temporarily – to that anti-doping organization.[289]

WADA is committed, also under Article 14.5 of the Code, to producing annual reports on its data management and making itself available "for discussions with national and regional data privacy authorities". Finally, WADA, as well as its ADAMS system, comes under the jurisdiction of the Canadian Office of the Privacy Commissioner since its headquarters are in Montreal. It is therefore subject to regulation by the Office as well as the International Standard.

- **Other obligations of anti-doping organizations**

Certain other obligations are imposed on anti-doping organizations to ensure equal protection of data crossing borders.

First, anti-doping organizations shall process only information pertaining to drug tests, for the sole purpose of conducting such tests (Articles 5.2 and 5.3 of the International Standard). Because the activities of the anti-doping organizations are limited, it is easier to manage access to the ADAMS database, and guarantee minimal intrusion into the privacy of participants. Moreover, unless an organization is able to give valid legal grounds such as fulfillment of a contract or protection of a participant's vital interests, the participant must give consent before his or her personal information is processed (Article 6.1).

To give informed consent, the participant must receive certain types of information listed in Article 7.1. For example, the organization must disclose "other potential recipients of the Personal Information, including *Anti-Doping Organizations* located in other countries where the *Participant* may compete, train or travel" as well as "the purposes for which the Personal Information may be used and how long it may be retained". The participant thus retains some control over his or her personal information. Of course, a participant's refusal to participate in doping controls may entail certain sanctions (Article 6.3).

Finally, anti-doping organizations must establish safeguards to maintain the security of personal information. These safeguards may include "physical, organizational, technical, environmental and other measures" to prevent the disclosure of personal information (Article 9.2). Information considered "sensitive" (genetic, medical and legal information) must be the subject of a higher level of security (Article 9.3).

289 WORLD ANTI-DOPING AGENCY, *Questions & Answers on ADAMS,* online: http://www.wada-ama.org/en/ADAMS/QA-on-ADAMS-/ (consulted June 30, 2010).

Furthermore, anti-doping organizations must designate a "person who is accountable for [the organization's] compliance with this International Standard and all locally applicable privacy and data protection laws" (Article 9.1). This person must be readily available to the participants. Finally, anti-doping organizations are obligated to destroy personal information at the end of its useful life (Article 10).

In short, the *International Standard for the Protection of Privacy and Personal Information* provides equivalent protection to the personal data of athletes crossing from one jurisdiction to another.

2.3.3.3 APEC's Privacy Framework

Asia-Pacific Economic Cooperation (APEC) is a forum comprising 21 economies throughout the Asia-Pacific region. Operating by consensus, the objective of this group of States is to develop cross-border trade by adopting resolutions that are not legally binding. Given the strategic importance of personal information and differences in the laws of the member economies, APEC has sought, since 2003, to provide guides and tools to ensure the security of such data and thereby facilitate trade and commerce.

APEC adopted its Privacy Framework in 2005. Based on the OECD principles established in 1980, this regulatory framework represents a minimum "floor" for protection of information in the region. As with the Spanish initiative, this project is also the result of a conference that was organized by the Center for Information Policy Leadership and the Office of the Data Protection Commissioner. The participants of the conference were public office holders responsible for the protection of personal information in their respective countries and representatives from the business sector.

This framework has been highly criticized, and many view it as a watered-down version of the OECD Guidelines.[290] However, it should be noted that, just like the Spanish initiative, the APEC legislative framework is an agreement that includes many countries. The framework is not so much a legislative effort on privacy than it is an effort to harmonize and develop laws that facilitate corporate trade and commerce.[291] This is not a document designed to establish standards, but rather principles.[292] Links between the APEC principles and the principles of the OECD Guidelines are explicitly woven into the APEC Framework.[293] Moreover, although some member economies have passed

290 See, for example, the first part of Graham GREENLEAF, "Five years of the APEC Privacy Framework: Failure or promise?" (2009) 25 *Computer Law & Security Review.* 28.

291 ASIA PACIFIC ECONOMIC COOPERATION, *APEC Privacy Framework*, (2005) APEC#205-SO-01.2, art. 3.

292 *Id.*, art. 14-26.

293 *Id.*, art. 5.

stronger legislation in this regard, the practical effects of this framework on the other economies are limited by its non-binding nature.

In 2007, the Data Privacy Subgroup proposed the Pathfinder projects to control the security of data crossing borders. These projects, based on the principles in the *APEC Privacy Framework*, were inspired by the U.S. approach to data protection, the "Safe Harbor" framework. The Pathfinder projects establish certification mechanisms available to businesses. These "trustmarks", as the project calls them, assure consumers of the safety of their personal data in the hands of certified companies.

This certification-based approach relies on consensus and private stakeholders. It differs in this way from the European approach which proposes national legislation, harmonized with international standards, as well as the concept of "adequate legislation". We will therefore begin by examining the operation of APEC's Cross-Border Privacy Rules and Pathfinder projects. We will then look at the many criticisms made with regard to APEC's framework.

A. Pathfinder projects and the Cross-Border Privacy Rules system

The Pathfinder projects arise from application of the ninth principle underlying the *APEC Privacy Framework,* which pertains to accountability. Since 2006, representatives of the member economies have worked on nine projects, aimed at, among other things, establishing certification criteria for businesses and for the accountability agents themselves.

Under the Cross-Border Privacy Rules (CBPR) system, like the Safe Harbor model, a company voluntarily establishes a data protection system. Following self-assessment of its corporate system, a company may receive certification from a private agent or a government authority.[294]

APEC identifies four pillars supporting its CBPR system.[295] First, self-assessment: organizations develop rules and procedures that will protect personal information. Second, compliance review: an accountability agent ensures that the rules developed comply with the *APEC Privacy Framework* and other national and international documents that are legally binding in that jurisdiction. Some writers express reservations about the need for compliance with documents other than the APEC framework (or only a portion of it). We will return to the scope of the certification in the second section. Third, certification: APEC establishes a certification system, a "trustmark". Fourth, enforcement and dispute resolution: organizations establish procedures to respond to consumer complaints.

---

294 HUNTON & WILLIAMS LAW FIRM, *Background paper on APEC Privacy Framework Pathfinder Projects*, 2008, p. 3, online: http://www.hunton.com/files/tbl_s47Details/FileUpload265/2302/Bruening_APEC_Privacy_Framework.pdf (consulted July 5, 2010).

295 *Id.*

By establishing these pillars, APEC seeks to produce models for review, complaint resolution, organizational self-assessment and other mechanisms. These models can then be used by companies seeking to improve their effectiveness in this area. The CBPR system is similar to the U.S. approach, therefore, although this system focuses more specifically on the problems associated with international data transfers.

The nine Pathfinder[296] projects are designed to test this system through the development of clear criteria and practical experience. They represent the practical expression of the pillars described above.

> *Project 1: Self-assessment guidelines for business*
>
> This project will develop a standard self-assessment guidance document for organizations participating in the certification process. This document will enable companies to assess their internal data protection practices.
>
> *Project 2: Trustmark (accountability agent) guidelines*
>
> This project will develop the recognition criteria for public and private sector accountability agents. To be able to give APEC certification, agents must meet certain criteria for independence and impartiality in complaint resolution and have a process for reviewing compliance of organizations before and after their certification.
>
> *Project 3: Compliance review of organizations' cross-border privacy rules*
>
> This project will develop guidelines for accountability agents to use when assessing an organization's compliance with the *APEC Privacy Framework*. This project will create a standard process for review of corporate self-assessments.
>
> *Project 4: Directory of compliant organizations*
>
> APEC will eventually establish a directory of organizations that have been certified.

Projects 5, 6 and 7 will enhance cooperation among privacy protection authorities. These projects are based on the OECD advances in cooperation.

---

296 ASIA-PACIFIC ECONOMIC COOPERATION, *APEC Data Privacy Pathfinder Projects Implementation Work Plan -Revised*, Doc. off. 2009/SOM1/ECSG/SEM/027 (23 February 2009), online: aimp.apec.org/Documents/2009/.../09_ecsg_sem1_027.doc (consulted July 2, 2010).

Project 5: Directory of personal data protection authorities

APEC will establish a directory of relevant authorities in its member economies.

Project 6: APEC cooperation arrangement for cross-border privacy enforcement

This project will develop a cooperative arrangement between relevant authorities. On a voluntary basis, authorities will share information to facilitate investigations and enforcement of privacy rules. It seems that this cooperation project includes both government agencies in the member economies and accountability agents from the private sector.

Project 7: Template request for assistance form

This project will develop a template form for use by the different authorities when requesting assistance. This will ensure more effective identification of problems and their referral to the relevant party (an organization's internal complaint management system, private sector accountability agent, government data protection authority, etc.).

Project 8: Guidelines and procedures for enforcement procedures in the CBPR system

This project is linked to the preceding one, in that it will develop criteria and procedures for referring complaints to the relevant parties. The CBPR system will take the form of a pyramid, with different regulators assigned to different types of complaints.

Project 9: Pilot program to test and analyse the results of the preceding projects leading to the establishment of a complete system

Some member economies and companies in these economies have offered to test the CBPR system. In accordance with Project 1, they will submit a self-assessment of their personal data protection system. This self-assessment will be analysed by the accountability agents in accordance with the procedures in Project 3. The regulatory mechanisms in Projects 6 and 7 will then be tested to determine their effectiveness.

The member economies are free to participate in all, some or none of the projects. The International Chamber of Commerce, United States, Australia and Canada are the most enthusiastic participants. A number of economies

are participating in certain projects only, while others are content to act as observers.

B. A much-criticized approach

According to some authors,[297] APEC's traditional approach, operating by consensus and giving business a central role in developing a regulatory system, is not compatible with a certification system. The main criticisms revolve around the idea that criteria that are overly permissive or differ from one jurisdiction to another will create a certification system that misleads consumers seeking to do business with companies that provide adequate data protection.

- **Standards applicable to companies**

These authors have focused on Projects 1 to 3, pertaining to certification criteria for both companies and accountability agents and their relationship to the *APEC Privacy Framework*. They note, for example, that the standards against which the companies must assess themselves (Project 1) and which are used for the assessment of accountability agents (Project 3) have not yet been specified. Where member economies have not passed legislation with regard to these projects, they fear that a company's sole obligation will be to comply with the ninth principle in the APEC framework, which pertains to accountability, and that the *APEC Privacy Framework* will therefore represent the minimum desirable standard. This ninth principle, which they consider too vague, pertains specifically to cross-border data flows. It states that the company must either obtain the consumer's consent regarding such transfers or that it must "exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles".[298]

In light of the official documentation made public, consumers have similar fears. They wonder if certification will be limited to the APEC principles regarding cross-border transfers. According to the working documents for Projects 1 and 3, certain principles, such as limitations on data collection and the consumer's right to exercise choice in relation to use of his or her data may not be included in the APEC certification. If this scenario comes to pass, some commentators have expressed the opinion that companies could be included in APEC's

297 Graham GREENLEAF, "Five years of the APEC Privacy Framework: Failure or promise?" (2009) 25 *Computer Law & Security Review* 28.; N. WATERS, "The APEC Asia-Pacific Privacy Initiative – A new route to effective data protection or a Trojan horse for self-regulation?" (2008) *U. New South Wales Faculty of Law Research Series 2008, Working Paper 59*.

298 *Id.*, Greenleaf criticizes the wording of this principle, which does not provide clearer definitions of reasonable practices, seeing it as an opportunity for the first organization to release itself from its obligations to the consumer. It would be the same for the second organization, even if a clause bound the two companies with respect to appropriate data processing, at least in those jurisdictions where provisions for the benefit of third parties are not recognized.

directory of compliant organizations (Project 4) without being in compliance with all of APEC's principles. Moreover, in the case of data that does not cross borders, companies will not be bound by any of the APEC principles. The APEC certification may become a source of confusion in the minds of consumers and other business partners.[299]

- **Standards applicable to accountability agents**

Like Projects 1 and 3, Project 2 remains vague with respect to the standards with which agents must comply for certification. One problem identified is the following: what degree of impartiality can we expect from a company that "sells" its certification to other private companies, particularly when the time comes to resolve a conflict between a consumer and a company, the agent's client? Criticism of the model for certification by private agents dates back to the early 2000s.[300] At that time, Howes saw it as a system that was too "soft" and favoured business. Consumers will be the big losers, since the certification companies' sympathies and interests will be those of the companies that they are required to regulate.

In a 2008 study, Connolly paints a bleak picture of the model for certification by private agents. He claims that these agents' standards are lower than any national or international legislation and enforcement against delinquent companies is poor.[301] Here too, the author is sceptical of the independence guarantees given by private agents and sees this model as no more than a marketing operation that is potentially misleading for consumers.

In contrast, Project 2 does not pertain solely to private sector accountability agents. Giving government authorities the status of accountability agent is not ruled out. In such an eventuality, the national legislation of various countries, including Canada, could be amended to assign new powers to a public authority, such as the Office of the Privacy Commissioner. This avenue appears, at least at first glance, more promising from the standpoint of providing a public authority with greater impartiality in decisions with regard to certification requests.

299 Note, however, that the scientific literature raises questions in response to official documents released up until 2009. Since they are only working documents, these problems may be resolved prior to launching the certification program.

300 R. GELLMAN, "TrustE fails to justify its role as privacy arbiter" (2000) 25 *Privacy Law & Policy Reporter* (2000), online: http://www.austlii.edu.au/au/journals/PLPR/2000/53.html (consulted July 2, 2010); E. HOWES, *No guarantee of privacy*, 2002, online: http://spywarewarrior.com/uiuc/privpol.htm#no-guarantee (consulted July 2, 2010).

301 C. CONNOLLY, *Trustmark schemes struggle to protect privacy*, 2008, online: http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.pdf (consulted July 2, 2010).

The second problem is that of harmonization. Since APEC operates by consensus and the member economies seem to want to avoid harmonizing their laws, commentators wonder whether each economy will develop its own system for certification of private sector agents, making the foundations of the system unequal. Here, the question raised is whether it is possible to avoid harmonization of national legislation.

Despite APEC's certification approach, trying to bypass the European concept of "adequate" legislation (and the ensuing harmonization of legislation) through an approach based on the Safe Harbor model, Waters (2008) and New Zealand Assistant Commissioner Stewart (2003) believe that this concept of adequate legislation cannot be completely avoided.[302] In their view, no State can avoid assessing another State's certification process; it will have to judge the compliance of another economy's certification criteria for companies and agents with its own national rules.

Beyond these criticisms, Waters raises some positive points with regard to corporate self-assessments.[303] He believes that the level of self-assessments will go beyond what is required by domestic legislation, which is complaint-based and assumes the company's compliance with domestic laws. The self-assessment in Project 1 will, in contrast, go much deeper and be more systematic. Moreover, information provided by companies to accountability agents would be much more extensive and detailed than that provided under any other model, including the European legislation. However, the official documents do not tell us whether this information or a portion of it will be made public. Publication of these self-assessments, allowing civil society to conduct its own analysis, represents a potential solution to the problem of impartiality raised above.

Finally, as even the most sceptical commentators note, the issues outlined above can still be resolved before the APEC certification process is finalized. The future will show whether this certification constitutes a low-cost way for companies to reassure consumers without offering them the protection they think they are getting or whether it will be an original way of making companies more responsible. The first scenario would represent a severe blow to globalization of the Safe Harbor model. Such a system, of benefit to a handful of companies, would not resolve the problem of personal data transfers, and the participating countries, disappointed by this inconclusive approach, might consider turning to "adequate legislation" and the adoption of international standards.

---

302 WATERS, *supra* note 297; B. STEWART, *A suggested scheme to certify substantial observance of APEC Guidelines on data privacy*, APEC E-commerce Steering Group Meeting, 2003, online: http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2003.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2003/pdf.Par.0009.File.v1.1 (consulted July 5, 2010).

303 WATERS, *supra* note 297.

* *
*

To summarize this section on construction of the global administrative law pertaining to personal information protection, an initial observation can be made. These new networks of supranational standards are already well established and producing significant results in terms of compliance by the parties in question. While this brief description of the supranational initiatives to establish harmonization and enforcement mechanisms does not include every privacy protection initiative,[304] it is intended to show that we are witnessing a genuine supranational construction of an integrity system for privacy, including sets of standards and mechanisms with both general and specific aims. This system includes mechanisms for developing standards, intended to promote the adoption of harmonizing principles, as well as cooperation mechanisms, whose objective is more effective enforcement of privacy standards. To this integrity system are being grafted federal initiatives, namely PIPEDA, as well as provincial and territorial ones, but also initiatives by companies which are setting up mechanisms for handling consumer complaints. What is interesting about all these initiatives is that they highlight the emergence of a principle of horizontal accountability that applies to all stakeholders involved in exchanging and trading personal information.[305] That is to say, certain institutions oversee others, which in turn oversee others, and so on. This is a vast network linking public and private institutions and implementing a system based on mutual oversight.

It is because of this complex of interrelated standards that the metaphor of the bird's nest has been proposed by certain Australian researchers to describe this phenomenon.[306] They explain that they chose this metaphor because the bird's nest is an object found in nature, serving a vital function to protect something fragile. They add that if a few of the nest's structural twigs break, the nest is built so that the eggs stay safe all the same. The twigs form a solid nest only if they are assembled together. The researchers close by emphasizing that the twigs are not the institutions themselves, but rather the connections between them.

By way of final comment, we can also mention that the authors identify three different types of interrelations that may exist between the institutions that are part of the system: relations that take place at a "policy" (i.e. policy development), "operational" and "constitutional" level. It would be helpful to

304 For a more complete picture of the network of standards, one can read, for example, the speech by the Assistant Privacy Commissioner, Elizabeth Denham, for the *2009 Privacy Invitational Forum* (Cambridge, Ontario, November 19, 2009).

305 KEY CENTRE FOR ETHICS, LAW, JUSTICE AND GOVERNANCE, GRIFFITH UNIVERSITY and TRANSPARENCY INTERNATIONAL AUSTRALIA, *supra*, note 211 (Nisa Report), p. 14-18.

306 *Id.*

carry out additional research in order to better understand the legal aspects of these relations between institutions responsible for privacy protection. Such research might allow us to better understand the extent to which these relations between policy statement and policy implementation are creating a constitutional or quasi-constitutional normativity.[307] This research might also aim to better understand the strengths and weaknesses of the systems being networked, and in particular the Canadian system.

Conclusion to part 1

Ten years after the passage of PIPEDA, what are the points of convergence and divergence between the economic, legal and political contexts in the new millennium, and what new contemporary realities have emerged in the 10 years since the Act was passed?

First of all, the economic discourse continues to favour the imposition of a minimum of constraints on companies, with the aim of guaranteeing access to national and international markets. However, reflection on the role of social regulations (the category into which PIPEDA falls) has progressed toward greater sensitivity to providing more protection for consumers. In fact, the State's objective of protecting its citizens (consumers) from abuses of corporate power is seen as an entirely legitimate role.

Furthermore, this protection must be thought out at the domestic but also the international level, since States are obliged to harmonize their social regulations as far as possible, in order to guarantee effective protection against inter-state exchanges of information. This objective is all the more important in that the technological developments of Web 2.0 suggest that this sort of harmonization will be necessary for the protection to be effective. In view of these new technological developments in particular, the idea of consolidating the integrity system on the national and international levels assumes its full significance.

On this subject, additional, targeted research on the impacts of these technological changes on the capacity of public agencies to implement their privacy protection mission is essential for assessing the effectiveness of PIPEDA. This analysis should not only focus on the economic dimension. What is needed is a thorough review of the multiple new applications through which companies may violate a consumer's right to personal information protection. It is also important to consider the public sector. This means reviewing potential violations by Canadian and foreign governments of the right to personal information protection for Canadian citizens. Finally, we need to explore the possibility that the growing ties between the private and public sectors may be detrimental to the establishment of balanced ethical relationships (as noted by Gunasekara with regard to the problems associated

307 On this question, see the excellent work by David SCHNEIDERMAN, *Constitutionalizing Economic Globalization: Investment Rules and Democracy's Promise* (Cambridge: Cambridge University Press, 2008).

with the interaction between the two sectors from the standpoint of the war on terror and the accumulation of personal information by the private sector).

These issues raise questions on various levels with significant legal and political repercussions. First, there are problems with regard to institutional organization. With a view to developing answers to all the problems associated with the use of data by private sector companies, Canadian and foreign governments, and in interactions between the private and public sectors, it would be worthwhile to consider whether to keep two distinct federal laws: the *Privacy Act* and PIPEDA. Consideration should also be given the type of administrative body that could be created to meet these new challenges, so as to equip it with adequate financial and human resources, as well as functions and powers adapted to the new realities of today.

In this regard, although there have been no radical changes in political/administrative discourse on the organization and powers of public agencies charged with implementing legislation, the dogmatism of the ideas prevalent in the 1980s which actively opposed the setting up of new public agencies seems to have softened. This is especially true when one goes down the list of agencies created in order to consolidate our national integrity system. One can in fact see a real enthusiasm among politicians over the last four years for parliamentary agencies that provide oversight for government activities. A better understanding of the foundations of this type of agency and the limits on their powers, particularly when they are called upon to act in the private sector, would be useful. This process of reflection and verification will be especially relevant if Parliament considers granting additional powers (such as regulatory and punitive powers) to the Office of the Privacy Commissioner, powers that are not normally associated with an ombudsman *or* a parliamentary type of ombudsman. One question that arises is whether powers assigned to these agencies can be extended to the private sector without unduly sacrificing the State's institutional coherence in the name of what seem to be more pragmatic solutions.

In this regard, it seems that replacing the Office of the Commissioner with an agency belonging to the category of decentralized organizations and more specifically, by a social regulatory agency ("social" rather than "economic" since the function of PIPEDA is social rather than economic regulation) equipped with administrative powers (such as the power to investigate), decision-making powers (for example the power to make orders and impose penalties) as well as regulatory powers, is an option that deserves consideration.

At least three observations can be made about the legal context, ranging from the macro to micro levels.

First, it should be noted that construction of the Global Administrative Law on privacy protection is continuing and becoming more complex. Additional research will be necessary to better identify and understand the strengths and weaknesses of our Canadian system for protecting information relative to this network of standards. It might also be useful to consider assigning powers to the Office of the Privacy Commissioner so that it can clearly participate in

the debates at the supranational level. One option here might be to form a cooperation committee (composed of the federal commissioner and provincial commissioners, federal and provincial public servants, representatives of small, medium-sized and large industries, representatives of interest groups (especially in consumer protection) and citizens' representatives). This would be like creating a Canadian delegation (in the form of an advisory board) with sufficient authority to discuss privacy issues and intervene on the creation of global administrative law standards and mechanisms in this area.

Second, it should be noted that the constitutional problems raised by the passage of PIPEDA in 2000 have still not been resolved. It will be necessary to monitor debate in the courts of law, particularly on the validity of harmonization processes. Any consideration of granting the Office order-making powers that could be applicable to all Canadian businesses would generate stormy federal-provincial debate. This sort of matter should first be discussed among the entities of the federation, to ascertain the extent to which a federal-provincial agreement might be an option. From this perspective, the issue of the creation of a federal regulatory agency for securities (a current proposal of the Harper government) is something to be monitored since it also raises questions of the interpretation of sections 91.2 and 92.13 of the *Constitution Act, 1867*, just like PIPEDA. The arguments presented by the federal and provincial governments will be decisive in setting guidelines for the interpretation of these sections since the Court's reasons will flow from them. Although at the time of this report's writing, the governments' submissions were not available, it is reasonable to think that some of the federal government's arguments will be functional in nature. It is therefore possible that the Supreme Court will find them valid, which could be the signal for implementation of a more functional interpretation of our constitution, paving the way for implementation of a form of networked federalism. Whatever happens in this regard, if a more functional approach were to be considered to resolve some problems in enforcing PIPEDA, the parameters for action by the Office of the Privacy Commissioner should be the subject of more thorough research and analyses. At the very least, the possibility of establishing a secretariat to coordinate reflection and research at all levels of government (including the municipal governments) could be a worthwhile start to the search for more effective solutions and administrative practices.

Third, as regards the possible assignment of criminal powers, it should be noted that, for the moment within the federal government, it appears that only the CRTC (an economic regulatory agency) has such powers. In Quebec, the Human Rights Tribunal can assess punitive damages to natural and legal persons who knowingly violate the Charter of Human Rights and Freedoms. It is interesting to note here that the Human Rights Tribunal examines the infringement of rights of a quasi-constitutional nature. Since it is likely that privacy protection has acquired this same legal status, certain analogies could be made to justify the assignment of such powers to the Office of the Commissioner.

Although there is a strong movement toward granting greater protections to citizens and consumers concerning the flow of their personal information, it is

also important to consider their freedom and to maintain a balance between rights and freedoms. We need a better understanding of what citizens want. Do they want more protection? Are distinct trends observable for the different generations in question? To understand these changes in perspectives, the Office of the Privacy Commissioner could be conceived not only as a forum for public education, but also a forum where *one learns from the public*. Therefore it might be helpful to provide the OPC with the powers and funds necessary to hold periodic community forums to learn what is expected by citizens, industry and interest groups.

Part II: Approaches and alternatives in evaluating the Privacy Commissioner's PIPEDA jurisdiction

The goal of this study is to develop a conceptual framework for evaluating the efficiency and effectiveness of the Office of the Privacy Commissioner (OPC) with respect to its mandate under *Personal Information Protection and Electronic Documents Act* (PIPEDA), and to apply that framework in light of the OPC's activities. Having elaborated a conceptual framework in Part 1, our analysis now turns to an examination of the OPC's effectiveness in fulfilling PIPEDA's objectives. The concept of effectiveness, as discussed in Part 1, is intended to capture a range of dynamics relating to the OPC's internal and external environment. To the extent that Part 1 canvassed the macro-environment within which the OPC's PIPEDA activities take place, Part 2 is directed toward the microenvironment.

Evaluating efficiency and effectiveness involves a blend of empirical, comparative and normative assessments. Empirical assessments relate to quantifiable and qualitative data that provide measurements of the OPC's level of activities, value for investment and perception of performance. Comparative assessments relate to assessing the OPC through the lens of analogous agencies in Canadian and/or peer jurisdictions. Normative assessment, finally, relates to whether the OPC is fulfilling the goals that expressly or impliedly accompanied the introduction of PIPEDA.

This bring us to the issue of the criteria to be used to evaluate the OPC's oversight of compliance with PIPEDA. To address this question, it is necessary to understand the scope and aim of the OPC's jurisdiction, and in particular, the "Ombuds" model which the OPC has adopted (in this part, "Ombuds" and "Ombudsman" will be used interchangeably). In evaluating the performance of the OPC, in other words, it is important to start with the mandate and mission of the OPC and the legislation it interprets and applies (in this case, PIPEDA).

Part 2 is divided into four sections. The first section examines the mandate and mission of the OPC in the context of PIPEDA and the adoption of the Ombuds model. This section also reviews the existing powers and tools available to the OPC to ensure compliance with PIPEDA. The second section compares the OPC's powers with those of other Canadian privacy regulators, and with other data regulators in peer jurisdictions. The third section continues the comparative analysis, and is focused on regulators of analogous subject matter in Canada and in the U.S. The fourth section, finally, explores the lessons

learned from the analysis of the OPC and the comparative analysis with respect to evaluative approaches. This section also includes a qualitative review of the perceptions of the OPC.

Section 1: The mandate and mission of the Office of the Privacy Commissioner & the Ombuds Model under PIPEDA

The scope of PIPEDA and mandate of the OPC

The mandate of the Office of the Privacy Commissioner of Canada (OPC) is overseeing compliance with both the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and PIPEDA. The mission of the OPC is to protect and promote the privacy rights of individuals. The OPC's mandate is to act as an ombudsman for privacy and the protection of personal information rights of Canadians, including both an advocacy and guardianship component.

The Commissioner works independently to investigate complaints from individuals with respect to the federal public sector and the private sector. In public sector matters, individuals may complain to the Commissioner about any matter specified in Section 29 of the *Privacy Act* (which applies to personal information held by Government of Canada institutions).

PIPEDA applies to every organization in respect of personal information that the organization collects, uses or discloses in the course of its commercial activities. PIPEDA also applies to federal works, undertakings and businesses in respect of employee personal information that they collect, use or disclose in connection with their operations.

Federalism is another context with an impact on the administration of PIPEDA. The Constitutional implications of PIPEDA were discussed in Part 1, and in part because of those implications, PIPEDA was designed to work in tandem with provincial legislation. PIPEDA contemplates the harmonization of provincial and federal privacy protection. For matters relating to personal information in the private sector, the Commissioner may investigate all complaints under Section 11 of PIPEDA except in the provinces that have adopted substantially similar privacy legislation, namely Québec, British Columbia, and Alberta. Ontario now falls into this category with respect to personal health information held by health information custodians under its health sector privacy law. However, even in those provinces with substantially similar legislation, and elsewhere in Canada, PIPEDA continues to apply to personal information collected, used or disclosed by all federal works, undertakings and businesses, including personal information about their employees. PIPEDA also applies to all personal data that flows across provincial or national borders, in the course of commercial transactions involving organizations subject to the Act or to substantially similar legislation.

A key consideration in the development of PIPEDA was the powers by which the Commissioner would be able to enforce the Act. The Commissioner focuses on resolving complaints through negotiation and persuasion, using

mediation and conciliation if appropriate. However, if voluntary co-operation is not forthcoming, the Commissioner has the power to summon witnesses, administer oaths and compel the production of evidence. In cases that remain unresolved, particularly under PIPEDA, the Commissioner may take the matter to Federal Court and seek a court order to rectify the situation. The mandate of the OPC under PIPEDA also extends to the development and dissemination of public education and information regarding privacy protection, so that prevention could be as significant an activity of the OPC as enforcement.

In 2008, the OPC Inquiries Branch responded to 6,344 inquiries about PIPEDA, received 422 new PIPEDA-related complaints, and closed the file on 412 complaints.[308] These numbers, on their own, disclose little about the effectiveness of the OPC in the context of PIPEDA, though the Commissioner observes, "The sheer volume of calls and letters we receive demonstrates the extent to which Canadians recognize and cherish their right to privacy."[309]

Additional insight into the effectiveness of the OPC may be gleaned from looking at trends over time. The number of complaints in 2008, for example, is equal to the number received in 2006 after a decline in 2007. The number of inquiries, by contrast is down after a three-year period of increase. While the level of inquiry and complaint activity represent important data, it is not possible to draw from such data conclusions about performance. For example, the decrease in the number of complaints in 2008 could be a sign of success of the OPC initiative encouraging consumers to bring privacy concerns directly to the companies who control their personal information, or it could signal an erosion of confidence in or awareness of the OPC. Data of this kind needs to be understood in context, against the conceptual backdrop set out in Part 1 and the empirical, comparative and normative backdrop explored in this part. In that context, the inquiries and complaints which are not made, because prevention, education and outreach ensure compliance with PIPEDA, are as important or perhaps more important than the occasions when people seek the intervention of the OPC.

Evaluating the activities of the OPC also must take into consideration the goals of the PIPEDA – those goals are aimed at providing Canadians with a right of privacy with respect to their personal information that is collected, used or disclosed by a private sector organization. In particular, PIPEDA was designed with the expanding flow of information and data in an electronic age in mind.

PIPEDA's obligations build on the Canadian Standards Associations Model Code for the Protection of Personal Information, which recognized 10 core principles:

308 2008 Annual Report to Parliament: Report on PIPEDA, Office of the Privacy Commission (August 2009) at http://www.priv.gc.ca/information/ar/200809/2008_pipeda_e.pdf.

309 *Id.*, p. 3.

(1) Accountability
(2) Identifying Purposes for Collecting Personal Information
(3) Consent
(4) Limiting the Collection of Personal Information
(5) Limiting Use, Disclosure and Retention of Personal Information
(6) Accuracy
(7) Safeguards
(8) Openness
(9) Individual Access
(10) Individual Recourse to Challenge Compliance

PIPEDA contains the over-arching rule (under s. 5(3)) that organizations may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. PIPEDA provides a mechanism for individuals to file written complaints with the OPC against an organization for contravening specified provisions of the Act. PIPEDA also authorizes the Commissioner to initiate a complaint where the Commissioner is satisfied that there are reasonable grounds to investigate a matter.

Concerns About the OPC's jurisdiction with respect to PIPEDA

The activities of the OPC under this jurisdiction since 2001 have been subject to extensive scrutiny, both internal and external to the OPC, and from academic, business, governmental, judicial and Parliamentary perspectives.

In *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA)*,[310] a study prepared by the OPC to review the first seven years of the OPC's operations under its PIPEDA jurisdiction, the OPC reviews some of its major findings, some important judicial considerations of PIPEDA and some areas for future attention, but refrains from offering any assessment either of PIPEDA or its own activities. This report demonstrates the significant impact both of PIPEDA and of the OPC's compliance related activities, and in particular its responses to written complaints.

Parliament completed a major review of PIPEDA in 2006-2007, pursuant to section 29(1) of PIPEDA, which mandates a review every five years. The House of Commons Standing Committee on Access to Information, Privacy and Ethics held hearings between November 20, 2006 and February 22, 2007, heard from 67 witnesses and received 34 submissions from individual Canadians and Canadian organizations (including the OPC).

The *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA): Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, was presented in the House of Commons on

310 Accessible online at http://www.priv.gc.ca/information/pub/lbe_080523_e.pdf.

May 2, 2007, and included 25 recommendations. Noteworthy among these recommendations was Recommendation 18: "The Committee recommends that the Federal Privacy Commissioner not be granted order-making powers at this time." The Committee did recommend an additional power for the OPC relating to the mandatory notification of privacy breaches to the OPC.[311]

The government response to the Committee's Report indicates that more data would be needed before any "radical changes" to the legislation would in its view be warranted.[312]

While the Parliamentary review did not result in a call for a major overhaul of the OPC's model in relation to PIPEDA, the academic and advocacy community has been more critical. In "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices,"[313] Lisa Austin argues that the evaluation of the effectiveness of the OPC should be tied to the issues which its jurisdiction under PIPEDA was designed to address. She argues that the central problem to which PIPEDA responds is "control over personal information is meant to provide individuals with informational privacy." She argues further that informational privacy may protect a broader set of values, including the exercise of choices regarding privacy options. The evaluation of the OPC's Ombudsman model, in other words, cannot be separated from the norms of PIPEDA. Austin is particularly critical of the fact that the OPC publishes only "summaries" of its findings and refrains from identifying the respondents in such summaries. Thus, the OPC does not produce binding precedents, nor do its findings form the basis of a jurisprudence that could govern privacy standards under PIPEDA.

The Canadian Internet Policy and Public Interest Clinic (CIPPIC), similarly, concluded that the OPC lacks "teeth," the evidence for which in its view, is the conclusion of a CIPPIC study which found widespread non-compliance with PIPEDA requirements.[314]

Critics have expressed concern not only with the effectiveness of the OPC's current model in achieving compliance with PIPEDA, but have also characterized the choice of the Ombuds model as one *intended* to be less effective. Christopher Berzins, who is critical of the selection of the Ombuds model, identifies seven factors which he asserts resulted in the particular model

311 See recommendations 23 and 24.

312 See http://www2.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&Parl=39&Ses=1&DocId=3077726&File=0

313 Lisa AUSTIN, "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices", (2006) 44 *Canadian Business Law Journal* 21.

314 CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC, *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?*, 2006, Ottawa, Canadian Internet Policy and Public Interest Clinic, http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf

selected for the OPC to implement PIPEDA: (1) the desire to keep organized business interests "onside"; (2) there was no mobilized privacy constituency at the time with the capacity to influence policy; (3) the privacy advocates which were active at the time were prepared to compromise on enforcement in order to secure private sector privacy legislation; (4) expert input emphasized broader compliance strategies beyond complaint mechanisms and enforcement powers; (5) the federal level of government had a history of turning to Ombuds oversight in analogous settings such as the existing the Privacy Commissioner and the Access to Information Commissioner; (6) the Privacy Commissioner at the time, Bruce Phillips, favoured an Ombuds model for PIPEDA; and (7) Government was not inclined to establish more rigorous oversight for the private sector than it accepted over its own sphere of activity.[315]

1.1. The OPC's Ombuds Model

The most significant aspect of the OPC's jurisdiction with respect to PIPEDA is the Ombuds model that the OPC has chosen in exercising its jurisdiction over private sector privacy. In her 2005 paper, "Cherry Picking Among Apples and Oranges: Refocusing Current Debate About the Merits of the Ombuds-Model Under PIPEDA,"[316] Commissioner Jennifer Stoddart explains the rationale for this choice and addresses some of its critics. Stoddart adopts the following definition of the Ombudsman model:

> a mechanism that monitors the conduct of public administration to ensure that it is conducted legally and fairly. The Ombudsman is usually a single individual, but occasionally the institution may comprise a number of persons. An Ombudsman is usually appointed by the legislative branch of government to investigate the administrative activities of the executive.[317]

Former Commissioner Bruce Phillips elaborated on his preference for the Ombuds model as a mechanism for problem solving and as a progressive force for change:

> The federal Privacy Commissioner functions as an Ombudsman, and I have no power to order anybody to do anything. I can tell you I'm perfectly happy not ordering people around, because the great value of the Ombudsman's

315 Christopher BERZINS, "Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building", (2002) 27 *Queen's Law Journal* 609. Berzins approach to the OPC is discussed further in Part 1.

316 See http://www.priv.gc.ca/information/pub/omb_051021_e.cfm.

317 This definition was quoted from Linda C. REIF, "Building Democratic Institutions: The Role of National Human Rights Institutions in Good Governance and Human Rights Protection", (2000) 13 *Harvard Human Rights Journal* 1, at 8.

> office is not, first and foremost, to find blame and tell people what to do, but to find solutions to problems. I would make this argument, immodestly perhaps but confidently, that this has been an enormous success, because there have been literally hundreds if not thousands of cases that have come before my office in the eight years or so I've been there in which we have—thanks to negotiation, discussion, and careful examination of problems—identified areas in the federal public service, where our bill applies, where information management has been significantly improved to eliminate privacy problems.[318]

The Ombuds model involves more, however, than the absence of coercion. The characteristic features of the Ombudsman model can be summarized as:

- Advancing goals of fairness, transparency, accountability, and equity;
- Committed to pursuing mutually agreeable and/or consensual resolution of disputes;
- Flexibility;
- Confidentiality;
- Independence from government;
- Authority to conduct investigations;
- Authority to issue public reports; and
- The absence of binding orders, remedial sanctions or disciplinary powers.

As demonstrated by these characteristics, the Ombudsman plays a unique institutional role in ensuring accountability between the individual and the administrative state.

The Supreme Court of Canada characterized the Ombudsman's important role in facilitating democratic accountability by concluding that, "the powers granted to the Ombudsman allow him to address administrative problems that the courts, the legislature, and the executive cannot effectively resolve."[319] While the Ombudsman model first emerged in early 19th century Sweden, it only began to be adopted outside of Scandinavia in the mid-20th century. The Ombudsman model spread in response to a growing demand for greater governmental accountability and had been adopted by an estimated 90

318 Submission to the House of Commons Standing Committee on Industry, December 2, 1998, accessible online at http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1039144&Language=E#T1532, beginning at 1625. For additional discussion of the Ombudsman model in the proceedings of Parliamentary committees, see Jennifer BARRIGAR, "Consider Consideration and Order-Making" (paper prepared for the OPC, September 2009).

319 *B.C. Development Corp.* v. *Friedmann*, [1985] 2 S.C.R. 447, at para. 40.

countries by the end of the 1990s.[320] The rising popularity of Ombudsman model saw its adoption by all levels of government, as well as by private industry and academe.

As the model spread, the Ombudsman took different forms that can generally be classified into two categories: the public "classical" Ombudsman who operates under statutory authority, and the private "organizational" Ombudsman, who works within institutions such as universities and corporations.[321]

The OPC's oversight of PIPEDA is a hybrid of the two primary Ombudsman models – the public sector Ombudsman and the private sector Ombudsman: while it is publicly funded and operates under a statutory mandate, the OPC has jurisdiction over the private sphere. Unlike the general purpose Ombudsman model adopted by provincial parliamentary Ombudsmen in Canada, the OPC follows a special mandate Ombudsman model as it has jurisdiction over a particular area of administration.

Despite the manifold forms that the Ombudsman model has taken in adapting to local needs over time, there remain common elements that characterize the model. The Ombudsman typically has the power to investigate complaints made by the public and can often launch her own investigations. In many jurisdictions, the Ombudsman can also investigate issues referred to her by legislators or government ministers. By contrast to the court system, the Ombudsman model is designed to be accessible and inexpensive for complainants, while offering greater flexibility and creativity in its recommendations.

In contrast to the adversarial approach taken by common law courts, the Ombudsman proceeds by means of inquisitorial investigations into complaints. The Ombudsman's role is not viewed within the context of a "battle of adversaries." Nor is the model one, strictly speaking, of mediating or resolving disputes. The Ombudsman does not seek to settle disputes but rather to advance the goals such as integrity, transparency, fairness and equity.[322]

---

320 Roy GREGORY and P Philip GIDDINGS, "The Ombudsman Institution: Growth and Development" in Roy GREGORY and Philip GIDDINGS (eds.), *Righting Wrongs: The Ombudsman in Six Continents*, Washington, IOS Press, 2000, p. 1, at page 1.

321 Howard GADLIN, "The Ombudsman: What's in a Name?" (2000) 16(1) Negotiation Journal 37, at 38-39.

322 See the description of the Ombuds role in correspondence from Commissioner Bruce PHILLIPS to Susan WHELAN, MP, Chair of the Standing Committee on Industry, February 8, 1999, in response to submissions to the Committee calling for the OPC to be given the authority to issue binding orders (on file with authors).

André Legrand has observed that, "the main peculiarity of the institution of the Ombudsman lies in the fact that he does not belong to the administration but at the same time possesses extensive capabilities for accessing information."[323] Accordingly, the Ombudsman's investigation is generally a fast, informal and impartial procedure. The Ombudsman typically has the power to call on individuals for information, and on organizations for open access to records and procedures.

1.2 Powers and tools available to the OPC

As a general matter, while an Ombudsman typically does not have the power to make decisions or orders that are binding on government, she derives her authority from the quality of her investigations and the continued legitimacy of her office. Thus, accuracy, non-partisanship and credibility are paramount to the success of the Ombudsman's investigation. To facilitate effective investigations, the Ombudsman generally will be provided broad and potentially intrusive investigative powers.

In other words, the Ombudsman's broad investigative powers are moderated by the non-compulsory nature of her decisions. Upon completing her investigation, the Ombudsman has the power to report her findings and to make recommendations to both improve systems and to offer redress for those adversely affected by the administrative activity under review.

Many argue that the non-compulsory powers of Ombudsmen are their greatest strength. Stephen Owen observes,

> While a coercive process may cause reluctant change in a single decision or action, by definition it creates a loser who will be unlikely to embrace the recommendations in future actions. By contrast, where change results from a reasoning process it changes a way of thinking and the result endures to the benefit of potential complainants in the future.[324]

As ombudsmen do not make legally binding decisions, they have greater flexibility than courts, which are bound by the rules of procedural law. Thus the seemingly restricted remedial powers enjoyed by ombudsmen actually strengthen their investigative and persuasive capabilities.

The non-binding nature of an Ombudsman's role may also blunt opposition to the Ombudsman's goals. This dynamic appeared to play a role in the choice

323 Rhita BOUSTA, "The Ombudsman: Proposal for a Definition," (2005) 9 *The International Ombudsman Yearbook* 36, at 49.

324 Stephen OWEN, "The Ombudsman: Essential Elements and Common Challenges" in Linda C. REIF (ed.), *The International Ombudsman Anthology*, The Hague, Kluwer Law International, 1999, p. 51, at page 52.

of the Ombuds model for the OPC. As former OPC Commissioner Bruce Phillips noted in his defence of the Ombuds model for the IPC:

> My pragmatic reason for rejecting an order making power lies in the hostility and intransigence that such a power is almost certain to foster in the business community. It is one thing to approach an enterprise to discuss unacceptable privacy practices and look for ways to prevent their recurrence. It is quite another to approach that same enterprise when its management knows full well that you have the power to force co-operation. The immediate response in the latter case is almost certain to be to draw out the big guns – the legal advisers and the consultants – and to eye with great suspicion any request for discussion, review or change of current practices. The process becomes bogged down in legalities and technicalities, delaying resolution to the issue and adding greatly to the frustration of an already-aggrieved complainant.[325]

Phillips went on to note that, in his view, the Ombuds model is not "toothless" because it provides the OPC with a highly effective power to publicize issues of the improper handling of personal information. The OPC, in other words, has a «Bully Pulpit» from which to influence industry wide practices.

A good example of this function in action is the OPC's interaction with Facebook over its privacy controls. The OPC's investigation of a complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) highlighting the allegedly inadequate privacy controls employed by the social networking site attracted national and international media attention. The OPC investigated 24 separate allegations, and found 8 violations of the Act in the operation of Facebook's social networking site – 4 of which had been remedied at the time the findings were issued, 4 of which had not and Facebook was given a 30 day period to demonstrate evidence that it was implementing the recommendations in the Report to remedy its contravention of the Act.[326] The publicity surrounding this investigation and report allowed the OPC an unprecedented opportunity to raise awareness of privacy issues relating to social

325 Supra note 323.

326 The various allegations and conclusions are set out in the *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook inc. under the Personal Information Protection and Electronic Documents Act*, July 16, 2009, at http://priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.

networking. University of Ottawa Law Professor Michael Geist referred to the investigation and settlement as a "major success."[327]

A month after the Report of Findings was issued, the OPC issued a press release indicating that, "Facebook has agreed to add significant new privacy safeguards and make other changes in response to the Privacy Commissioner of Canada's recent investigation into the popular social networking site's privacy policies and practices."

While issues remained as to Facebook's compliance with key recommendations around the over-sharing of personal information with third-party developers of Facebook applications such as games and quizzes, the Commissioner was reported as "satisfied Facebook is on the right path to addressing the privacy gaps on its site."

As we discussed in Part 1, privacy concerns are becoming increasingly borderless and increasingly tied to advances in new technologies to obtain, analyze and disseminate information. Commissioner Stoddart observed in her 2009 Annual Report on PIPEDA, "We saw an exponential growth in investigations dealing with new technologies – and it seems clear that technology issues will dominate our work in the years ahead."[328] In January of 2010, the OPC announced that it is examining on-line tracking, profiling and targeting of consumers by business through Facebook and other social network sites such as MySpace and LinkedIn.[329]

Another dimension of this shift is that data protection regulators may need to work in concert to be effective. In April of 2010, the Commissioner joined with data protection agencies in France, Germany, Ireland, Israel, Italy, the Netherlands, New Zealand, Spain and the United Kingdom to raise serious concerns with Google's "Buzz" program, which was described in the following terms:

> In essence, you took Google Mail (Gmail), a private, one-to-one web-based e-mail service, and converted it into a social networking service, raising concern among users that their personal information was being disclosed. Google automatically assigned users a network of "followers" from

327 Michael GEIST, "Facebook Settles Privacy Commissioner of Canada, August 29, 2009, accessible online at http://www.michaelgeist.ca/content/view/4330/196/. See also Michael GEIST, "Standing on Guard for Privacy – Before Facebook", *Toronto Star*, September 14, 2009, accessible online at http://www.thestar.com/business/article/695147.

328 Office of the Privacy Commissioner, 2009 Annual Report to Parliament, at http://www.priv.gc.ca/information/ar/200910/2009_pipeda_e.pdf (Accessed August 2, 2010), at p.2.

329 See http://www.priv.gc.ca/media/nr-c/2010/nr-c_100601_e.cfm (Accessed on July 12, 2010)

> among people with whom they corresponded most often on Gmail, without adequately informing Gmail users about how this new service would work or providing sufficient information to permit informed consent decisions. This violated the fundamental principle that individuals should be able to control the use of their personal information.[330]

The signatories to the letter called on Google (and other social networking companies) to incorporate privacy protections into all of their on-line services, including the collection of as little personal information as possible, and ensuring that privacy protections are available, prominent and easy to control.

In June of 2010, the OPC launched a separate investigation into Google's "Streetview" initiative by which cameras mounted on cars captured street level video across urban areas in Canada. Google indicated it also obtained data from WiFi networks where its camera was operating in order to enhance location-based services. Commissioner Stoddart issued the following statement:

> We are very concerned about the privacy implications stemming from Google's confirmation that it had been capturing Wi-Fi data in neighborhoods across Canada and around the world over the past several years. We have a number of questions about how this collection could have happened and about the impact on people's privacy. We've determined that an investigation is the best way to find the answers.[331]

In its dealings with large multinational technology companies such as Google or Facebook, attracting media attention is as important for the OPC's effectiveness as any regulatory powers it might attempt to exercise against such companies.

The 2009 Facebook investigation represented a potential "tipping point" for the OPC not because of its investigation but because of the global coverage its investigation generated, and perhaps even more importantly, the substantial public support for its efforts that this coverage both reflected and augmented.

The ability to command public attention and therefore leverage, however, is not the only way in which the OPC's current model is not toothless. As the Facebook and Google examples show, the Commissioner has a range of enforcement tools to deploy in order to advance the OPC's mandate in relation to PIPEDA:

---

330 « Letter to Google CEO » at http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm (Accessed on July 12, 2010)

331 Privacy Commission Investigates Google WiFi Data Collection (June 1, 2010) at http://www.priv.gc.ca/media/nr-c/2010/nr-c_100601_e.cfm.

- Investigating complaints and issuing reports with recommendations to federal government institutions and private sector organizations to remedy situations, as appropriate;
- Pursuing legal action before Federal Courts where matters remain unresolved;
- Assessing compliance with obligations contained in the *Privacy Act* and PIPEDA through the conduct of independent audit and review activities, and publicly report on findings;
- Advising on, and review, privacy impact assessments (PIAs) of new and existing government initiatives;
- Providing legal and policy analyses and expertise to help guide Parliament's review of evolving legislation to ensure respect for individuals' right to privacy;
- Responding to inquiries of Parliamentarians, individual Canadians and organizations seeking information and guidance and taking proactive steps to inform them of emerging privacy issues;
- Promoting public awareness and compliance, and fostering understanding of privacy rights and obligations through: proactive engagement with federal government institutions, industry associations, legal community, academia, professional associations, and other stakeholders; preparation and dissemination of public education materials, positions on evolving legislation, regulations and policies, guidance documents and research findings for use by the general public, federal government institutions and private sector organizations;
- Providing legal opinions and litigate court cases to advance the interpretation and application of federal privacy laws;
- Monitoring trends in privacy practices, identify systemic privacy issues that need to be addressed by federal government institutions and private sector organizations and promoting integration of best practices; and
- Working with privacy stakeholders from other jurisdictions in Canada and on the international scene to address global privacy issues that result from ever-increasing trans-border data flows.[332]

The OPC, further, has a range of tools and powers under PIPEDA, involving reports, research, public education, investigating complaints, and audits. In describing her approach to the Ombudsman model in the context of PIPEDA, Commissioner Stoddart has asserted:

> It must be underscored that the Ombuds-role is not simply remedial, but transformative in nature. The aim is the resolution of individual complaints, but it is also the development of a lasting culture of privacy sensitivity among the parties through their willing and active

332 This information is drawn from the Office of the Privacy Commissioner's website.

> involvement in the process itself. In order to achieve these twin goals, the process must necessarily be flexible, participative and individuated in its approach.

How might the effectiveness of the OPC in achieving these twin goals be assessed? While there is always a subjective element in selecting criteria for evaluation, in light of the OPC's mandate, mission, activities, and powers, and considering also the general goals of the Ombudsman model, certain kinds of objective measures appear best suited to this context. These include (but would not be limited to):

1) The level of activity of the OPC (e.g. how many investigations or audits are conducted in a given year, or how many proceedings are commenced in Federal Court);
2) The impact of the activity of the OPC on the behaviour of private sector organizations, including measurable changes in organizational culture, the prevention of disputes, etc;
3) The level of satisfaction of those who have launched complaints; the belief of those subject to complaints in the fairness of the OPC's process.
4) The reputation of the OPC among industry, consumer and other affected groups;
5) The level of accessibility to the public (e.g. cost and convenience), as well as how visible the OPC is among potential complainants; and
6) The contribution of the OPC to public awareness and understanding of the public's rights under PIPEDA (including media coverage of investigations and reports, visitors to the OPC website, OPC sponsored public education initiatives, etc).

The above criteria focus on empirical measures that evaluate the OPC's fulfillment of its statutory and policy objectives. If the effectiveness of the Ombudsman model is the aim of empirical research, however, the performance of the OPC should also be compared against peer privacy regulators. For example, comparing the reputation and success in behaviour modification of the OPC with privacy regulators, or peer regulators in other fields, who possess order-making and binding enforcement powers, might provide a basis for conclusions regarding the relative success and effectiveness of the Ombudsman model.

Whether the OPC is compared with peer privacy regulators or other kinds of regulators, it is clear that any meaningful evaluation of the OPC will require both an internal and a comparative perspective. It is to elaborating these perspectives that we now turn.

Section 2: Canada's Privacy Commissioner's powers with respect to PIPEDA compared to provincial and selected international regulators, as well as peer oversight bodies

Over the past thirty years, there has been a global spread of data protection laws as they have come to be regarded as essential tools for regulating the use

of personal data, and as the basis for the work of the oversight bodies they create. More recently, the most legislative change has taken place in Europe as democratizing countries write privacy laws and as countries with existing legislation update their data protection regimes in compliance with the European Union Directive. In Canada, while we have long had data protection laws and independent privacy commissioners, we have only recently begun to extend this protection to the private sphere in a manner dictated by our federal constitutional system.

In extending and reforming a country's privacy laws, the importance of vigorous oversight authorities has proven to be critical. Good laws alone are unlikely to be properly implemented and do little to foster a culture of privacy.[333] Despite the importance of strong regulatory authorities, Colin Bennett and Charles Raab have argued that an active and assertive regulatory authority is only one identifiable yardstick by which one might measure the effectiveness of a data protection system. Bennett and Raab argue that a good privacy regime will also have: (1) a strong, clear law, (2) effective procedures for compliance among data collectors, (3) market incentives to promote private sector compliance, (4) a vigilant and concerned citizenry, and (5) extensive use of privacy-enhancing technologies.[334]

Bennett and Raab further posit that while a privacy and data protection commissioner may act as Ombudsman, she does so in conjunction with her role as auditor, consultant, educator, negotiator, policy adviser and enforcer.[335] An independent data protection authority must therefore balance a wide range of roles and an evaluation of its performance on all of these axes is a necessarily complex undertaking. Nevertheless, such an evaluation is important in both undertaking institutional reform and in striving for an optimal level of data security. Therefore, an assessment of the effectiveness of a country's privacy regime finds its logical starting point in an inter-provincial analysis.

2.1 Provincial privacy regulators

Privacy protection regimes worldwide have adopted a variety of approaches to overseeing the enforcement of their data protection or privacy laws. Data protection authorities may follow the licensing model (e.g. Sweden), the registration model (e.g. UK under the 1984 legislation), the commissioner model (e.g. Germany) and the self-help model (e.g. U.S.), though most countries typically have a hybrid system in which one of these models predominates.[336] Different countries may have officials, a Commissioner, Ombudsman, or Registrar oversee privacy regulation, having been delegated varying amounts of power. Canada presents a particularly complex privacy

333 Colin J. BENNETT and Charles D. RAAD, *supra*, note 74, at p. 107.

334 *Id.*, at p. 207.

335 *Id.*, at p. 109.

336 *Id.*, at p. 107.

regime as both federal and provincial governments have enacted legislation and empowered oversight bodies to protect privacy.

While PIPEDA was implemented in stages beginning in January 2001, it allowed provinces to opt out of its application to commercial activity in provincially regulated sectors where provinces enact "substantially similar" legislation. While nearly all Canadian provinces and territories have both public sector data protection laws and sector-specific privacy laws (e.g. governing healthcare), this is not true of privacy legislation regulating the private sphere. At the time of PIPEDA's implementation, Quebec was the only province with such substantially similar privacy laws; however, Alberta and British Columbia also have successfully implemented their own substantially similar privacy laws.

In January 2004, British Columbia and Alberta passed statutes entitled the *Personal Information Protection Act* (PIPA) that are largely indistinguishable, having been developed under a common process.[337] While such sub-national privacy laws create a more complex privacy regime, Canada is not alone in adopting such overlapping privacy regulations: various U.S. sates, Germany's Länder, and Australian states have adopted similar national and sub-national privacy regimes. In evaluating the differences between the provincial privacy Ombudsmen and the federal Privacy Commissioner, it becomes evident that while the provincial Commissioners' offices are substantially similar to that of the federal Commissioner, the provincial Ombudsmen have stronger enforcement powers. Moreover, the general trend both among Canadian privacy Ombudsmen and with the United Kingdom's Information Commissioner, which has just undergone fundamental structural reforms, is to expand oversight powers over privacy in the private sector, giving Ombudsmen more teeth to deal with increasingly complex and pervasive privacy issues.

2.2. Quebec's Commission d'accès à l'information

At a time when privacy matters in the Canadian private sector were still governed by a self-regulatory system, Quebec implemented the toughest privacy rules in North America.[338] In the *Act respecting the Protection of Personal Information in the Private Sector* (Quebec's Private Sector Act), which has been in force since 1994, four key principles are set out to guide the regulation of personal information:

1. A person or a corporation must have a serious and legitimate reason for establishing a file on someone.

337 Colin J. BENNETT and Robin M. BAYLEY, "Video Surveillance and Privacy Protection Law in Canada," in Sjaak NOUWT, Berend R. de VRIES and Corien PRINS (eds), The Hague, Asser Press, 2005, p. 65

338 Vagelis PAPAKONSTANTINOU, *Self-Regulation and the Protection of Privacy,* Baden-Baden, Nomos Veralgsgesellschaft, 2001, at p. 127.

2. Every individual has the right to access his or her file, unless the rights of third parties must be protected or there is a serious reason for refusing access.
3. Every individual has the right to rectify an incorrect, incomplete or obsolete file.
4. Every person or corporation that opens a file on an individual has an obligation of confidentiality.

The Commission d'accès à l'information (CAI) oversees the application of both Quebec's private sector act and of its public sector act, the 1982 *Act respecting Access of Documents to Public Bodies and the Protection of Personal Information*. In December 2003, as Canada was preparing to implement PIPEDA for the private sector, Quebec's private sector privacy legislation was found to be substantially similar to the incoming federal legislation.

CAI has three primary functions. Firstly, CAI plays an adjudicative role as it reviews decisions by public authorities to withhold access from private individuals to administrative documents or to their personal files. Quebec's private sector act further empowers the CAI to resolve misunderstandings with respect to the protection of personal information in the private sector. CAI holds hearings only where mediation is unsuccessful and makes binding findings of fact, while questions of law or jurisdiction may be appealed to the Court of Québec. Secondly, CAI plays a supervisory role, overseeing compliance with data security regulations in both the public and private sectors. Thirdly, CAI plays an advisory role in engaging in education to ensure compliance with the spirit and letter of Quebec's privacy laws.

On 14 June 2006, the Quebec National Assembly enacted Bill 86 (*An Act to amend the Act respecting Access to documents held by public bodies and the Protection of personal information and other legislative provisions*),[339] which changed the structure of CAI, dividing it into two sections: the Oversight Division and the Adjudication Division. The changes were brought about as a result of the fourth quinquennial review of CAI.[340] This reform was undertaken in response to criticism that CAI had been jeopardizing its independence and impartiality by allowing the same group of CAI members to both adjudicate and execute CAI's oversight powers. Thus, the Oversight Division now supervises compliance with Quebec's private sector act, while the Adjudication Division resolves disagreements related to access or modifications of one's personal information.

339 QUEBEC NATIONAL ASSEMBLY, *An Act to amend the Act respecting Access to documents held by public bodies and the Protection of personal information and other legislative provisions*, June 14, 2006, http://www.assnat.qc.ca/eng/37legislature2/Projets-loi/publics/index.htm.

340 The changes were also a response to the Supreme Court's interpretation of the independence and impartiality protection for adjudicators contained in the Quebec *Charter of Human Rights and Freedoms* – see *2747-3174 Québec Inc.* v. *Québec (Régie des permis d'alcool)*, [1996] 3 S.C.R. 919 (1996).

CAI was critical of these structural changes to its organization, arguing that in restricting any overlap in personnel between the oversight and adjudication divisions, the Committee on Culture of the National Assembly was depriving CAI of its versatility and ability to accomplish its purposes.[341] Bill 86 included further changes to Quebec's private sector act that tighten controls on cross-border data flows, though these have little import on the administrative structure of the CAI. The Bill 86 reforms came into effect gradually between June 14, 2006, and September 14, 2007.

In an OPC Commissioned study, "Learning from Experience: Judicial Interpretations of Quebec's Private Sector Privacy Regulation," Me Karl Delwaide and Me Antoine Aylwin discuss the distinguishing features of Quebec's *Private Sector Act*. They highlight the fact that harmonization of data protection does not mean each jurisdiction will or need look similar.

The Quebec experience highlights that independence and impartiality, as core administrative law norms, provide the backdrop against which institutional design and the search for the optimal model take place.

2.3 Alberta's Office of the Information and Privacy Commissioner

In May 2003, Alberta passed privacy laws that were substantially similar to PIPEDA with Bill 44, entitled The *Personal Information Protection Act* (PIPA). Since January 2004, Alberta's Office of the Information and Privacy Commissioner has been responsible for PIPA oversight. The Commissioner's office was created in 1995 as the Commissioner also has jurisdiction over the *Freedom of Information and Protection of Privacy Ac*t ("FOIP Act") and over the *Health Information Act* ("HIA"). The Commissioner has the responsibility of

- Informing Albertans about existing and proposed privacy legislation
- Commenting on the privacy and information implications of proposed legislation and programs
- Reviewing the access to information decisions made by the public bodies, custodians, organizations and agencies under the jurisdiction of the FOIP Act, HIA or PIPA
- Investigating how personal information is collected, used and disclosed to ensure compliance under the FOIP Act, HIA or PIPA
- Receive comments from the public about how each of the Acts are being administered
- Research of any factor which may affect the achievement of the purposes of the FOIP Act, HIA or PIPA

341 COMMISSION D'ACCÈS À L'INFORMATION, "The Commission d'accès à l'information is pleased with the automatic disclosure measures announced in Bill 86 but is concerned about the weakening of the rules of protection of personal information …", September 13, 2005, at the following website : http://www.cai.gouv.qc.ca/index-en.html.

- Giving advice and recommendations about the Acts to heads of public bodies, custodians and organizations

The Commissioner collaborates with stakeholders to educate the public, organizations and agencies subject to privacy legislation through community involvement, including, presentations, production of awareness materials including written guides, brochures and community service messages, sponsorship of educational programs through provincial educational institutions such as the University of Alberta, and sponsorship of industry related conferences.[342]

Alberta recently reviewed its PIPA legislation. On May 16, 2006, the Alberta legislature appointed an all-party Select Special Committee, as required under section 63 of PIPA. Alberta's legislative review happened to coincide with BC's review of its own private-sector privacy law (discussed below). The Alberta PIPA Review Committee received 65 written submissions, and heard ten oral presentations from Albertans and from various organizations, including the Office of the Information and Privacy Commissioner, Service Alberta, and the PIPA Advisory Committee.

The Committee's final report was submitted to the Alberta Legislature on November 14, 2007 and it includes 39 recommendations.[343] The key recommendations included,

- Require organizations to inform individuals of trans-border flows of their personal information
- Create a new duty for notification of privacy breaches
- Bring all not-for-profit organizations fully within the scope of the Act
- Provide privacy protection for health-related personal information under HIA rather than PIPA
- Clarify the rules governing personal employee information
- Revise consent provisions to better address longstanding business practices
- Create time limits for the retention of personal information
- Establish new offence provisions
- Establish more appropriate standards for prosecuting offences
- Streamline Commissioner's processes and clarify powers

With respect to the final recommendation that there be some institutional change to the Privacy Commissioner's office, the Committee recommended three main amendments to PIPA. First, the Committee recommended that

342 OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA, http://www.oipc.ab.ca/pages/About/Commissioner.aspx.

343 SELECT SPECIAL PERSONAL INFORMATION PROTECTION ACT REVIEW COMMITTEE, *Review of the Personal Information Protection Act*, Edmonton, Legislative Assembly of Alberta, 2007, accessible online at : www.assembly.ab.ca/committees/reports/PIPA/finalpipawReport111407.pdf.

PIPA be amended to give the Commissioner explicit authority to discontinue an investigation or a review when he believes the complaint or request for review is without merit or where there is insufficient evidence to proceed. Secondly, the Committee recommended that PIPA be amended such that the Commissioner may request information covered by solicitor-client privilege without affecting the privilege in question. Thirdly, the Committee recommended that a provision be added to PIPA allowing the Commissioner to disclose information relating to an offence so long as the information is not subject to solicitor-client privilege.

Thus, the Committee recommended that the Commissioner's powers and discretion be broadened. However, there was recommendation to fundamentally modify the Commissioner's Ombudsman role. Thus, the Alberta example demonstrates that an Ombuds model may coexist with and complement a range of enforcement and compliance measures.

2.4 British Columbia's Office of the Information and Privacy Commissioner

In March 2003, British Columbia passed privacy laws that were substantially similar to PIPEDA with Bill 38, entitled The *Personal Information Protection Act* (PIPA). The Office of the Information and Privacy Commissioner monitors and enforces BC's public sector privacy legislation, *Freedom of Information and Protection of Privacy Act* (FIPPA), in addition to PIPA. The IPC's powers and responsibilities are to:

- investigate and resolve complaints that personal information has been collected, used or disclosed by an organization in contravention of PIPA;
- initiate investigations and audits to ensure compliance with PIPA if the Commissioner believes there are reasonable grounds that an organization is not complying, including issuing binding orders;
- inform the public about PIPA;
- conduct or commission research into anything affecting the achievement of the purposes of PIPA;
- comment on the privacy implications of programs, automated systems or data linkages proposed by organizations;
- authorize the collection of personal information from sources other than the individual to whom the personal information relates; and
- investigate and resolve complaints that a duty imposed by PIPA has not been performed, an extension of time has been improperly taken, a fee is unreasonable or a correction request has been refused without justification[344]

As indicated above, British Columbia recently reviewed its PIPA legislation. The Special Committee to Review the *Personal Information Protection Act*, chaired by Ron Cantelon, reported its statutory review entitled Streamlining

344 "OIPC's Role and Mandate," www.oipc.bc.ca/pdfs/public/OIPC-Role-and-Mandate.pdf.

British Columbia's Private Sector Privacy Law on 17 April 2008.[345] Section 59 of BC's PIPA requires that the statute be reviewed within three years of its introduction and every six years thereafter. The Committee received 31 written submissions, primarily from industry and professional associations, as well as from individuals. The Commission heard a further 12 oral presentations from organizations and individuals at public hearings in Victoria and Vancouver.

When the report was published, a spokesperson for McCarthy Tétrault captured the impact on the private sector in concluding that there has been "a minimal tweaking of the existing legislation" reflecting "a perception that the legislation is working well for both individuals and organizations."[346] Nonetheless, the Committee voiced criticism of the low level of public awareness of the purpose, rules and scope of the act.[347] The Committee made a total of 31 recommendations in an effort to harmonize practices with federal and provincial privacy regulators and to ensure PIPA's continued effectiveness going forward. The key recommendations include:

- Making private-sector organizations accountable for personal information they transfer for processing outside Canada
- Requiring organizations to notify affected individuals of privacy breaches in certain circumstances
- Banning the use of blanket consent forms by provincially regulated financial institutions
- Revising consent exceptions to better address business practices in the insurance industry
- Permitting disclosure of personal contact information for health research
- Retaining the minimal fee for access to personal information
- Streamlining the complaints process in the province's privacy laws
- Strengthening the Information and Privacy Commissioner's oversight powers

With respect to the final recommendation that there be some institutional change to the Privacy Commissioner's office, the Committee recommended two main amendments to PIPA (recommendations 27 and 29). First, the Committee recommended that PIPA be amended to give the Commissioner explicit authority to discontinue an investigation or a review where he believes the complaint or request for review is without merit or where there is

345 SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT, *Streamlining British Columbia's Private Sector Privacy Law*, Victoria, Legislative Assembly of British Columbia, 2008, http://www.leg.bc.ca/cmt/38thparl/session-4/pipa/.

346 Cappone D'ANGELO, "Committee Recommends Amendments to British Columbia's Private Sector Privacy Legislation," *McCarthy Tétrault*, August 8th, 2008, http://www.mccarthytetrault.ca/article_detail.aspx?id=4101.

347 LEGISLATIVE ASSEMBLY OF BRITISH COLUMBIA, "Special Committee recommends changes to streamline B.C.'s private-sector privacy law," April 17, 2008, at the following website : http://www.leg.bc.ca/.

insufficient evidence to proceed. Second, The Committee recommended that PIPA be amended to make it clear that the Commissioner has the discretion not to proceed with an inquiry in certain circumstances, as well as the authority to reasonably determine his own process so that he has control over the time frame for his inquiries. Thus, British Columbia's review process produced recommendations closely resembling those made by the Alberta review Committee.

As in Alberta, the BC Committee recommended that the Commissioners powers and discretion be broadened, though there was no suggestion that the Commissioner's Ombudsman role be fundamentally modified.

The fact that the Ombuds model for privacy commissioners with respect to regulation of the private sector has been viewed favourably in provincial jurisdictions does not mean this model is the most effective, but it does speak to its broad appeal, and the generally positive perception it enjoys.

2.5 Provincial and federal privacy regulation compared

PIPEDA and the Quebec, British Columbia and Alberta privacy statutes differ in key areas.[348] While PIPEDA rules are generally premised on consent, the provincial acts define consent obligations in specific areas like employee information and business transactions. Furthermore, the British Columbia and Alberta Acts contain a grandfathering provision, which omits information collected by the private sector before the Act comes into force from any consent requirements. The British Columbia and Alberta Acts also do not require consent for the collection, use and disclosure of an employee's personal information so long as it is done for "reasonable" purposes, while PIPEDA does not distinguish between personal information collected for employment or commercial activities.

In terms of institutional powers, the Quebec, Ontario, British Columbia, Alberta and federal Privacy Commissioners have the same powers of investigation and mediation, as well as the shared ability to initiate complaints and to conduct audits. The primary difference between the powers of these provincial commissioners and the federal Privacy Commissioner is that they have the added power to issue final decisions in order to settle disputes surrounding complaints, subject to judicial review.[349]

---

348 The Alberta Office of the Information and Privacy Commission has created a useful table comparing various aspects of PIPEDA with Alberta and British Columbia's PIPA: ACCESS AND PRIVACY SERVICE ALBERTA, "PIPA Compared", 2008, accessible online at : http://pipa.alberta.ca/legislation/pdf/PIPAcompared.pdf.

349 Gérard V. LA FOREST, "The Offices of the Information and Privacy Commissioners: The Merger and Related Issues", Ottawa, Department of Justice Canada, 2005, par III, accessible online at : http://www.justice.gc.ca/eng/ip/index.html.

These provincial commissioners have further order-making powers, enabling them to hold inquiries and to order organizations to do what is needed to comply with provincial privacy legislation. What might be termed an "Ombudsman with a stick" model appears to be most effective when it serves as a deterrent, rather than as a means of compelling compliance with privacy legislation, as Commissioners tend to prefer to resolve complaints through conciliation, mediation and informal measures.[350] This is a claim that will be important to substantiate.

In B.C., for example, the OIPC receives about 200 complaints annually, but has had to resort to orders during the first five years (2004-2009) in only a handful of cases (between 15-20 matters have proceeded to formal inquiries). While this number is significant, the meaning of its significance is open to interpretation. Is the paucity of recourse to order-making evidence that order making is necessary, so as to encourage settlement and deter non-compliance with statutory obligations, or is the same statistic evidence that order making is unnecessary, given how rarely it is invoked?

At a minimum, the experience of Canadian provincial jurisdictions where obligations similar to and consistent with PIPEDA are combined with regulators which possess order-making power is instructive. The experience in these provinces demonstrates, for example, that businesses can adapt to a regulatory environment that includes order making without any significant problems. The experience of Quebec, Alberta and B.C. is instructive in another respect as well. All of these provinces have had a chance to observe the OPC's Ombuds model and, in recent statutory reviews, none of the three suggested that the federal model be adopted. In each case, the reviews considered additional powers as part of « second generation » privacy legislation.

2.6 The United Kingdom's Information Commissioner's Office

The U.K. Information Commissioner's Office (ICO) is an independent official body appointed by the Queen who enforces and maintains the register for the 1998 *Data Protection Act* (DPA) and the 2000 *Freedom of Information Act* (FIA). Unlike in Canada where the Privacy Commissioner and the Information Commissioner offices are distinct, the UK's Information Commissioner is a single Ombudsman. The Information Commissioner seeks to "promote public access to official information and protect personal information," and is supervised by both the Courts and the Information Tribunal with respect to this mission.

The DPA regulates the use of personal information, whether it is processed by public authorities or by private organizations. Thus, the Information Commissioner has set standards for data handling, and has established a

350 See ACCESS TO INFORMATION REVIEW TASK FORCE, *Access to Information: Making it Work for Canadians*, Ottawa, Public Works and Government Services, 2002.

notification system with criminal penalties where organizations that handle personal information fail to comply. This information is published in a register of data controllers for public review. Individuals who believe their rights have been violated under the DPA can complain to the Information Commissioner who can,

- Undertake assessments to check whether organisations are complying with the Act;
- Serve information notices requiring organisations to provide the ICO with specified information within a certain time period;
- Serve enforcement notices and "stop now" orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice; and
- Report to Parliament on data protection issues of concern.[351]

The DPA has attracted criticism since its inception, having been described by courts as a "cumbersome and inelegant piece of legislation."[352] In recent years, there have been increasing calls to give the ICO greater investigative and enforcement powers due to a series of embarrassing information leaks and losses, culminating in November 2007 with the loss of 25 million child benefit claimants' records by Her Majesty's Revenue and Customs.

The ICO has seen an increasing number of reported data breaches. The ICO reports that from October 2008 to January 2009, the number of reported breaches increased from 277 to 376. The ICO urges the private sector to make data protection part of corporate governance as 112 of the 376 breaches were in the private sector.[353] Commissioner Richard Thomas[354] responded to the 3-month rise in data breaches by calling for a further increase in ICO powers:

> For more than 20 years, my office has not had the power to carry out any inspection without the consent of the organisation concerned…In the six and a half years that I

351 *Data Protection Act 1998*, ch. 29 (U.K.), Part V, accessible online at:http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&activeTextDocId=3190610.

352 *Campbell* v. *MGN Ltd*, Court of Appeal (Civil Division), (2002) EWCA Civ 1373, (2003) QB 633 (U.K.) (Opinion of Lord Phillips).

353 INFORMATION COMMISSIONER'S OFFICE, "Data breaches reported to the ICO", February 9, 2009, accessible online at: www.ico.gov.uk/upload/documents/pressreleases/2009/data_breaches_ico_statement20090209.pdf.

354 Christopher Graham has been approved by the House of Commons Committee in February 2009 to be the new Information Commissioner beginning in June 2009. At the time this memo was drafted, however, Thomas was still listed as Commissioner on the ICO website.

> have been commissioner, I have strenuously argued that that is not acceptable. One would not expect a food inspector to have to get the restaurant's consent before carrying out an inspection.[355]

On July 7 2008, Thomas voiced further criticism of the Information Commissioner's powers in the Data Sharing Review that he prepared in conjunction with Dr. Mark Walport, who is the Director of Wellcome Trust.[356] In this review, Thomas and Walport evaluated the framework for how personal information is used in the public and private sectors. The review calls for changes within private organizations, both with respect to how they train their employees to deal with personal data and with respect to the culture surrounding how personal information is viewed and handled.

Thomas and Walport call for a stronger regulator to facilitate these improvements. The review supports stronger inspection and audit powers, the implementation of powers to impose financial penalties that had formerly been promised, as well the replacement of the single Information Commissioner with an executive team. The Data Sharing Review inspired a series of legislative reforms, expanding the Commissioner's powers of investigation and enforcement.[357]

Thomas' calls for greater ICO powers were answered by the *Criminal Justice and Immigration Act*, given Royal Assent on 8 May 2008.[358] Section 144 of the Act gives the ICO the power to impose fines on both the public and private sectors where section 55 of the DPA is violated. Section 55 makes it a criminal offence to knowingly or recklessly obtain or disclose personal data without consent. Penalties can be appealed to the Information Tribunal; however, the Commissioner's new power has yet to be brought into force and the Secretary of State has not yet set the maximum penalty. This increased fining authority brings ICO enforcement powers in line with other UK regulators like the Financial Services Authority that was granted the power to impose fines on financial institutions for breaches in data security in 2001. While the Information Commissioner has also called for the ability to impose prison

355 Alexi MOSTROUS, "UK citizens' private information being lost at record rate," *London Times*, February 9, 2009, http://www.timesonline.co.uk/tol/news/politics/article5688347.ece.

356 Richard THOMAS and Dr. Mark WALPORT, "Data Sharing Review," *Ministry of Justice*, July 2008, http://www.justice.gov.uk/reviews/datasharing-intro.htm.

357 The government responded to the Thomas-Walport Review: MINISTRY OF JUSTICE, "Response to the Data Sharing Review Report", November 24, 2008, http://www.justice.gov.uk/publications/response-data-sharing-review.htm.

358 Office of Public Sector Information, *Criminal Justice and Immigration Act 2008* < http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_1>.

sentences for the illegal buying and selling of information,[359] these powers have not been granted to the ICO.[360]

The Information Commissioner's Freedom of Information activities are funded by an annual grant-in-aid from the Department of Constitutional Affairs. The Commissioner's Data Protection activities are funded from the annual notification fees collected from data controllers. In response to Thomas' calls for greater funding for the ICO's private sector regulatory activities, the ICO intends to introduce tiered notification fees,[361] allowing higher fees for larger data controllers who currently pay the standard 35 pounds per year.

The House of Lords undertook a privacy investigation in order to determine "the impact that government surveillance and data collection have upon the privacy of citizens and their relationship with the State" and to ascertain whether the necessary protections are in place.

The report was published on 21 January 2009 and is entitled "The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State." [362] On 13 January 2009, Thomas gave his views on the development of the Information Commissioner role during his tenure to the House of Lords.[363] Thomas lauds the ICO's success in creating greater public awareness of data protection since 2004 and that the Data Sharing Review has had constructive legislative results. Thomas' positive assessment of recent legislative reforms giving the ICO greater powers and funding was largely echoed by the House of Lords in its evaluation of the role of Information Commissioner. The House of Lords expressed satisfaction at the government's agreement to create multi-tiered data protection duties in response to recommendations in the Thomas-Walport review. Nonetheless, the House of Lords echoed the ICO's calls to extend the Information Commissioner's new public inspection power, laid out in the *Coroners and Justice Bill*, to the private sector.

---

359 INFORMATION COMMISSIONER'S OFFICE, "Information Commissioner calls for prison sentences for illegal buying and selling of personal information," May 12, 2006, accessible online at : http://www.ico.gov.uk/global/search.aspx?collection=ico&keywords=prison.

360 DEPARTMENT FOR CONSTITUTIONAL AFFAIRS, "Increasing penalties for deliberate and willful misuse of personal data", October 30, 2006, accessible online at : www.dca.gov.uk/consult/misuse_data/cp0906.htm *[this is a review of the feasibility of prison as a penalty]*.

361 INFORMATION COMMISSIONER'S OFFICE, "Minutes – Management board", January 26, 2009, accessible online at : www.ico.gov.uk/upload/documents/library/corporate/notices/minutes_3_march_2008v1.8.pdf.

362 HOUSE OF LORDS, "Surveillance: Citizens and the State", February 6, 2009, accessible online at : http://www.parliament.uk/hlconstitution.

363 Richard THOMAS, *Evidence to the Justice Select Committee – January 2009*, United Kingdom, Information Commissioner's Office, 2009, accessible online at : http://www.ico.gov.uk/about_us/news_and_views/current_topics/ic_evidence_to_js_committee.aspx.

Section 3: Peer oversight bodies

In addition to focusing on other information and privacy regulators, it may also be helpful to consider the models chosen by other regulators who oversee private sector activity in the public interest, both in Canada and in peer jurisdictions. As with the analysis of peer privacy regulators, our focus is on the criteria by which these bodies have been assessed.

3.1 Canadian Radio-television and Telecommunications Commission

The CRTC is an independent public organization established in 1968 that regulates broadcasting and telecommunications in Canada. The CRTC is overseen by a government appointed board and reports to Parliament through the Minister of Canadian Heritage, who is responsible for broadcasting policy. While the CRTC originally regulated only privately held common carriers (e.g. BC Tel, Bell Canada), court rulings in the 1990s extended CRTC jurisdiction over the entire sector, including roughly fifty small independent carriers.

The CRTC's mandate is laid out in the 1991 *Broadcasting Act*, the 1993 *Telecommunications Act* and the 1976 *CRTC Act*. In broadcasting, the CRTC seeks to regulate and supervise the variety and quality of Canadian programming in addition to ensuring that Canadians have access to jobs in the broadcasting industry. In telecommunications, the CRTC supervises and regulates the quality and cost of telephone and telecommunication services for Canadians. More specifically, in regulating broadcasters and telecommunications carriers, the CRTC is involved in

- Issuing, renewing and amending broadcasting licenses
- Making decisions on mergers, acquisitions and changes of ownership in broadcasting
- Approving tariffs and certain agreements for the telecommunications industry
- Issuing licences for international telecommunications services, whose networks allow telephone users to make and receive calls outside Canadian borders
- Encouraging competition in telecommunications markets
- Responding to requests for information and concerns about broadcasting and telecommunications issues[364]

In addition to these regulatory activities, the CRTC holds consultations with both the public as well as international regulators. Furthermore, the CRTC has the authority to exempt public telecommunications carriers from the *Telecommunications Act*, it may choose not to regulate a sufficiently competitive service, and it can approve tariffs on services already offered by public carriers and can approve agreements and settle disputes among carriers. The CRTC

364 List available on the CRTC website: http://www.crtc.gc.ca/eng/backgrnd/brochures/b29903.htm.

has broad investigative powers and its decisions can be appealed back to the CRTC, to the Federal Court of Appeal or to Cabinet, though this last option is seldom employed. While the court can apply fines, the CRTC itself cannot.[365]

In March 2006, the Telecommunications Policy Review Panel released its report to the federal government recommending that the telecommunications market be substantially deregulated.[366] While the Panel found that the Canadian telecommunications policy and regulatory framework has served Canadians well, it needs to be updated in response to new technology and market developments. The Panel published a 2005 Consultation Paper, in response to which they received nearly 200 written submissions. The Panel drew upon additional policy fora in Whitehorse and Gatineau, and extensive consultation with stakeholders and experts in the telecommunications industry.

The Panel recommended that the *Telecommunications Act* be clarified where it is inconsistent, and updated to foster the goals of promoting access to advanced telecommunications services, enhancing the efficiency of telecommunications markets, and allowing for market forces to achieve Canada's telecommunications policy objectives where possible. Accordingly, the report recommends that the CRTC's economic regulatory activities be scaled-back.

Comparing the Canadian regulatory framework to the framework used in other OECD countries, the Panel recommended the creation of a Telecommunications Competition Tribunal that would facilitate the application of Canadian competition policy to the telecommunications service markets. This temporary Tribunal would examine allegations of anti-competitive behaviour and address deregulation issues. The Panel recommended that the CRTC's powers to resolve technical regulatory disputes (e.g. over rates, conditions of access, sharing of radio towers) be made clear. The report further recommends that the Commission establish an Ombuds office that would protect consumer interests as part of the CRTC's mandate to implement the social policy objectives of telecommunications policy (e.g. promoting greater access).

The Panel recommended institutional reforms to boost the CRTC's professional capacity, including a reduced number of commissioners, which would give the CRTC the capacity to retain expert consultants, transferring Industry Canada's regulatory responsibilities with respect to licensing to the CRTC, greater use of public consultations, and streamlined licensing requirements and regulatory fees.

365 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Canada: maintaining leadership through innovation*, OECD Publishing, 2002, at p. 111.

366 TELECOMMUNICATIONS POLICY REVIEW PANEL, *Final Report 2006,* Ottawa, Public Works and Government Services Canada, http://www.telecomreview.ca/eic/site/tprp-gecrt.nsf/eng/rx00101.html.

Like the OPC, the CRTC has had to respond to a rapidly changing external environment, with new forms and content of media threatening to make established regulatory mechanisms obsolete. For example, the Report states,

> In the Panel's view, the time has come to reform Canada's telecommunications policy and regulatory framework. In spite of the fact that Canada has one of the most competitive telecommunications markets in the world, we continue to have one of the most detailed, prescriptive and costly regulatory frameworks. This framework is particularly burdensome for Canada's major telecommunications service providers, who now face stronger competition in a number of market segments from well-established facilities-based rivals as well as from new entrants. The Panel believes the Canadian telecommunications industry has evolved to the point where market forces can largely be relied on to achieve economic and social benefits for Canadians, and where detailed, prescriptive regulation is no longer needed in many areas.[367]

The 2006 evaluation of Canada's telecommunication policy, including the role of the CRTC, appears to be animated more by perception than an evidence-based approach to evaluation. The Report contains no studies of the past effectiveness of market forces or the cost of regulation to the sector. That said, the telecommunications policy proposals might reflect a trend in the information sector (distinct, for example, from the banking sector) for less state regulation and more market-driven reform.

3.2 Canadian Competition Bureau

The Canadian Competition Bureau is an independent agency that is responsible for the administration and enforcement of the *Competition Act*, the *Consumer Packaging and Labeling Act*, the *Textile Labeling Act* and the *Precious Metals Marking Act*. The Competition Bureau is part of Industry Canada, an institutional connection that has often raised questions regarding the Bureau's independence. The Bureau is headed by the Commissioner of Competition, who has the authority to launch inquiries, challenge civil and merger matters before the Competition Tribunal, make recommendations on criminal matters to the Attorney General of Canada, and intervene as a competition advocate before federal and provincial bodies.

The Bureau responds to consumer complaints on competition issues and investigates anti-competitive behaviour such as price fixing, bid-rigging, false or misleading representations, deceptive notice of winning a prize, abuse of dominant position, exclusive dealing and tied selling and market

367 *Id.*, at p. 1-22.

restrictions, mergers, multi-level marketing plans and pyramid schemes, deceptive telemarketing, and deceptive marketing practices. The *Competition Act* distinguishes between criminal conduct, subject to fines and/or imprisonment, and "reviewable conduct" , subject only to a remedial order. While criminal offences are dealt with by the courts, reviewable practices are dealt with by the Competition Tribunal ("Tribunal"), which is composed of Federal Court judges and laypersons.

Where the Competition Bureau finds that a further investigation is needed, it sends the issue before the Competition Tribunal, which has the power to impose fines and issue orders. Canada has a "bifurcated" system of applying competition law as the Bureau investigates, while the Commissioner recommends action and the courts and Competition Tribunal make decisions. There is debate over how this bifurcated structure is evolving in practice as the Commissioner increasingly plays the primary role in a functionally unitary system.[368]

Since the 1986 *Competition Act* was adopted, Canada has regularly amended its competition law. Between 2002 and 2004 Industry Canada led an extensive review and public consultation process on the *Competition Act* that culminated with the adoption of Bill C-19 that died on the table with the fall of the Liberal government. The Bill would have imposed significant penalties ($1 million for a first offence, and $15 million for a second offence) for violations of abuse of dominance laws, increased penalties for deceptive marketing practices, increased fines for anti-competitive agreements between competitors, and strengthened powers to investigate industries suspected of anticompetitive practices.[369]

Most recently, the *Competition Act* underwent substantial review in June 2008 when the Canadian Competition Review Panel delivered its report, entitled *Compete to Win*, in which Canada's competition and foreign investment law and policy was evaluated.[370] The Competition Policy Review Panel describes the report as "a series of policy recommendations aimed at making Canada a more attractive destination for talent, investment and innovation, as well as a sweeping national Competitiveness Agenda based on the proposition that Canada's standard of living and economic performance will be raised through more competition in Canada and from abroad."[371] More specifically, the panel's

368 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Canada – The Role of Competition Policy in Regulatory Reform*, 2002, www.oecd.org/dataoecd/47/48/1960522.pdf, at p. 18.

369 MINISTRY OF INDUTRY, *Bill C-19*, November 2, 2004, http://www2.parl.gc.ca/HousePublications/Publication.aspx?pub=bill&doc=C-19&parl=38&ses=1&language=E.

370 COMPETITION POLICY REVIEW PANEL, *Compete to Win : Final Report June 2008*, accessible online at : http://www.ic.gc.ca/eic/site/cprp-gepmc.nsf/eng/h_00040.html.

371 COMPETITION POLICY REVIEW PANEL, *Competition Policy Review Panel Releases Report*, June 26, 2008, see : www.competitionreview.ca.

recommendations to the federal government include measures to enhance both the transparency and predictability of competition enforcement, and the penalties available to the Bureau to remedy breaches of the Act. [372] While the *Competition Act* reforms have strengthened the Competition Bureau's enforcement powers, they have left the Bureau's institutional structure largely unchanged. Like the CRTC reform proposal, the criteria for reform of Canada's competition policy is efficiency, effectiveness and modernization.

3.3 U.S. Federal Communications Commission

As in Canada, the watchwords in regulatory settings in the U.S. dealing with information media have been change and reform.

The United States Federal Communications Commission (FCC) was established by the *Communications Act* in 1934 as an independent United States Government regulatory agency with a mandate to regulate interstate and international communications by radio, television, wire, satellite, and cable. The FCC was one of several independent regulatory agencies created in the 1930s out of the New Deal era belief that such a multimember bipartisan group of expert commissioners could regulate with independence.[373] Accordingly, the FCC is comprised of five commissioners who are appointed by the President and confirmed by the Senate for five-year terms that expire on a staggered basis. Commissioners cannot be fired for reasons other than corruption or serious misconduct. The FCC is divided into seven operating bureaus and ten offices that develop and implement regulatory programs, process applications for licenses or other filings, analyze complaints, conduct investigations, and participate in Commission hearings.

While the FCC's 1934 founding Act remains the basis for federal communications regulation, both the *Cable Acts* of 1984 and 1992 and the *Telecommunications Act* of 1996 have significantly altered the FCC's powers.[374] The *Telecommunications Act* established that the FCC has the responsibility of promoting competition and of reducing regulation in order to obtain lower prices and higher quality services for consumers. The FCC carries out this task by rulemaking, notifying the public of a proposed rule and offering an opportunity for public input. These decision-making powers add to the FCC's broadcast licensing powers by which the FCC licenses all major users of the electromagnetic spectrum.

---

372 COMPETITION BUREAU, *Frequently Asked Questions About the Amendment of the Competition Act*, see : http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03046.html.

373 Randolph J. MAY, "The FCC's Tumultuous Year 2003: An Essay on an Opportunity for Institutional Agency Reform", (2004) 56 *Administrative Law Review* 1307, at 1310-1311.

374 Michael J. Zarkin, The Federal Communications Commission, Santa Barbara, Greenwood Publishing Group, 1998, at p. xv.

Congress retains influence over the FCC because the Senate approves the presidential appointments of commissioners, Congress controls the budgets of federal agencies, the FCC is overseen by the Committee on Energy and Commerce and the Senate Committee on Commerce, Science and Transportation, and Congress can direct FCC activity by passing legislation to that effect. Regulated industry exerts a similarly powerful influence over the FCC both by direct lobbying and by its influence over Congress.[375] Thus, while the FCC was intended to be an independent regulatory body, there are several partisan forces influencing its decisions.

There have been many calls for FCC reform as changing technology has sparked debate over the FCC's structure as the communications industry has been described as plagued by outdated regulatory requirements, by a lack of clarity in the agency's decisions and regulations, and by embarrassing delays in reaching decisions and promulgating new rules.[376] The FCC has attracted much criticism for making politicized decisions based on inadequate information and for relying too often on the parties it regulates to bring forward issues and information on which the FCC bases its investigations.[377] The congressional committee looking into the criticisms reviewed several hundred thousand documents, conducted 73 interviews with current and former FCC employees, and with people associated with the telecommunications industry, solicited and received e-mails form FCC employees and contractors and reviewed dozens of allegations.

On 5 January 2009, the public interest organizations Public Knowledge and Silicon Flatirons sponsored a conference and ongoing project entitled "Reforming the FCC."[378] In the "Reforming the FCC" conference, keynote speaker Philip J. Weiser observed, "because the agency operates with limited imagination, almost no strategic thinking or planning, and with an absence of well-developed sources of data to guide its decisions, it often misses

375 *Id.*, at p. 49-54.

376 R.J. MAY, *supra*, note 307, at 1309.

377 On 9 December 2008, the House Energy and Commerce Committee's Oversight and Investigations subcommittee released its findings from a bipartisan investigation into the FCC's regulatory processes and management practices. The investigation was launched on 8 January 2009 when the Committee and subcommittee Chairman's sent a letter to then FCC Chairman Kevin Martin announcing "a formal investigation into FCC regulatory practices to determine if they are being conducted in a fair, open, efficient, and transparent manner." See COMMITTEE ON ENERGY AND COMMERCE, *Deception and Distrust: The Federal Communications Commission Under Chariman Kevin J. Martin*, December 2008, accessible online at : http://energycommerce.house.gov/index.php?option=com_content&task=view&id=1455&Itemid=1.

378 An extensive bibliography on FCC reform as well as discussion papers are accessible on the website http://fcc-reform.org/.

opportunities to chart independent courses of action."[379] Weiser contends that the FCC needs both reformed institutional processes and a new culture. Weiser further found that the FCC lacks transparency, as stakeholders tend to prefer to conduct ex parte meetings behind closed doors, giving limited public notice of their positions. Weiser found that FCC decisions have an arbitrary character, as the Commission lacks a broad policy vision and sufficiently independent leadership.

The move away from ad-hoc, politicized regulation toward evidence-based, strategic regulation in the U.S. is worth consideration.

3.4 U.S. Federal Trade Commission

The prime example of a strategic regulator in the U.S. field closest to the mandate of the OPC under its PIPEDA jurisdiction is the Federal Trade Commission (FTC).

The federal government created the Bureau of corporations in 1903. in 1914, President Woodrow Wilson signed the Federal Trade commission act into law, and the Bureau of corporations became the FTC. The FTC's jurisdiction extends both to consumer protection and competition regulation, which brings broad sectors of the economy under the umbrella of the FTC's jurisdiction. It is a law enforcement agency, as opposed to an Ombuds model, and the FTC administers and enforces a wide variety of laws and regulations, such as the *Federal Trade Commission Act*, *Identity Theft Act*, *Fair credit Reporting Act*, and the *Clayton Act*. The FTC operates its headquarters in Washington, DC, and seven regional offices located across the United States. In 2009, the FTC had a staff of over 1,100 full-time equivalent employees and an annual budget of US$259 million.

The FTC's Bureau of Consumer Protection engages in a range of public education, industry compliance and enforcement activities. The Bureau conducts investigations, prosecutes corporations and individuals in breach of their legal obligations, and shares information obtained through its investigations with other law enforcement agencies both domestically and internationally. The Bureau develops and disseminates rules to protect consumers, and educates consumers and businesses about their rights and responsibilities.

One of the Bureau's seven divisions (and its newest) deals specifically with privacy and identity protection. This division is responsible for protecting consumers' financial privacy, and devotes resources both to investigating breaches of data security and preventing identity theft.

379 Philip J. Weiser, "FCC Reform and the Future of Telecommunications Policy," 2009, at 6, accessible online at http://fcc-reform.org/paper/fcc-reform-and-future-telecommunications-policy.

The Division derives its authority and mandate from multiple statutory sources, including Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, including deceptive statements and unfair practices involving the use or protection of consumers' personal information; The *Fair Credit Reporting Act*, which ensures the accuracy and privacy of information kept by credit bureaus and other consumer reporting agencies, and gives consumers the right to know what information these entities are distributing about them to creditors, insurance companies and employers; and The *Gramm-Leach-Bliley Act*, which requires financial institutions to ensure the security and confidentiality of customer information, provide notice to consumers about their information practices, and give consumers an opportunity to direct that their personal information not be shared with certain non-affiliated third parties. The Division also operates the Identity Theft Data Clearinghouse, which houses the federal government's centralized repository for consumer identity theft complaints. The Division analyzes identity theft trends, promotes the development and efficacy of identity fraud prevention strategies in the financial services industry, and identifies targets for referral to criminal law enforcement. While the FTC's data protection mandate is relatively modest, it has a wide range of tools to draw upon in advancing this mandate, including the power to impose significant fines. In February 2010, the FTC's joint breach notification jurisdiction with the Department of Health and Human Services came into effect, requiring notification of breach involving health records.

The FTC's approach to evaluation is multi-pronged. It engages in annual performance reviews and periodic five-year strategic plans. Its 2009-2014 strategic plan highlights three goals: (1) protect consumers; (2) maintain competition; and (3) advance performance. Each goal includes a set of objectives and each objective includes performance measures, strategies to achieve goals, and methods of evaluation. For example, in furtherance of the goal of protecting consumers, the FTC sets out as an objective: "Identify fraud, deception, and unfair practices that cause the greatest consumer injury." The strategies used to achieve this objective include a "consumer sentinel network" to receive complaints and obtain data on fraud and share it more broadly with a network of law enforcement agencies. The performance measures include the quantity of complaints and inquiries received, the percentage of FTC consumer protection actions that target the subjects of consumer complaints and the rate of consumer satisfaction with the FTC consumer response center. The appendix to the strategic plan includes overall performance measures and annual data. For example, in 2009, the percentage of all cases filed by the FTC that were successfully resolved through litigation, a settlement, or issuance of a default judgment was listed as 75-80%. While impressive, this statistic is not broken down in a manner that would allow the reader to assess whether litigation followed by a judgment was more or less effective than settlement.

Section 4: Measuring the performance of the Office of the Privacy Commissioner: Lessons learned

While there is some degree of international convergence over best practices for privacy protection (for example, the leading European directive 95/46/EC builds on the 1981 obligations and rights set-out by the Council of Europe

Convention No107, which are also similar to both the 1980 OECD guidelines and the 1990 UN guidelines), no similar consensus has emerged as to how to evaluate the performance of privacy regulators.

That being said, expert observers generally agree on assessments of the relative strengths of different privacy regimes. For example, the U.S. privacy regime is commonly regarded as fundamentally weaker than most other regimes, with European privacy regimes attracting the most praise. Such informal rankings are greatly influenced by the fact that the U.S. lacks a federal data protection agency and a comprehensive data privacy legislation regulating its private sector.[380] Nonetheless, beyond such cursory comparative assessments, there have been few rigorous academic studies that explore how privacy regulators ought to be assessed.

The former Australian Privacy Commissioner, Malcolm Crompton observed that there has been too little emphasis on how privacy regulators operate, as "the focus is often on the nature of the legal structures and the economic incentives they create as opposed to whether, within the bounds of the law and surrounding environment, the regulator itself has performed well or badly."[381] As most academic research on privacy issues are generally focussed on the issues themselves rather than on the discourse in theory and political science analysis, there is little holistic evaluation of privacy protection systems.[382]

4.1 The European Union model

The EU Directive on the Protection of Personal Data with Regard to the Processing of Personal data and on the Free Movement of such Data established guidelines for drafters of national data protection legislation.

380 Lee A. BYGRAVE, "Privacy Protection in a Global Context – A Comparative Overview", "Privacy Protection in a Global Context – A Comparative Overview," (2004) 47 *Scandinavian Studies in Law* 319, at 344.

381 Malcolm CROMPTON, "'Light Touch' or 'Soft Touch' – Reflections of a Regulator Implementing a New Privacy Regime", Australia, The Office of the Privacy Commissioner, 2004, accessible online at : http://www.privacy.gov.au/news/speeches/sp2_04p.html#link04. Crompton delivered a speech in March 2004 in which he proposed a framework for measuring the performance of a regulator. Crompton suggests that regulators must be ethical, effective and efficient and lays out a framework for how a regulator's performance on these measures can be tested. Crompton suggests that the performance of a regulator must be founded in an analysis of the regulator's economic impact, social outcomes, public accountability for resources, independence, fairness, transparency and accountability in decision making, active engagement in policy formation, and in efficient, responsible and transparent provision of services. Crompton suggests that all of these benchmarks should be assessed given the environment in which the regulator operates. Crompton looks at different factors that affect the regulator's capacity to exercise power, including: the law, available resources, government expectations, global environment, market forces, and extent of technological change.

382 Charles RAAB, "Beyond Activism: Research Perspectives on Privacy," *TILT Law & Technology Working Paper Series* (22 February 2008), no. 007/2008

Article 29 of the Directive established an advisory body ("Working Party") comprised of representatives from each Member State's supervisory authority, from the European Commission, and from other Community institutions. The Working Party assesses the adequacy of national and third party privacy protection as Article 35 prohibits member states from transferring personal data to other countries unless they have adequate protection. The criteria used by the Working Party to assess privacy regimes has become an important benchmark, as Raab and Bennet observe, "the EU's adequacy provisions are the de facto rules of the road for the increasingly global character of personal data processing activities, and have been a main focus of international attention, debate and controversy."[383]

In July 1998, the Article 29 Working Party developed a consistent approach to determining when a country has achieved an "adequate level of protection" in processing individuals' personal data.[384] In the working document, entitled "Transfer of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive,"[385] the Working Party concluded that both the content of privacy rules and the system adopted to ensure their effectiveness must be evaluated in assessing the adequacy of a data protection regime,

> Using directive 95/46/EC as a starting point, and bearing in mind the provisions of other international data protection texts, it should be possible to arrive at a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate.[386]

While these requirements are meant to be applied flexibly given the context, the Working Party has laid out two lists of basic requirements for adequate data rules and enforcement mechanisms.

---

383 Charles RAAB and Colin BENNETT, "The Governance of Global Issues: Protecting Privacy in Personal Information," *European Consortium for Political Research*, 2003, p. 6.

384 Peter J. HUSTINX, Adequate Protection – Opinion 6/99 of the Article 29 Working Party revisited," *Ten Years of DP & FOI Commissioner's Office, 2006*, p. 251, see : http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/231.

385 WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, *Transfer of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, European Commission Internal Market and Financial Services, 24 July 1998, accessible online at : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf

386 *Id.*, at p. 5.

The Working Party's basic content principles for privacy regulations are:

1. The purpose limitation principle: data should be processed for a specific purpose and subsequently used for related purposes, with limited exceptions.
2. The data quality and proportionality principle: data should be accurate, up-to-date, adequate, relevant and not excessive in relation to the purpose for which the data was transferred or processed.
3. The transparency principle: individuals should provided with information as to purpose of the processing and the identity of the data controller in the third country, with limited exceptions.
4. The security principle: the data controller should take technical and organizational security measures appropriate to the riskiness of the data processing.
5. The rights of access, rectification and opposition: with limited exceptions, the data subject should have a right to obtain a copy of all data related to him, to rectify inaccurate data, and to object to its processing.
6. Restrictions on onward transfer: further transfers of personal data by the original recipient should be permitted only where the second recipient is also subject to rules affording an adequate level of protection, with limited exceptions.

The Working Party has developed further requirements for when data is sensitive, or is used for direct marketing or is used for an automated decision.

The Working Party has identified three objectives of data protection systems that can be used to evaluate enforcement mechanisms. These three objectives are:

1. Deliver a good level of compliance with the rules, where data controllers have a high degree of awareness of their obligations and data subjects similarly have a high degree of awareness of their rights and how to exercise them. Effective sanctions and systems of direct verifications by authorities, auditors, or independent data protection officials can be important in assuring compliance.
2. Provide support and help to individual data subjects enabling individuals to enforce their rights quickly and effectively and without prohibitive cost. This requires an institution that facilitates an independent investigation of complaints.
3. Provide appropriate redress to the injured party where rules are not complied with, requiring a system of independent adjudication or arbitration allowing compensation and/or sanctions where appropriate.

The Commission of the European Communities' November 2006 assessment of PIPEDA illustrates how these criteria and guidelines are meant to be applied.[387] The Commission concluded that PIPEDA "continues to provide an adequate level of protection of personal data within the meaning of Article 25 of the Directive."[388] The Commission found that PIPEDA reflects the Directive's principles as it requires that data transfers be limited to a specific purpose (though with exceptions for cases where transfers are necessary in a free and democratic society) and data must be accurate, complete and up-to-date in view of the purpose for which they are collected and processed. Moreover, PIPEDA requires transparency, access and correction rights and security measures designed to protect information, while onward data transfers are limited to recipients who are also subject to rules providing adequate protection. The Commission commended PIPEDA's consent requirements that vary in relation to the sensitivity of information. Furthermore, other member states' data protection authorities have not had difficulties with data transfers to Canada. Lastly, the Commission commended the OPC's independence and powers, as complainants have recourse to the Federal Court in cases where their privacy has been violated, compensating, in their view, for the Commissioner's lack of enforcement powers.

It is worth noting European concerns regarding a Canadian regulator's constrained enforcement powers is worth noting. In her recent study of privacy regulation in Europe (France, Britain, Germany and Italy), Francesca Bignami links the massive structural transformation in Europe over the past twenty-five years (highlighted by the privatization of state-owned industries, the liberalization of markets, and the rise of the European Union) with a tangible change in European regulatory styles. European regulatory culture was generally thought to be informal and flexible compared to the litigation-driven and legalistic American regulatory style. Bignami argues that European countries are converging on a model of administration that relies on legalistic regulatory enforcement and that gives market actors extensive opportunities for self-regulation, but that otherwise leaves intact earlier regulatory styles. In particular, contrary to claims of Americanization, litigation remains a relatively insignificant component of the regulatory process. The explanation for the emerging regulatory model— which she terms "cooperative legalism"— reflects both the diffusion of self-regulation from northern to southern countries

387 COMMISSION OF THE EUROPEAN COMMUNITIES, *The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act*, November 2006, accessible online at : http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/canada_st15644_06_en.pdf. See the website of the European Data Protection Supervisor : http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/78.

388 *Id.*, at p. 6.

within the EU and the pressure on national governments to demonstrate their commitment to EU policies through enforcement.[389]

Cooperative legalism captures two interlinked trends, namely, the desire for greater enforcement and the preference for self-regulation. Bignami explains that this twin dynamic is particularly apparent in the context of privacy regulation:

> Tougher enforcement and more self-regulation are regulatory imperatives experienced on the ground by policymakers and administrators seeking to deal with an unwieldy and quickly changing market environment. This is especially the case in a policy area like data privacy, where new information technologies have dramatically expanded the population of firms and citizens covered by regulation and the fast-paced nature of technology change makes it particularly difficult for regulators to keep up with social and economic realities. On the one hand, regulators, outnumbered by market actors and faced with growing societal demands, do not have the resources necessary to flexibly apply policy mandates to the circumstances of individual firms. Neither can they rely on informal, trust-based compliance mechanisms in expanding markets. Thus they must set down rules, backed by a significant probability that violators will be caught and suffer consequences—inspections and sanctions. On the other hand, the same societal overload and market complexity drives regulators to enlist market actors in devising regulatory solutions and achieving public goals. Bureaucrats, short on resources and expertise, ask market actors to self-regulate.[390]

Cooperative legalism represents a helpful framework to understand the support apparent in Canada both for a greater role for the state and for a greater role for the market. The measure of the OPC in the future may well be how effective it is in demonstrating progress and achievements in both contexts.

European jurisdictions also reflect a wide range of regulatory options. One of the most activist regulators is Spain's Data Protection Agency (AEPD). In Spain, data protection is constitutionally entrenched through Article 18.4 of the Constitution, which states that "the law shall restrict the use of informatics in order to protect the honour and the personal and family privacy of Spanish citizens, as well as the full exercise of their rights".

389 Francesca BIGNAMI, "Cooperative Legalism", 2009, (on file with the authors – please note we do not yet have permission from Professor Bignami to circulate her paper beyond our team but will obtain permission prior to finalizing the report).

390 *Id.*, at p.11.

This provision was further developed by Organic Law 5/1992 on the Regulation of the Automatic Processing of Personal Data.[391] The Spanish Data Protection Agency was formally created by Royal Decree 428/1993 of 26 March.

The AEPD has at its disposal a range of regulatory tools,[392] including the levying of fines, a data protection general registry (by 2007, more than one million filing systems have been registered, with the largest increases in filing systems belonging to private companies, particularly those of small and medium-sized companies and independent professionals). The AEPD also engages in a wide array of enforcement activities, which is essential for raising the profile of citizen's rights, and which in turn increases the breaches brought to the regulator's attention. In 2007, complaints were up 7% (to 1263 annually), with a particular focus on financial and telecommunication institutions. Video surveillance complaints were up a striking 400% over the previous year following an outreach and public education campaign. The AEPD resolved 399 proceedings involving sanctions, a 32.5% increase, which resulted in over € 19.5 million in fines. While the number of investigations and resolutions are up, the number of resolutions resulting in fines being levied are down, which the AEPD claims is an indication that it is able to ensure compliance through the threat of fines and orders without actually having to resort to these steps as often. In a sense, therefore, Spain may represent an example of cooperative legalism in action.

4.2 Towards an evaluative framework

While scholars such as Bignami have attempted to explore trends in privacy regulation, Charles Raab and Colin Bennett have been working to develop an evaluative framework for privacy regulators.[393] In their 1996 article entitled "Taking the measure of privacy: can data protection be evaluated?" Raab and Bennett explored the hazards of evaluating data protection, and revisited this question in their 2003 book, *The Governance of Privacy,* in which they assessed the possibility of 'measuring' the effectiveness of data protection systems by investigating "the extent to which certain standards of data protection can be objectively identified and moulded into a reliable instrument for measuring the performance of these systems, both over time and comparatively."[394]

Raab and Bennett identify two primary goals that serve as reference points for evaluating data protection: 1. protecting privacy, and 2. promoting good

391 Law 5/1992 was subsequently amended by Organic Law 15/1999 on the Protection of Personal Data. Organic Law 15/1999 implemented Directive 95/46/EC into Spanish law.

392 For discussion, see AEPD's information brochure accessible online at https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/AEPD_en.pdf.

393 Raab and Bennett have produced a series of reports over the years that have culminated with their 2003 publication of *The Governance of Privacy* in which they devote a chapter to measuring privacy regimes.

394 C. RAAB and C. BENNETT, *supra*, note 74, at p. 187.

information technology practices. They argue that data protection regimes typically seek to balance these two goals by aiming to provide privacy to individuals without unduly interfering with the conduct of government or business.[395] In this context, Raab and Bennett propose four measures of the quality of a data protection regime:

- **Economy**: the cost of input resources, i.e. money and staff deployed by the data protection agency and by data controllers.
- **Efficiency**: the relationship between inputs and outputs, the latter being much more difficult to assess. Outputs of a regulatory agency might include the advice and guidance they give to the public and to policymakers, negotiation of codes of practice, publicity materials, enforcement decisions, and the maintenance of a register of data controllers.
- **Effectiveness**: the relationship between outputs and ultimate objectives, which can be difficult to assess where there are multiple or vague goals and where it is not obvious how to match specific goals with specific performances. As there may be no consensus on outcomes, inputs and outputs may have to serve as proxies for outcomes. A more complex approach to effectiveness and its distinguishing facets from efficacy and efficiency is set out in Part 1.
- **Equity**: while this distributional criterion is not part of a conventional privacy analysis, it is worth evaluating who gets data protection, as well as who gets the most extensive data protection.

Raab and Bennett argue that there are at least five possible subjects for assessment that evaluators of data protection regimes can consider.

- **The Law**: its scope (i.e. whether it covers both private and public sectors), clarity, consistency (i.e. whether there is room for interpretation in its definitions and in how rights and responsibilities are allocated), scope of exceptions, possible remedies and sanctions, enforcement machinery, the extent to which the law is tied to technologies.
- **The implementation machinery**: taking into account formal appraisals by independent bodies, internal measurements and reports on activities that indicate productivity via statistics on the number of inquiries handled, information booklets disseminated, orders or rulings made etc.
- **The performance of data-users**: how well data-users comply with the law and fair information principles, which can be discerned by looking at data-users' own "privacy auditing," which is sometimes mandated by privacy regulators.
- **The performance of data-subjects**: the degree to which the general public is aware of privacy dangers and how they can abate them, which can be assessed by looking at the public's protective behaviour. E.g. by the number of complaints, as well as by surveys of public attitudes towards privacy.

395 *Id.*, at p. 193.

- **The data-protection system as a whole**: measure whether the data system has 1. A strong and unambiguous law, 2. An active and assertive regulatory authority, 3. A strong commitment by users, 4. Vigilant, concerned and activist citizenry. Such holistic evaluations capture the interactions of the different parts of the privacy regime, but are less useful in diagnosing how to improve performance.

In evaluating the performance of regulatory authorities, Raab and Bennett observe that such evaluation can be facilitated by the internal records that these authorities tend to keep for annual reports and for similar internal reviews. Nonetheless, they stress that such quantitative measurements can be misleading as it can be difficult to transform statistics on inputs and outputs into performance indicators. Moreover, outputs should not necessarily be equated with the achievement of goals (e.g. where there is an increased number of complaints, this may indicate greater public awareness of the regulatory body rather than growing dissatisfaction). Thus, Raab and Bennett suggest that more qualitative indicators can yield less contradictory insights in assessing how effectively a regulator is able to influence government or business policy. They conclude by finding:

> Quantitative indicators generally assume a 'top-down' approach to evaluation: an unambiguous definition of goals, a measurement of goal attainment across time, across organizations, across sectors, across technology and ultimately across systems. In contrast, qualitative indicators lend themselves to a 'bottom-up' approach which is concerned with evaluation as diagnosis…Although the measurement of performance and the use of indicators owes more to the 'top-down' approach, the realism of the 'bottom-up' perspective may have much to commend it because it opens up to analysis those situations in which the formulation and implementation of policy run together.[396]

We believe a balanced approach to evaluating the OPC is optimal. In the context of the OPC, qualitative and quantitative performance analyses seem feasible in light of the July 2007 5-year PIPEDA review, the significant and growing body of scholarship analyzing PIPEDA, the extensive data available on OPC activities and the information contained in its Annual Reports. We also believe it is necessary to augment this analysis with interviews with key stakeholders and experts, journalistic accounts and other narrative resources.

396 Charles RAAB and Colin BENNETT, "Taking the measure of privacy: can data protection be evaluated?", (1996) 62 *International Review of Administrative Sciences* (1996) 535, at 553-54.

4.3 Provincial privacy regulators' review processes

Raab and Bennett's dichotomy of qualitative and quantitative evaluative approaches correspond to the two primary types of review that privacy regulators typically undertake: periodic reviews and annual reports.

Alberta, British Columbia and Quebec have their own private sector privacy legislation that covers the same areas that PIPEDA covers in other provinces. All three provinces have undertaken relatively recent broad reviews of their private sector privacy regimes.

In Alberta, the review process culminated in the November 2007 report entitled *Review of the Personal Information Protection Act*.[397] British Columbia undertook a similar review process that resulted in the publication of the 2008 report, *Streamlining British Columbia's Private Sector Privacy Law*.[398] Similarly, Quebec underwent its quinquennial review of its provincial privacy regime, which was initiated by the Commission d'accès à l'information's internal review that produced a report entitled *Une réforme de l'accès à l'information: le choix de la transparence*.[399] As part of the quinquennial review, this internal report was followed by a May 2004 report by the Commission de la culture that relied on the public review process,[400] in a similar fashion to the reviews undertaken by the Alberta and British Columbia governments in reviewing their private sector privacy regimes. The report emanating from the Commission de la culture's study will be assessed below along with the Alberta and British Columbia reports. The Quebec quinquennial review encompassed the entirety of the province's privacy regime, though only those sections covering private sector privacy regulation are assessed below.

397 SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT, *Streamlining British Columbia's Private Sector Privacy Law*, Victoria, Legislative Assembly of British Columbia, 2008, http://www.leg.bc.ca/cmt/38thparl/session-4/pipa/

398 SELECT SPECIAL PERSONAL INFORMATION PROTECTION ACT REVIEW COMMITTEE, *supra*, note 331.

399 COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Une réforme de l'accès à l'information: le choix de la transparence*, November 2002, see : http://www.cai.gouv.qc.ca/.

400 ASSEMBLÉE NATIONALE, COMMISSION DE LA CULTURE, "Observations, conclusions et recommandations à la suite de la consultation generale et des auditions publiques à l'égard du document intitulé: *Une réforme de l'accès à l'information: le choix de la transparence*", May 2004, see : http://www.cai.gouv.qc.ca/.

Jurisdiction	Review Body	Method
Alberta	Select Special Personal Information Protection Act Review Committee	The consultation was initiated in July 2006 when the committee distributed a Discussion Guide to more than 362 organizations. The committee received 65 submissions in response, 24 of which came from industry and business or professional associations, 18 from individual organizations, 13 from professional regulatory organizations and seven from individuals. The committee also heard 10 oral presentations from various organizations and individuals.
British Columbia	Special Committee to Review the Personal Information Protection Act	The committee placed two call-for-submission ads in the province's daily newspapers, and sent e-mail invitations to over 130 organizations asking them to participate in the statutory review process. 31 individuals and organizations made written submissions and the committee held 11 public hearings in Victoria and Vancouver, in which they heard 12 presentations from individuals and organizations.
Quebec	Commission de la culture	45 individuals and organizations made written submissions and 37 of these participants also made presentations during public hearings (September to October 2003).

Criteria	Regulators
Whether the provincial privacy legislation is consistent with PIPEDA	Alberta
Adequacy of protection of information transferred outside the province	Alberta, BC, Quebec
Whether there should be a mandatory notification requirement for privacy breaches	Alberta, BC
Whether/How provincial privacy legislation should apply to non-profit organizations	Alberta
Whether/How provincial privacy legislation should apply to health information	Alberta
Appropriateness of consent requirements	Alberta, BC
Adequacy of protection of personal employee information	Alberta
Adequacy of regulation of access by a data-subject to his personal information	Alberta, BC
Adequacy of regulation of fees for accessing and correcting personal records	Alberta
Adequacy of regulation of professional regulatory organizations (e.g. for doctors, lawyers)	Alberta, Quebec
Adequacy of regulations controlling how records are managed within an organization	Alberta
Commissioner investigative and enforcement powers (early dismissal of complaints, solicitor-client privilege, enforcement powers, time limits for inquiries, audit powers, powers of investigation, etc.)	Alberta, BC, Quebec
Frequency at which privacy legislation must be reviewed	Alberta
Whether organizations should be obligated to publicize their privacy policies	BC
Whether institutional procedures should be undertaken in order to diminish delays	Quebec
Accessibility of privacy protections to handicapped people	Quebec

Annual reports

In addition to periodic performance reviews, provinces with their own private-sector privacy laws publish annual financial statements and performance reports.[401] These performance reports provide quantitative data tracking outputs as they change over time. There is a large degree of consensus over what quantitative data should be measured and reported every year. Trends in this reporting are organized below:

Criteria	Regulator
Number of cases opened	Alberta, BC, QC
Who initiated cases (i.e. Commissioner, public or public body)	Alberta, BC
Type of case opened (e.g. request for information, request for review, complaints etc.)	Alberta, BC
Time taken to close cases	BC, QC
Number of cases closed	Alberta, BC, QC
Type of cases closed	Alberta, BC
Method of resolution (e.g. by order or by mediation/ investigation)	Alberta, BC, QC
Summaries of selected mediated cases	BC, QC
Number/details of investigation reports published	Alberta
Number/details of case summaries published	Alberta
Number of compliance resources published in collaboration with other private sector privacy regulators	Alberta, BC
Conferences and statutory/institutional review	Alberta, BC, QC
Summaries of orders issued	Alberta, BC
Summaries of court decisions and judicial reviews	Alberta, BC

Thus, while there is no single generally accepted study of how to evaluate privacy regulators, a rough consensus can be inferred from trends in how provincial regulators evaluate themselves, or are evaluated by Government/ Parliament. There is significant convergence in the criteria they use.

401 For Alberta, see : http://www.oipc.ab.ca/pages/About/AnnualReports.aspx; for BC, see : http://www.oipc.bc.ca/ann_report.htm; for Quebec, see : http://www.cai.gouv.qc.ca/index.html.

4.4 A review of existing evaluative approaches

The goal of our analysis is to build on and extend existing knowledge about the effectiveness of the OPC's administration of PIPEDA. How is the performance of the Office of the Privacy Commissioner currently measured?

As noted above, in 2006-2007, the House of Commons Standing Committee on Access to Information, Privacy and Ethics launched the first five-year-review of PIPEDA. The committee received 42 submissions from organizations, 16 submissions from individuals and 5 submissions from privacy and consumer advocates and privacy commentators. The consultation paper identified 12 key issues for consideration that ranged from the Commissioner's powers to PIPEDA's standards and procedures. The committee often found that there was no consensus among respondents, which is not surprising given how broad the questions in the consultation document were. The OPC further reviews its own activities in an Annual Report to Parliament, and periodic studies such as the *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA)*.

While these Annual Reports and Reports include broad reviews of major issues and investigations, they focus primarily on output performance measures.[402] Through these annual reports, the Privacy Commissioner keeps a record of such measures as the number of PIPEDA inquiries, the number of investigations, the time it takes to close investigations etc. The OPC further produces annual Audits by the Office of the Auditor General and the Public Service Commission that gives a sense of how the OPC has performed in terms of input performance measures.[403] The OPC's Annual Report and Departmental Performance Reports offer a more empirical quantitative assessment of the Commissioner's performance, in contrast to the more impressionistic five-year review. The combination of these evaluative efforts provides a rich and constructive point of departure for this analysis.

We believe that the evaluation of PIPEDA and the OPC to date may be enhanced by incorporating the lessons learned from other Canadian jurisdictions (notably Quebec, Alberta and B.C.) as well as from the U.S. and U.K settings. We also believe that qualitative data about stakeholder and academic assessments of the OPC may enrich the comparative analysis presented above.

4.5 A review of perceptions of the OPC

As part of our analysis, we conducted a series of interviews in order to gain a better understanding of how the current model of OPC activities under

402 Reports on the Personal Information Protection and Electronic Documents Act, see : http://www.priv.gc.ca/information/02_05_b_e.cfm#contenttop.

403 OPC Audits by the Office of the Auditor General and the Public Service Commission, see : http://www.priv.gc.ca/information/an-av_e.cfm#contenttop.

PIPEDA is perceived. Below, we discuss the questions we posed in these interviews and the responses provided.

1) Is the Office of the Privacy Commission (OPC) fulfilling its statutory agenda under PIPEDA?

Respondents indicated that the OPC is generally well regarded and has had notable successes in encouraging voluntary compliance with PIPEDA obligations, particularly with respect to larger and more established industries. To some extent, the effectiveness of the OPC is bound up with the effectiveness of PIPEDA itself. Survey data suggests PIPEDA has made a positive difference in the way large (100+ employees), medium (21-100 employees) and small businesses (1-20 employees) handle the personal information of their customers.

An EKOS survey conducted in March of 2010 demonstrates the impact of PIPEDA.[404] The respondents to that survey were asked about the impact of PIPEDA on their company. Over two-thirds of the survey respondents indicated they were more concerned about protecting their customers' personal information due to PIPEDA and a similar proportion stated that PIPEDA had increased their awareness of privacy obligations. Over half the respondents credited PIPEDA with improved security of personal information and one third believed PIPEDA had resulted in fewer breaches of their customers' personal information.

While that survey did not explore the activities of the OPC directly, those with whom we spoke regard the OPC as innovative in terms of outreach, its support for research and grassroots initiatives. It is lauded for its collaborative approach to working with industry and consumer groups.

The investigation into privacy protection at Facebook in 2009 was cited by many as a turning point, both in enhancing the credibility of the OPC and in significantly raising its profile, particularly among younger Canadians.

While the Facebook settlement demonstrates the upside potential of the OPC's complaint-based compliance activities, some respondents also emphasized that the OPC has been limited by its lack of resources, especially in terms of prevention and raising profile.

While respondents are positive about the evolution of the OPC, the consensus is that the OPC has been less successful in achieving fulfilling its agenda with respect to the medium and especially the small business sector. Small business represents approximately 85% of all businesses in Canada. Small businesses tend to view privacy concerns as an added cost with little added value, and it

404 See EKOS, *Canadian Businesses and Privacy-Related Issues* (March 2010) at http://www.priv.gc.ca/information/survey/2010/ekos_2010_01_e.pdf (accessed July 15, 2010), at p.18.

is in this setting that respondents tend to highlight the shortcomings of the OPC's model, and its lack of enforcement powers in particular. In this sector, the OPC has failed to create significant incentives for compliance.

The EKOS survey discussed above indicated small businesses are less likely to be aware of privacy laws, less likely to have privacy policies in place, less likely to have implemented the policies which they do have, and less likely to have safeguards in place to protect personal information.[405]

One of the areas where progress is recognized but respondents believe more needs to be done is with respect to backlogs.

Other respondents pointed to the failure of the OPC to "name names" in relation to businesses complained against, which limits its publicity leverage.

The quality of reasons and findings was seen as improving over time, though some respondents believe an impediment of the Ombudsman model is the limited detail provided to accompany decisions.

While the OPC's administration of PIPEDA is becoming more sophisticated, some respondents felt a more consultative approach to guidelines, and the development of a rapid settlement regime would enhance the effectiveness of the OPC.

Finally, while the objectives of PIPEDA in the protection of personal information might appear self-evident, several respondents highlighted that that the OPC has not devoted significant attention to establishing performance objectives and benchmarks in relation to PIPEDA.

> *2) We are particularly interested to know your views on the idea of the OPC having greater order-making or enforcement powers. Would you support this idea? Could you explain your thoughts on this issue?*

Respondents from industry groups tended to support the status quo powers of the OPC, and to highlight the effectiveness of the Federal Court as an ultimate "stick," but most other respondents would be in favour of greater order-making powers, particularly as a means of inducing and ensuring compliance in the small and medium business sectors. While most respondents favoured providing the OPC with order-making powers, most also agreed that these powers should be used sparingly. Rather, they believed that possessing a credible and effective threat of order making, would enhance the effectiveness of the OPC's other proactive and educational activities.

Some respondents adopted an approach that recourse to an order-making power should be had only when necessary. They highlighted the ways in which

405 Ibid. at pp. 5, 7-8 and 13.

existing powers could be used more creatively to achieve similar results. They observed that the cautiousness of the early years of administering PIPEDA needs to be replaced with bolder initiatives. For example, creating a certification regime for businesses could be far more effective in the small and medium business sector than the threat of sanctions.

Other powers, such as auditing, could be further enhanced with additional resources. Mandatory breach notification creates further possibilities for enhanced compliance tools short of order-making powers.

While order making may not address all the problems the OPC has had in ensuring compliance with PIPEDA, most respondents recognized that, logically, order-making power would enhance compliance. The experience of provincial privacy commissioners, moreover, is that compliance is enhanced even when order-making powers are used sparingly. OSFI is another example of this model.

Beyond enhancing compliance, respondents noted other benefits to order-making regimes, including greater rigour and detail in the findings released by the regulator. The profile and importance of industry compliance officers also would be enhanced if such individuals were responsible for avoiding sanctions, which in turn likely would lead to greater resources being allocated by the private sector to PIPEDA compliance.

3) How do you believe the private sector would react to the OPC having greater order-making or enforcement powers?

Respondents believe that whether or not order-making powers would harm industry, they will likely oppose it on principle, or because they originally opposed such powers and would have no basis to change their position. Some indicated that the establishment of the Ombudsman model was perceived as a "victory" for industry at the time. Others indicated that industry was sceptical about order making powers at the outset and "the case has yet to be made" that such powers are needed.

On the other hand, some respondents emphasized that the private sector has adjusted well to similar jurisdiction in the context of provincial privacy commissioners. Other respondents observed that the relationship of trust between established industries and the OPC make the prospect of order making powers less concerning than might have been the case a decade ago.

4) What criteria do you believe should be used in assessing the OPC's activities under PIPEDA?

Respondents raised a wide range of possible criteria and metrics by which to evaluate the effectiveness of the OPC's PIPEDA activities. These include:

- Surveying businesses across different sectors (business, consumers, etc) to ascertain how the OPC and PIPEDA are perceived

- Carrying out studies into the "credibility" of the OPC and PIPEDA in the media
- Developing a strategic plan with transparent performance benchmarks and targets in terms of compliance with PIPEDA, and OPC processes (e.g. reducing backlog, delay, etc.)
- Focusing on more strategic activities in the context of higher risk areas
- Developing compliance metrics to allow for longitudinal and latitudinal analysis
- Assessing whether consultation processes are viewed as worthwhile (and what impact these processes have on the outcomes). Obtain the views of those who participate in multiple consultation exercises regarding the OPC's position in relation to peer regulators such as FCAC and/or OSFI

5) What future challenges, if any, do you see affecting the OPC's activities under PIPEDA?

This open-ended question generated a broad array of responses, including:

- Technological convergence and new uses (and abuses) of personal information
- Emerging generation of young people who view privacy in entirely different ways – shaped through social networking
- A significant loss in a court case could undermine the OPC's credibility
- The increasing need for borderless privacy protection, and expectation that Canada will exercise leadership (e.g. Facebook)
- The increasing need for better coordination with other regulators (e.g. working with the CRTC to enhance the effectiveness of the no-call list or anti-spam measures)

CONCLUSIONS TO PART II

In this part, we have explored in greater detail the operational environment of the OPC in relation to PIPEDA. In order to highlight appropriate evaluative criteria, we have explored empirical, comparative and normative perspectives on the OPC's Ombuds model.

From an empirical perspective, we discussed why a review of OPC's outputs based on dates alone is unsatisfactory. Whether the number of inquiries or complaints has gone up or down does not disclose whether the OPC's model for assuring compliance with PIPEDA is successful. The data alone can support any number of arguments about the OPC's effectiveness or ineffectiveness. We also believe that qualitative data about stakeholder and academic assessments of the OPC enriches the quantitative data. Especially striking is the widely shared perception that the OPC's model is far more effective in established industries such as banking and insurance, than in the small business context, where personal information is likely to be most vulnerable.

From a comparative perspective, we believe that the evaluation of PIPEDA and the OPC to date may be enhanced by incorporating the lessons learned from

other Canadian jurisdictions (notably Quebec, Alberta and B.C.) and the U.S. and U.K.

From other Canadian jurisdictions, for example, we noted that the Quebec experience highlights that independence and impartiality, as core administrative law norms, provide the backdrop against which institutional design and the search for the optimal model take place. The Alberta and B.C. examples demonstrate that an Ombuds model may coexist with and complement a range of enforcement and compliance measures, including order-making powers.

U.S. examples such as the FCC and the FTC reflect the move away from ad-hoc, politicized regulation toward evidence-based, strategic regulation. This approach to regulation emphasizes planning, benchmarks and performance evaluation. From Europe, we observed that cooperative legalism represents a helpful framework to understand how a greater role for the state and for the market may be complementary aims for a privacy regulator. The European example, like that of other Canadian privacy regulators, suggests a complex and complementary mix between Ombuds and order making models.

From a normative perspective, we analyzed how any choice of evaluative criteria is an expression of particular values. For example, Bennett and Raab's prioritizing of economy, efficiency, effectiveness and equity, which resonate in the privacy sphere, suggest that measuring distributive justice in privacy regulation (who has more of their data protected than others?) is as important as ensuring compliance by industry.

Whether viewed from an empirical, comparative or normative point of view, we believe there is a basis both to confirm that the OPC's Ombuds model is a success, which has had a concrete and significant impact on the goals set out in PIPEDA, and to suggest that the OPC remains constrained from fulfilling its mandate under PIPEDA. There is strong support, for example, for the argument that a shift toward a consumer protection orientation of PIPEDA, or a push to ensure small business compliance with PIPEDA, requires greater order making power to complement the existing Ombuds responsibilities.

In the third and final section, we sketch how a blend of the creative use of existing powers and additional order making powers might lead to more efficient and effective activities to enhance compliance with PIPEDA.

GENERAL CONCLUSIONS AND RECOMMENDATIONS

The following conclusions and recommendations are based on our analysis and informed by our review of the relevant literature, including primary and secondary studies, reports and articles, and our discussions with a range of people with insight and expertise on the OPC's Ombuds model, including OPC staff, academic experts on privacy law and policy, lawyers who advise clients on PIPEDA, and representatives of industry groups. Our discussions were not exhaustive, but rather provided valuable, qualitative insight into the questions we have sought to address in this study.

There is a subjective element to our conclusions and recommendations as well. They represent our best judgment as to the effectiveness of the OPC's Ombuds model in light of the criteria we have mapped out in Parts 1 and 2 of this study, and the mechanisms which in our view have the potential to further enhance the effectiveness of the OPC.

Through the Ombuds model, and existing compliance activities, the OPC has succeeded in achieving important goals. These include:

- Raising PIPEDA compliance levels, through working with particular industries (e.g. banking, airlines, insurance, etc) and on particular issues (e.g. social networking, etc);
- Building trust in the business sector, collaborating with business and privacy advocates/NGOs, and developing relationships with privacy/compliance officers and industry groups;
- Providing guidance on the interpretation of PIPEDA standards;
- Responding to complaints, inquiries and concerns; and
- Enhancing the profile of privacy issues generally and PIPEDA specifically.

The recent positive media coverage of the OPC's response to concerns with Facebook and Google highlight the success and potential of the Ombuds

model, and its growing reach into new areas of consumer protection (e.g. youth engaged in on-line activities involving their personal information). However, in light of these achievements, should more be accomplished and, if yes, how should it be done?

As we have explained in Part 1, dominant economical, political and legal ideas circulating in the 1990's shaped the OPC's Ombuds model. For example, at the time of its inception, the OPC's Ombuds model was the result of a policy compromise whose ultimate form was, in part, a response to concerns in the private sector about intrusive and costly regulation, and a response to growing political concerns over the vulnerability of personal information in the private sphere. Understanding the evolution and the shifts of these ideas is crucial to not only explaining the evolution of the OPC's jurisdiction with respect to PIPEDA but also to supporting the direction it could take in the future.

On this point, there is no doubt that more research will be needed to better understand the actual environment and to make projections as to future trends. Indeed, an adequate examination of the effectiveness of an institutional model requires that attention be paid to several key macro and micro factors that affect its functioning. As a consequence, our report should be read as an exploration of key factors bridging the context of the emergence of PIPEDA with the current context with a view to identifying paths for further research. From this perspective, we begin our recommendations with a call for further research in the following areas:

- **Recommendation #1: Future research questions**

1. What challenges does Web 2.0 pose and what new issues are raised by this new environment, particularly with respect to the harmonization of regulations and mechanisms for the protection of personal information at the national and supranational levels?
2. Does the Ombuds model instituted by PIPEDA adequately meet these new challenges and address today's issues? While this research has focused on the Ombuds model for the OPC, other, more radical changes may also be explored, such as the creation of a decentralized regulatory agency rather than an administrative commission. What are the advantages and drawbacks of each option from an economic, political and legal perspective?
3. In the current constitutional context, how far can we go to ensure consistency in federal, provincial/territorial and supranational regulations given the division of powers, human rights and numerous intergovernmental frameworks and agreements, including the Agreement on Internal Trade? Are the Privacy Commissioner's powers under PIPEDA sufficient to act effectively in these various areas? Should the institution be given additional powers and resources (e.g. by setting up an advisory committee)?

Although several pieces of the puzzle are missing to form a better picture of the actual environment in which PIPEDA will have to operate, our research has led us to believe that there is a shift toward ensuring greater consumer protection, especially with respect to new technologies. If this view is correct, a number

of questions will need to be addressed, such as: What will be the adequate level of protection to offer to consumers? If a significant increase in the level of protection is needed, what would be its impact on the competitive capacity of industries operating on national and transnational levels? How should this greater level of protection be implemented in PIPEDA? Should the OPC be given more powers to fulfill greater responsibilities to protect consumers?

If the answer to the last question, in particular, is positive, the OPC will need additional financial and human resources to be able to deliver on its evolving mandate. To this end, a meaningful cost-benefit analysis will need to be made: scarce resources must be allocated in such a way as to achieve the most significant results (for example, engaging with the media allows the OPC to raise its profile with respect to PIPEDA without the expense of attempting to communicate directly with all those affected by the legislation). The OPC presently has a budget of approximately $22 million and a staff of approximately 178 FTEs. Therefore, with too few staff to engage in a vast array of audits or investigations, it is clear that the OPC's capacity to fulfill a mandate to ensure greater protection to consumers will need to be based on strategies that do not rely on significant resources for enforcement.

In addition to capacity and resources, other factors must be taken into consideration while reflecting on future changes, in particular those which have come to shape the OPC's activities under PIPEDA. For example, it might be challenging for an Ombudsman's office to consider a shift in operating model given that staff are trained, and the culture of the office is built around, the Ombuds model. For the OPC, however, which has significant order-making powers to enforce the *Privacy Act* such that its staff and culture already are engaged with these broader methods, not only would this make a shift in operating model more administratively feasible, but such a shift might also address what has been described by some respondents to our interviews as an institutional schism between *The Privacy Act* and PIPEDA compliance activities at the OPC.

Beside these caveats and with this broad perspective in mind, we recommend an examination of the following issues:

- **Recommendation #2: Extending the limits of the Ombuds Model**

The Ombuds model enjoys significant success in larger industries, which are more likely to have well trained privacy professionals, more likely to collaborate with regulators and more likely to be vulnerable to negative publicity. The Ombuds model was particularly well suited to the first phase of regulating industry, where there was considerable concern about the impact of regulation on commercial enterprise. The Ombuds model has succeeded in building trust and credibility, in creating the space for education and outreach opportunities and for developing buy-in of the OPC and its mandate under PIPEDA. However, as our consultations made clear, for many, the current model does

not appear to be as well suited to the small and medium business sector, where compliance rates are lower, and the risk to personal information is greater.[406]

The OPC should continue to use its existing leverage under the Ombuds model to achieve compliance with PIPEDA, especially from large businesses (e.g. banks, insurance, utilities, information technology and media); and in particular to continue to harness media attention and public profile in its efforts to infuse a culture of privacy rights protection in the social media industry. The OPC should target medium and small business sectors for outreach, education and incentives for compliance. It may also be that these two streams of Ombuds activity are mutually reinforcing. As the OPC gains more profile for its efforts to protect privacy in the context of multinational social media companies, it may gain credibility and additional leverage in its efforts to protect personal information in medium and small business contexts.

In this vein, it is worth noting the OPC opened a Toronto office in the summer of 2010, which is led by a former privacy officer for a major Canadian bank, as part of an exchange initiative. This kind of innovative arrangement may also have potential to enhance the OPC's reach in the medium and small business communities.

- **Recommendation #3: Granting limited order-making powers**

Ultimately, notwithstanding the important successes of the OPC, compliance levels with PIPEDA arguably remain too low, and the risk that consumers face with their personal information in the hands of small and medium sized businesses in Canada arguably is too high. While outreach, education and incentives for compliance targeted to small and medium business sectors are important, they may well be insufficient. Looking to the experience of provincial regulators in Canada, as well as to the American and European experience, the ability to levy fines and other order-making capabilities can lead to additional compliance and serve as an important deterrent even if not used often. The benefits to adopting this approach appear tangible while the risks appear less concerning now than in the past. Discussion of the risks, for example, tends to focus on the anticipated negative reaction from businesses, increased adversarial tensions, litigiousness, as well as added cost and complexity both for the OPC and for businesses. The provincial experience with regulators who have order-making powers, however, suggests these risks may be overstated. The treatment of privacy concerns in the media and especially in the context of social media and new technology arguably has created a climate that is more hospitable to regulation, and may also have raised consumer

406 See the distinctions drawn between large, medium and small business in EKOS Research Associates, "Canadian Businesses and Privacy Related Issues" (OPC 2007), section 2 at http://www.priv.gc.ca/information/survey/2007/ekos_2007_01_e.cfm#section2 and again in the follow up survey in 2010 at http://www.priv.gc.ca/information/survey/2010/ekos_2010_01_e.pdf.

expectations that companies will comply with privacy regulations and that regulatory efforts by the OPC will be effective.

While we are certainly not the first to advocate for greater order-making powers[407], we do not believe the OPC at this point needs broad and intrusive powers, such as cessation orders. We believe that enhancing the order-making power of the OPC should be narrowly targeted to the kinds of enforcement activities appropriate to small and medium sized businesses (for example, fines and penalties). It is in these sectors where compliance appears to be the lowest, and where all the available data from provincial enforcement suggests that only the threat of penalties which affect the bottom-line can lead to a change in business behaviour, and ultimately, in business culture. While order-making may not be as necessary in the large business sectors, where the OPC already has made progress in enhancing compliance, it may have salutary effects in this context as well. The order-making power may enhance the significance of privacy policies through these sectors and the profile of compliance officers. Further, given the positive experience with collaboration, consultation and engagement from this sector with the OPC, there is an important foundation of institutional knowledge, trust and credibility on which to build if additional regulatory tools are provided to the OPC.

We also conclude that it does not appear to be the case that enhancing the order making capability of the OPC under PIPEDA would undermine the effectiveness of the OPC's Ombuds model. The relative success of hybrid privacy regulators in B.C., Alberta and elsewhere, in addition to the "cooperative legalism" approach of several European jurisdictions, all suggest that an Ombuds model enhanced with limited order making allows for effective and versatile compliance strategies. Indeed, it may well be that the most effective order-making power in the regulation of privacy context is one that rarely is used.

The additional powers described are likely to lead to the OPC becoming a more efficient and more effective regulator under PIPEDA. Returning to the four criteria set out by Bennett and Raab and discussed in Part 2, these potential enhancements are apparent.

1) **Economy** - (e.g. the cost associated with setting up a regulatory regime). The shift to a hybrid model may well reduce the need for the existing separation of OPC operations into discrete PIPEDA and *Privacy Act* spheres. There may be a range of additional expenses associated with a hybrid model, but as a general approach, there is no clear justification for

407 In particular, CIPPIC has consistently advocated for greater regulatory powers for the OPC. See its submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics http://www.cippic.ca/en/projects-cases/privacy/submissions/CIPPIC_Submission_Nov06wFNs.pdf.

why either the budget or staffing of the OPC would need to change in any significant way if a hybrid model were adopted.

2) **Efficiency** (e.g. the cost of the regime measured against its results). The shift to a hybrid model would likely lead to greater efficiencies, particularly with respect to the small and medium sized business sectors. The combination of greater penetration in these sectors, which typically are more sensitive to financial risk and penalties, and the deterrent effect of avoiding regulatory intervention, is likely to lead to more significant results for the same investment of effort and resources. Further, this model would address the current situation, where litigating a matter in Federal Court represents the only, and unfortunately inefficient, means by which the OPC now may have an order enforced.
3) **Effectiveness** (e.g. the extent to which the practical results of the regime fulfil its ultimate aims) The OPC and CIPPIC studies discussed in Part 2 show that non-compliance remains high. The shift to a hybrid model is likely to increase levels of compliance, particularly in the small and medium sized business sectors (effectiveness is impossible to measure without specific benchmarks and targets).
4) **Equity** (e.g. the extent to which the regime extends protection equitably across social groups). While consumers appear to enjoy greater protection as a result of the OPC's activities if they are customers of banks or insurance companies, social media or mainstream media, there is significantly less protection for consumers of small and medium sized businesses. A shift to a hybrid model would enhance equity and ensure consumer protection was not as dependent on the size and sophistication of the business as is the case now.

For the reasons discussed above, and in light of our analysis in Part 1 and Part 2, we believe there is a compelling case for a limited enhancement to the OPC's regulatory powers, at least to include the power to levy fines for non-compliance.

- **Recommendation #4: Granting explicit guideline-making power**

While the risks of greater order-making powers and the hybrid model suggested above cannot be excluded altogether, they can be mitigated in significant ways, for example, by communicating the policy rationale of the additional powers clearly, issuing guidelines to enhance coherence and predictability in the exercise of the additional powers following a consultative process, and building on the relationships of trust already established through the operation of the Ombuds model. The use of "soft law" by the OPC has provided an important bridge between legislative powers and administrative practices.

Clear guidelines for the use of this order-making power, and safeguards to ensure fairness to those subject to it, will be essential accountability tools, and in our view, ought to accompany the additional regulatory authority. The development of guidelines also provides an opportunity for consultation with stakeholders, a scan of best practices among peer regulators and a context

in which the OPC's values can be communicated clearly to those subject to PIPEDA.

- **Recommendation #5: Exploring other creative regulatory powers**

Our analysis also indicates that there may be additional areas for extending the scope of the Ombuds model. As Commissioner Stoddart has observed, "Increasingly, those responsible for privacy within organizations need to think outside the box."[408]

It is beyond the scope of this analysis to suggest what other regulatory powers might exist within the current context of PIPEDA but which have not yet been utilized by the OPC. Based on our consultations, however, it does appear that there is the potential for additional regulatory initiatives. For example, one of the respondents interviewed suggested the OPC could offer a certification program whereby the imprimatur of the Commission could be given to companies adopting "best practices," much like LEED certification can be earned by buildings with environmental best practices. Such certification or rating systems could then be used by municipal and provincial governments for other regulatory purposes or by companies for commercial benefit (e.g. as part of an advertising strategy). The OPC is not precluded under PIPEDA from developing certification standards and there may be significant upsides to doing so.

Some private initiatives have attempted to develop privacy "seals" such as TRUSTe[409]. These initiatives typically charge businesses for the seal or for the process of obtaining the seals. For this reason, there is a potential conflict between the business interests of the certification provider and the public interest in greater compliance with privacy standards. This conflict does not arise with a public regulator engaging in certification.

Certification or standard setting initiatives rarely are successful on their own. Rather, their success depends on other regulators and industries to create the incentive for businesses to make the additional investment in compliance. For example, if a government, agency or large corporation agreed to limit its procurement to companies with a particular privacy rating, or if particular government permits or grants were tied to a particular privacy rating, this could create effective incentives.

While we are not suggesting the OPC should be certifying, inspecting or imposing labels on the entire private sector, a pilot initiative in a particular industry with low compliance or where vulnerable members of the public are particularly at risk (e.g. youth who share their personal information on-

408 Comments given at the 10th anniversary of the International Association of Privacy Professionals (IAPP) (March 16, 2010) at http://www.priv.gc.ca/media/nr-c/2010/nr-c_100316_e.cfm.

409 See http://www.truste.com/index.html.

line) might well demonstrate whether this regulatory strategy is efficient and effective.

If the Ombuds model is to continue be a successful component of the OPC's regulatory strategy with respect to PIPEDA, the model will need to evolve, adapt and respond in creative ways to challenges of scarce resources and the needs of businesses and the public.

- **Recommendation #6: Improving accountability mechanisms to ensure longer-term strategic planning and meaningful benchmarks**

Whether the Ombuds model, an order-making model or a hybrid model is adopted for the OPC, accountability will remain a key focus. PIPEDA itself contemplates reviews of the legislation and the OPC's activities, and the material arising out of the 2006 Parliamentary review has informed this study. The OPC has commissioned reviews and advocacy groups such as CIPPIC also publish reviews of the legislation and OPC's compliance strategies. The OPC provides detailed Annual Reports to Parliament with respect to its PIPEDA activities.

The Annual Report provides statistics on inquiries, investigations, resolutions of disputes, etc, and also discusses the initiatives and key themes for the past year (for example, in the 2008 Annual Report, the key theme was "Youth Privacy"). Additionally, the OPC publishes an annual Report on Plans and Priorities, which sets out the strategic directions, priorities, and outlines the expected results and spending estimates for the Office of the Privacy Commissioner for the coming fiscal year. The Report is divided into four areas of program activities: (1) compliance activities; (2) research and policy development; (3) outreach activities; and (4) internal services.

This approach to priorities, strategic outcomes and targets is helpful, but too general and "high level" to allow for meaningful performance evaluation. For example, the five corporate priorities for 2009-2010 are as follows:

- Continue to improve service delivery through focus and innovation;
- Provide leadership to advance four priority privacy issues (information technology, national security, identity integrity and protection, genetic information);
- Strategically advance global privacy protection for Canadians;
- Support Canadians, organizations and institutions to make informed privacy decisions; and
- Enhance and sustain the organizational capacity.

The OPC also issues Departmental Performance Reports, which provide an evaluation of the activities of the past year. Goals or targets are set out, activities are summarized, and a conclusion offered as to whether the goals or targets were "met," "mostly met," "partially met," or "not met." For example, for 2009, with respect to compliance goals, the OPC indicated that the Commissioner's investigation recommendations were accepted in 13 of the 17 (76 percent) PIPEDA-related investigations where specific recommendations were made.

Of the four remaining cases, two cases were settled by the parties prior to being heard by the Federal Court, one case was being litigated and, in the fourth, the OPC decided against proceeding with litigation. Consequently, the OPC concluded that its goals were "partially met." These reporting instruments are complemented by statements and speeches by the Commissioner, which add texture and context to the OPC's accountability. For example, the Commissioner's statements with respect to the scope of PIPEDA show an evolution from when the OPC was created.

Again, while such performance assessments are helpful, their impact is limited. What is lacking in the current accountability structure is a sense of longer-term strategic planning and meaningful benchmarks. While the OPC is hardly under-scrutinized, it is often difficult to discern the criteria by which the various reviews assess the OPC. More troubling, it is not clear by what standards the OPC evaluates its own performance. While the OPC collects data and notes trends in its activities, or the level of complaints or resolutions, the OPC has not identified benchmarks or targets by which its activities might be assessed. The FTC provides a helpful model in this regard. As we discuss in Part 2, the FTC publishes a five year strategic plan which highlights a number of overall goals (e.g. protect consumers), with each goal then including a set of objectives tied to performance measures, strategies to achieve the goal and method of evaluation.

Our final recommendation is that the OPC adopt a clearer strategic planning approach in relation to its activities under PIPEDA, involving:

- The establishment of benchmarks for compliance with PIPEDA;
- Monitoring and tracking compliance on an ongoing basis, at least in target or priority sectors such as small and medium sized businesses;
- Performance evaluation measures for OPC activities in this regard; and
- Short, medium and long-term strategic planning with established targets with specific timelines.

BIBLIOGRAPHY

Statutes

Access to Information Act, R.S.C. 1985, c. A-1

An Act Respecting Assisted Human Reproduction and Related Research, S.C. 2004, c. 2

An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., c. P-39.1

An Act to Amend the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information and Other Legislative Provisions, S.Q. 2006, c. 22

Auditor General Act, R.S.C. 1985, c. A-17

Canada Election Act, S.C. 2000, c. 9

Canada Grain Act, R.S.C. 1985, c. G-10

Canada Labour Code, R.S.C. 1985, c. L-2

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act*, [Schedule B of the *Canada Act 1982* (U.K.), 1982, c. 11

Canadian Human Rights Act, S.C. 1976-77, c. 33

Canadian Human Rights Act, R.S.C. 1985, c. H-6

Canadian Radio-television and Telecommunications Commission Act, R.S.C. 1985, c. C-22

Charter of Human Rights and Freedoms, R.S.Q., c. C-12

Civil Code of Québec, S.Q. 1991, c. 64

C*onstitution Act, 1867*, 30 & 31 Vict., c. 3 (U.K.)

Criminal Justice and Immigration Act 2008, c. 4 (U.K.), http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_1

Data Protection Act 1998, c. 29 (U.K.), http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&activeTextDocId=3190610

Employment Equity Act, S.C. 1995, c. 44

Federal Accountability Act, S.C. 2006, c. 9

Lobbying Act, R.S.C. 1985, c. 44 (4th Supp.)

National Energy Board Act, R.S.C. 1985, c. N-7

Official Languages Act, R.S.C. 1985, c. 31 (4th Supp.)

Parliament of Canada Act, R.S.C. 1985, c. P-1

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5

Privacy Act, R.S.C. 1985, c. P-21

Public Service Employment Act, S.C. 2003, c. 22

Salaries Act, R.S.C. 1985, c. S-3

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (*USA PATRIO ACT)* Act of 2001, Pub. L. No. 107-56, 272, Stat. 218, online: http://www.govtrack.us/congress/billtext.xpd?bill=h107-3162&version=enr

Cases

Attorney General (Que.) v. *Kellogg's Co. of Canada et al.*, [1978] 2 S.C.R. 211

Aubry v. *Éditions Vice-Versa inc.*, [1998] 1 S.C.R. 591

B.C. Development Corp. v. *Friedmann*, [1985] 2 S.C.R. 447

BC Govt Serv. Empl. Union v. British Columbia (Minister of Health Services), (2005) BCSC 446, online: http://www.canlii.org/en.bc/bcsc/doc/2005/2005bcsc446/2005bcsc446.html

Bombardier v. *Bouchard*, 1996 CanLII 6356 (QC C.A.)

Campbell v. *MGN Ltd*, Court of Appeal (Civil Division), (2002) EWCA Civ 1373, (2003) QB 633 (U.K.)

Canada (Attorney General) v. *Viola*, [1991] 1 F.C. 373

Canada (Privacy Commissioner) v. *Canada (Labour Relations Board)*, [1996] 3 F.C. 609

Canadian Indemnity Co. et al. v. *Attorney-General of British Columbia*, [1977] 2 S.C.R. 504, 512 and 519

Charkaoui v. *Canada (Citizenship and Immigration)*, [2007] 1 S.C.R. 350

Cheskes v. *Ontario*, 2007 CanLII 38387 (ON S.C.)

Citizens' Insurance Company of Canada v. *Parsons*, (1881) 7 App. Cas. 96

Dagg v. *Canada (Minister of Finances)*, [1997] 2 S.C.R. 403

Eastmond v. *Canadian Pacific Railway and Privacy Commissioner of Canada*, [2004] F.C. 852

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

Hondo v. *UCI, Swiss Olympic and WADA*, TAS, January 10, 2006, online: http://www.wada-ama.org/rtecontent/document/CASELAW_Hondo.pdf

Hunter et al v. *Southam*, [1984] 2 S.C.R. 145

Kirkbi AG v. *Ritvik Holdings Inc.*, [2005] 3 S.C.R. 302

Kitkatla Band v. *British Columbia (Minister of Small Business, Tourism and Culture)*, [2002] 2 S.C.R. 146

Lavigne v. *Canada (Office of the Commissioner of Official Languages*, [2002] 2 S.C.R. 773

Netbored v. *Avery Holdings Inc.*, 2005 FC 1405 (CanLII)

R. v. *Dyment*, [1988] 2 S.C.R. 417

R. v. *Nova Scotia Pharmaceutical Society*, [1992] 2 S.C.R. 606

R. v. *O'Connor*, [1995] 4 S.C.R. 411

R. v. *Turpin*, [1989] 1 S.C.R. 1296

Reference by the Government of Quebec pursuant to the Court of Appeal Reference Act*, R.S.Q., c. R-23, concerning the constitutional validity of sections 8 to 19, 40 to 53, 60, 61 and 68 of the* Assisted Human Reproduction Act*, S.C. 2004, c. 2 (In the matter of a)*, 2008 QCCA 1167 [unofficial English translation]

Reference re Employment Insurance Act *(Can.), art. 22 and 23*, [2005] 2 S.C.R. 669

Reference re Firearms Act *(Can.)*, [2000] 1 S.C.R. 783

Reference re Same-Sex marriage, [2004] 3 S.C.R. 698

Reference re Secession of Quebec, [1998] 2 S.C.R. 217

*Reference re Validity of Section 5(*a*)* Dairy Industry Act, [1949] S.C.R. 1

Rogers v. *Canada (Correctional Service)*, [2001] 2 F.C. 586

Monographs and collective works

BARRIGAR, J. *Consider Consideration and Order-Making*, 2009 (document prepared for the Office of the Privacy Commissioner of Canada).

BENNETT, C. and C. RAAB. *The Governance of Privacy: Policy Instruments in Global Perspective,* Aldershot, Ashgate, 2003.

BENNETT, C. *Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector*, Ottawa, Industry Canada, 1996.

BLACK, H., *11th Annual Meeting on Regulatory Compliance for Financial Institutions*. 2005, online: http://www.priv.gc.ca/speech/2005/sp-d_051118_hb_e.cfm

BUCHANAN, J. M. and G. TULLOCK. *The Calculus of Consent*, Ann Arbor, University of Michigan Press, 1962.

ELIADIS, P. F., M. M. HILL and M. P. HOWLETT. *Designing Government: from Instruments to Governance*, Montreal, McGill-Queen's University Press, 2005.

GAUTRAIS, V. and P. TRUDEL. *Circulation des renseignements personnels et le Web 2.0*, Montréal, Les Éditions Thémis, 2010, p. 231.

GUERRIEN, B. *L'Économie néo-classique*, Paris, La Découverte, 1989.

HAMILTON, J., *30th Anniversary of the OECD Privacy Guidelines, Remarks by Jane Hamilton, Industry Canada*, online: http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html.

HAYEK, F. A. von. *The Road to Serfdom*, London: George Routledge & Sons Ltd., 1944.

HUSTINX, P., *Recent developments in the European Union*, 2010, online: http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html.

JESSUA, C., C. LABROUSSE and D. VITRY (dir.). *Dictionnaire des sciences économiques*, Paris, PUF, 2001, p. 345.

KEY CENTRE FOR ETHICS, LAW, JUSTICE AND GOVERNANCE, GRIFFITH UNIVERSITY and TRANSPARENCY INTERNATIONAL AUSTRALIA, *Chaos or Coherence? Strengths, Opportunities and Challenges for Australia's Integrity Systems: National Integrity Systems Assessment (NISA) Final Report*, Australia, Key Centre for Ethics, Law, Justice and Governance and Transparency International Australia, 2005, http://www.griffith.edu.au/arts-languages-criminology/key-centre-ethics-law-justice-governance/research/integrity-anti-corruption/projects/?a=37155 (consulted January 20, 2010).

KIRBY, *M., The History, Acchievement and Future of the 1980 OECD Guidelines on Privacy*, 2010, online: http://www.oecd.org/findDocument/0,3354, fr_2649_34255_1_119802_1_2_1,00.html.

KRASNOW, E. G., L. D. LONGLEY, and H. A. TERRY. *The Politics of Broadcast Regulation*, 3rd ed., New York, Palgrave, 1982.

LAWSON, I. *Privacy and the Information Highway: Regulatory Options for Canada*, Ottawa: Industry Canada, 1996.

MACKAAY, E. and S. ROUSSEAU. *Analyse économique du droit*, 2nd ed., Montreal, Éditions Thémis, 2008.

MADER, L. *L'évaluation législative. Pour une étude empirique des effets de la législation*, Lausanne, Payot, 1985.

McNAIRN, C. and A. SCOTT. *A guide to the Personal Information Protection and Electronic Documents Act*, Markham, LexisNexis Canada Inc., 2007.

MOCKLE, D. *La gouvernance, l'État et le droit*, Bruxelles, Bruylant, 2007.

MORAND, C.-A. *Le droit néo-moderne des politiques publiques*, Paris, L.G.D.J., 1998.

NISKANEN, W. *Bureaucracy and Representative Government*, Chicago, Aldine Atherton, 1971.

PAPAKONSTANTINOU, V. *Self-Regulation and the Protection of Privacy,* Baden-Baden, Nomos Veralgsgesellschaft, 2001.

RONFELDT, D. F., *Tribes, Institutions, Markets, Networks: A Framework about Societal Evolution*. 1996, Santa Monica, CA: Rand.

ROSANVALLON, P. *Le libéralisme économique : histoire de l'idée de marché*, Paris, Seuil, 1989.

SALAMON, L. M. (ed.). *The Tools of Government: A Guide to the New Governance*, Oxford, Oxford University Press, 2002.

SCHNEIDERMAN, D. *Constitutionalizing Economic Globalization, Investment Rules and Democracy's Promise*, Cambridge, Cambridge University Press, 2008.

SHIELDS, R. *Publicly Available Personal Information and Canada's Personal Information Protection and Electronic Documents Act*, Ottawa, October 12, 2000, McCarthy Tétrault, DMS-Ottawa #5574162/v.2.

SMITH, A. *An Inquiry Into the Nature and Causes of the Wealth of Nations*, London: Charles Knight & Co., 1843.

STEVENSON, H. G. , *30 Years After: The Impact of the OECD Privacy Guidelines, Remarks of Hugh G. Stevenson*, 2010, online: http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html.

ZARKIN, M. J. *The Federal Communications Commission*, Santa Barbara, Greenwood Publishing Group, 1998.

Journal articles and chapters in collected works

ACKERMAN, B., "The New Separation of Powers", (1999-2000) 113 *Harvard Law Review* 633

AUSTIN L., "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices", (2006) 44 *Canadian Business Law Journal* 21

BECKER, R., "Recent Developments: Transborder Data Flows: Personal Data", (1981) 22 Harv. Int'l. L. J. 241

BENNET, C. and R. M. BAYLEY, "Video Surveillance and Privacy Protection Law in Canada," in Sjaak NOUWT, Berend R. de VRIES and Corien PRINS (eds), The Hague, Asser Press, 2005, p. 65

BERZINS, C., "Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building", (2002) 27 Queen's Law Journal 609

BIGNAMI, F., "Cooperative Legalism", 2009 (on file with the authors)

BOISVERT, A.-M., H. DUMONT and A. STYLIOS, "En marge de l'affaire Norbourg : les enjeux substantifs et punitifs suscités par le double aspect, réglementaire et criminel, de certains comportements frauduleux dans le domaine des valeurs mobilières", 2009, http://hdl.handle.net/1866/2913 (pre-publication)

BOUSTA, R., "The Ombudsman: Proposal for a Definition", (2005) 9 *The International Ombudsman Yearbook* 36

BYGRAVE, L. A., "Privacy Protection in a Global Context – A Comparative Overview," (2004) 47 Scandinavian Studies in Law 319

CONNOLLY, C., *Trustmark schemes struggle to protect privacy*, 2008, online: http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.pdf.

COURCHENE, Thomas J., "Global Future for Canada's Global Cities," in *Transitions: Fiscal and Political Federalism in an Era of Change*, Kingston, McGill-Queen's University Press, 2009.

FEINBERG, J., "Autonomy, Sovereignty, and Privacy : Moral Ideals in the Constitution?", (1982) 58 *Notre Dame L. Rev.* 445

FULLER, L. L., "Positivism and Fidelity to Law — A Reply to Professor Hart", (1958) 71:4 *Harvard Law Review* 630

GADLIN, H., "The Ombudsman: What's in a Name?", (2000) 16(1) *Negotiation Journal* 37

GEIST, M., "Privacy Takes Step Towards Global Enforcement," 2010, online: http://www.michaelgeist.ca/content/view/4994/135/ (consulted May 31, 2010).

GELLMAN, R., "TRUSTe fails to justify its role as privacy arbiter," 2000, 25, *Privacy Law and Policy Reporter* (2000), online: http://www.austlii.edu.au/au/journals/PLPR/2000/53.html.

GREENLEAF G., "Five years of the APEC Privacy Framework: Failure or promise?" (2009) 25 *Computer Law & Security Review* 28.

GREGORY, R. and P. GIDDINGS, "The Ombudsman Institution: Growth and Development" in Roy GREGORY and Philip GIDDINGS (eds.), *Righting Wrongs: The Ombudsman in Six Continents*, Washington, IOS Press, 2000, p. 1

GUNASEKARA, G., "The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows" (2007) 17, *International Journal of Law and Information Technology* 147.

HÉNIN, P.-Y. and P. RALLE, "Les nouvelles théories de la croissance. Quelques apports pour la politique économique", *Revue économique – Hors série* 82

HOWES, E., "No guarantee of privacy," 2002, online: http://spywarewarrior.com/uiuc/privpol.htm#no-guarantee.

HUNTON & WILLIAMS LAW FIRM, *Background paper on APEC Privacy Framework Pathfinder Projects*, 2008, p. 3, online: http://www.hunton.com/files/tbl_s47Details/FileUpload265/2302/.

KERR, I, J. BARRIGAR, J. BURKELL, and K. BLACK, "Soft Surveillance, Hard Consent", (2006) 6 *Personally Yours* 1

KINGSBURY, B., N. KRISCH and R. B. STEWART, "The Emergence of Global Administrative Law", (2005) 68:15 Law and Contemporary Problems 15

KRISCH, N. and B. KINGSBURY, "Introduction: Global Governance and Global Administrative Law in the International Legal Order", (2006) 17:1 E.J.I.L. 1

LASCOUMES, P. and É. SERVERIN, "Théories et pratiques de l'effectivité du droit", (1986) 2 *Droit et Soc.* 101

MACDONALD, R. A., "La réforme du droit et ses organismes", dans *Actes de la XIVe conférence des juristes de l'État*, Cowansville, Yvon Blais Inc., 2000, p. 377

MAY, R. J., "The FCC's Tumultuous Year 2003: An Essay on an Opportunity for Institutional Agency Reform", (2004) 56 *Administrative Law Review* 1307

McMILLAN, J., "The Ombudsman and the Rule of Law" (2005) 44 *Australian Institute of Administrative Law Forum* 1

NIGGLI, O. and Julien Sieveking, "Éléments choisis de jurisprudence en application du code mondial antidopage," (2006) 20 *Jusletter* 2.

NISKER, J., "PIPEDA: A Constitutional Analysis", 85 *Canadian Bar Review* 317

OWEN, S., "The Ombudsman: Essential Elements and Common Challenges", in Linda C. REIF (ed.), *The International Ombudsman Anthology*, The Hague, Kluwer Law International, 1999, p. 51

RAAB, C. and C. BENNETT, "Taking the measure of privacy: can data protection be evaluated?", (1996) 62 *International Review of Administrative Sciences* 535

RAAB, C. and C. BENNETT, "The Governance of Global Issues: Protecting Privacy in Personal Information", *European Consortium for Political Research,* 2003, p.6, also in M. Koenig-Archibugi and M. Zürn (eds), *New Modes of Governance in the Global System: Exploring Publicness, Delegation and Inclusiveness*, London, Palgrave Macmillan, 2006, p. 125

RAAB, C., "Beyond Activism: Research Perspectives on Privacy," *TILT Law & Technology Working Paper Series* (22 February 2008), no. 007/2008

REIF, L. C., "Building Democratic Institutions: The Role of National Human Rights Institutions in Good Governance and Human Rights Protection", (2000) 13 *Harvard Human Rights Journal* 1

ROCHER, G., «L'effectivité du droit», in Andrée LAJOIE, Roderick A. MACDONALD, Richard JANDA and Guy ROCHER (eds.), *Théories et émergence du droit : pluralisme, surdétermination et effectivité*, Montréal, Thémis, 1998, p. 133

ROUILLER, C., *Avis de droit sur la compatibilité de l'article 10.2 du Code mondial antidopage avec les principes fondamentaux du droit national suisse,* 2005, online: http://www.wada-ama.org/Documents/World_Anti-Doping_Program/WADP-Legal_Library/Advisory_and_Legal_Opinions/Compatibilit%C3%A9_droit_suisse_Document_entier.pdf.

SCHWARTZ, P. M., "Privacy and Preemption", (2009) 118 Yale L. J. 902

SPIGELMAN, J., "The Integrity Branch of Government", *Quadrant,* vol. XLVIII, nº 7, July-August 2004, p. 51

STEIN J. G., "Networked Federalism", in *Transitions: Fiscal and Political Federalism in an Era of Change*, Kingston, McGill-Queen's University Press, 2009, p. 347.

STEWART, B., *A suggested scheme to certify substantial observance of APEC Guidelines on data privacy*, APEC E-commerce Steering Group Meeting, 2003, online: http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2003.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2003/pdf.Par.0009.File.v1.1.

STUMCKE, A. and A. TRAN, "The Commonwealth Ombudsman: an Integrity Branch of Government?", (2007) 32 :4 *Alternative Law Journal* 233

TOPPERWIEN, B., "Separation of Powers and the Status of Administrative Review", (1999) 20 *Australian Institute of Administrative Law Forum* 32

URIO, P., "La gestion publique au service du marché", in Marc HUFTY (ed.), *La pensée comptable : État, néolibéralisme, nouvelle gestion publique*, Paris and Geneva, PUF and Les nouveaux Cahiers de l'IUED, 1998, p. 91

WATERS, N., "The APEC Asia-Pacific Privacy Initiative – A new route to effective data protection or a Trojan horse for self-regulation?", 2008, *University of New South Wales Faculty of Law Research Series 2008 Working Paper 59*.

WEISER, P. J., "FCC Reform and the Future of Telecommunications Policy," 2009, http://fcc-reform.org/paper/fcc-reform-and-future-telecommunications-policy

Treaties

Agreement Between the European Community and the Government of Canada on the Processing of Advance Passenger Information and Passenger Name Record Data, 3 October 2005, *Official Journal of the European Union* L 82/15 21.3.2006, Entry into force 22 March 2006, http://www.canadainternational.gc.ca/eu-ue/assets/pdfs/031005PNR_eng.pdf

Free Trade Agreement Between Canada and the Hashemite Kingdom of Jordan, 28 June 2009, http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/jordan-jordanie/agreement-toc-tdm-accord.aspx?lang=eng

Free Trade Agreement Between Canada and the Republic of Peru, 29 May 2008, Entry into force 1 August 2009, http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/peru-perou/peru-toc-perou-tdm.aspx?lang=eng

Lausanne Declaration on Doping in Sport,1999, http://www.sportunterricht.de/lksport/Declaration_e.html

North American Free Trade Agreement Between the Government of Canada, the Government of the United Mexican States and the Government of the United States of America, 17 December 1992, [1994] Can. T.S. No. 2, Entry into force 1 January 1994, http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/nafta-alena/texte/index.aspx?lang=eng

UNESCO, *International Convention Against Doping in Sport,* 2005, online: http://www.unesco.org/new/en/social-and-human-sciences/themes/sport/anti-doping/international-convention-against-doping-in-sport/.

Public agency documents and reports
Canada

ALBERTA, ACCESS AND PRIVACY SERVICE ALBERTA, *PIPA Compared,* Edmonton, Access and Privacy Service Alberta, 2008, http://pipa.alberta.ca/legislation/pdf/PIPAcompared.pdf

ALBERTA, SELECT SPECIAL PERSONAL INFORMATION PROTECTION ACT REVIEW COMMITTEE, *Review of the Personal Information Protection Act*, Edmonton, Legislative Assembly of Alberta, 2007, www.assembly.ab.ca/committees/reports/PIPA/finalpipawReport111407.pdf

BRITISH COLUMBIA, OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA, *The OIPC's Role and Mandate*, www.oipc.bc.ca/pdfs/public/OIPC-Role-and-Mandate.pdf

BRITISH COLUMBIA, SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT, *Streamlining British Columbia's Private Sector Privacy Law*, Victoria, Legislative Assembly of British Columbia, 2008, http://www.leg.bc.ca/cmt/38thparl/session-4/pipa/

CANADA, ACCESS TO INFORMATION REVIEW TASK FORCE, *Access to Information: Making it Work for Canadians*, Ottawa, Public Works and Government Services, 2002

CANADA, *Canadian Policy Against Doping in Sport,* http://www.pch.gc.ca/pgm/sc/pol/dop/index-eng.cfm.

CANADA, COMPETITION BUREAU, *Frequently Asked Questions About the Amendment of the Competition Act*, http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03046.html

CANADA, COMPETITION POLICY REVIEW PANEL, *Compete to Win : Final Report June 2008*, http://www.ic.gc.ca/eic/site/cprp-gepmc.nsf/eng/h_00040.html

CANADA, COMPETITION POLICY REVIEW PANEL, *Competition Policy Review Panel Releases Report*, 26 June 2008

CANADA, CRIMINAL INTELLIGENCE SERVICE CANADA, *Feature Focus: Identity Theft and Identity Fraud in Canada,* 2008, http://www.cisc.gc.ca/annual_reports/annual_report_2008/feature_focus_2008_e.html

CANADA, DEPARTMENTS OF INDUSTRY AND JUSTICE, TASK FORCE ON ELECTRONIC COMMERCE, *The Protection of Personal Information: Building Canada's Information Economy and Society*, Ottawa: Distribution Services, Communications Branch, 1998

CANADA, DEPARTMENTS OF INDUSTRY AND JUSTICE, *The Protection of Personal Information: Building Canada's Information Economy and Society* – Notice No. IPPB-002-98 — Release of Public Discussion Paper on the Protection of Personal Information in the Marketplace, January 24, 1998, *Canada Gazette*, Part I, Vol. 132, No. 4

CANADA, GOVERNMENT OF CANADA, *Cabinet Directive on Streamlining Regulation*, Ottawa: Her Majesty the Queen in Right of Canada, 2007, http://www.tbs-sct.gc.ca/ri-qr/directive/directive00-eng.asp (accessed on May 11, 2010)

CANADA, GOVERNMENT OF CANADA, "Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, http://www2.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&Parl=39&Ses=1&DocId=3077726&File=0

CANADA, MINISTRY OF INDUSTRY, *Bill C-19*, November 2nd, 2004, http://www2.parl.gc.ca/HousePublications/Publication.aspx?pub=bill&doc=C-19&parl=38&ses=1&language=E

CANADA, MINISTER OF INDUSTRY, «Speaking Notes for the Honourable John Manley, Minister of Industry, Presentation to the Senate Committee Studying Bill C-6», December 2, 1999, http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00217.html (accessed on May 11, 2010)

CANADA, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. *Annual Report to Parliament 2003-2004*, 2004, online: http://www.priv.gc.ca/information/ar/200304/200304_e.pdf.

CANADA, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *2008 Annual Report to the Parliament, Report on the Personal Information and Electronic Documents Act*, 2009, http://www.priv.gc.ca/information/ar/200809/2008_pipeda_e.pdf

CANADA, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Cherry Picking Among Apples and Oranges : Refocusing Current Debate About the Merits of the Ombuds-Model Under PIPEDA*, Toronto, Office of

the Privacy Commissioner of Canada, 2005, http://www.priv.gc.ca/information/pub/omb_051021_e.cfm

CANADA, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA)*, http://www.priv.gc.ca/information/pub/lbe_080523_e.pdf

CANADA, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Report to Parliament Concerning Substantially Similar Provincial Legislation*, Ottawa: Department of Public Works and Government Services, 2002, publication available at the Commissioner's website: www.priv.gc.ca (accessed on May 11, 2010)

CANADA, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Social Network Site Privacy: A Comparative Analysis of Six Sites*, Ottawa: Office of the Privacy Commissioner of Canada, 2009

CANADA, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Surveillance, Search or Seizure Powers Extended by Recent Legislation in Canada, Britain, France and the United States*, 2009, online: http://www.priv.gc.ca/parl/2009/parl_bg_090507_e.pdf.

CANADA, PARLIAMENT, HOUSE OF COMMONS, STANDING COMMITTEE ON JUSTICE AND SOLICITOR GENERAL, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, *Access and Privacy: The Steps Ahead*, Ottawa: Her Majesty the Queen in Right of Canada, 1987

CANADA, PARLIAMENT, *Officers and Officials of Parliament*, http://www2.parl.gc.ca/Parlinfo/compilations/OfficersAndOfficials/OfficersOfParliament.aspx?Language=E

CANADA, PARLIAMENT, STANDING COMMITTEE ON HUMAN RIGHTS AND THE STATUS OF DISABLED PERSONS, *Privacy, Where Do We Draw the Line?* Ottawa: Supply and Services Canada, 1997

CANADA, STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS, *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA): Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, 2007

CANADA, STANDING COMMITTEE ON INDUSTRY, Submission to the House of Commons Standing Committee on Industry, December 2nd, 1998, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1039144&Language=E#T1532

CANADA, TELECOMMUNICATIONS POLICY REVIEW PANEL, *Final Report 2006,* Ottawa, Public Works and Government Services Canada, http://www.telecomreview.ca/eic/site/tprp-gecrt.nsf/eng/rx00101.html

CANADA, TREASURY BOARD OF CANADA SECRETARIAT, *Regulatory Policy*, Ottawa: Treasury Board of Canada, 1992

CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC, *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?,* 2006, Ottawa, Canadian Internet Policy and Public Interest Clinic, http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf

CANADIAN STANDARDS ASSOCIATION (CSA), *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, Rexdale, CSA, 1996

DENHAM, E., Assistant Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook inc. under the Personal Information Protection and Electronic Documents Act*, July 16th, 2009, http://priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf

HOLMES, N. *Canada's Federal Privacy Laws*, Ottawa: Library of Parliament, Parliamentary Information and Research Service, 2008

LA FOREST, G. V., Special Advisor to the Minister of Justice, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues*, Ottawa, Department of Justice Canada, 2005, http://www.justice.gc.ca/eng/ip/index.html

PHILLIPS, B., Privacy Commissioner of Canada, *Response to the Government of Canada, Discussion Paper: "The Protection of Personal Information: Building Canada's Information Economy Society"*, Ottawa: Office of the Privacy Commissioner of Canada, 1998

QUÉBEC, ASSEMBLÉE NATIONALE, COMMISSION DE LA CULTURE, *Observations, conclusions et recommandations à la suite de la consultation générale et des auditions publiques à l'égard du document intitulé : Une réforme de l'accès à l'information: le choix de la transparence*, 2004

QUÉBEC, COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Une réforme de l'accès à l'information : le choix de la transparence*, 2002

QUÉBEC, MINISTÈRE DU CONSEIL EXÉCUTIF, *La Réglementation par objectifs, Propositions du Groupe de travail Justice – Secrétariat à l'allégement réglementaire*, Québec, Ministère du Conseil exécutif, 2001, http://www.mce.gouv.qc.ca/allegement/documents/reglementation_objectifs.pdf (accessed on July 14, 2009).

UNIFORM LAW CONFERENCE OF CANADA, 1995 Québec, QC, Annex M: *Personal Information and the Protection of Privacy* http://www.ulcc.ca/en/poam2/index.cfm?sec=1995&sub=1995ac (accessed on May 11, 2010)

UNIFORM LAW CONFERENCE OF CANADA, 1998 Halifax, N.E., Annex A: *Uniform Electronic Commerce Act*, http://www.ulcc.ca/en/poam2/index.cfm?sec=1998&sub=1998ja (accessed on May 11, 2010)

Public agency documents and reports
International

ASIA-PACIFIC ECONOMIC COOPERATION, *APEC Data Privacy Pathfinder Projects Implementation Work Plan -Revised*, Doc. off. 2009/SOM1/ECSG/SEM/027 (23 February 2009), online: http://aimp.apec.org/Documents/2009/.../09_ecsg_sem1_027.doc

ASIA-PACIFIC ECONOMIC COOPERATION, APEC Privacy Framework, (2005) APEC#205-SO-01.2.

CENTRE FOR INFORMATION POLICY LEADERSHIP and OFFICE OF THE DATA PROTECTION COMMISSIONER, «Global Discussion on the Commonly-accepted Elements of Privacy Accountability» Galway, Ireland, 2009

COMMISSION OF THE EUROPEAN COMMUNITIES, *The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act*, November 2006

COURT OF ARBITRATION FOR SPORT, *History of the CAS*, 2010, online: http://www.tas-cas.org/history.

CROMPTON, M. "'Light Touch' or 'Soft Touch' – Reflections of a Regulator Implementing a New Privacy Regime", Australia, The Office of the Privacy Commissioner, 2004, http://www.privacy.gov.au/news/speeches/sp2_04p.html#link04

EUROPEAN COMMISSION, INTERNAL MARKET AND FINANCIAL SERVICES, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data: annex to the annual report 1998 (XV D/5047/98) of the working party established by article 29 of directive 95/46/EC,* Luxembourg: Office for Official Publications of the European Communities, 1998

EUROPEAN COMMISSION, WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, *Transfer of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, European Commission Internal Market and Financial Services, July 24, 1998, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf

EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION, *Directive 95/46/EC of European Parliament and of the Council of*

24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23 November 1995, p. 31, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&type_doc=Directive&an_doc=1995&nu_doc=46&lg=en (accessed on May 11, 2010)

FRANCE, SENATE, *Proposition de loi visant à mieux garantir le droit à al vie privée à l'heure du numérique*, 2009, http://www.senat.fr/leg/ppl09-093.html.

HUSTINX, P. J., "Adequate Protection – Opinion 6/99 of the Article 29 Working Party revisited," *Ten Years of DP & FOI Commissioner's Office, 2006*, p. 251, http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/231

INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, Madrid, 5 November, 2009, see http://www.edri.org/edri-gram/number7.2/international-standards-data-protection (accessed on January 20, 2010)

INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, *Resolution on the Urgent Need for Protecting Privacy in a Borderless World, and for Reaching a Joint Proposal for Setting International Standards on Privacy and Personal Data Protection*, document adopted in Strasbourg, October 17, 2008, http://www.edps.europa.eu/EDPSWEB/edps/lang/en/Cooperation/Intconference (accessed on January 20, 2010)

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Action Plan for the Global Privacy Enforcement Network (GPEN)*, 2010.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Canada: maintaining leadership through innovation*, OECD Publishing, 2002

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Canada – The Role of Competition Policy in Regulatory Reform*, 2002, www.oecd.org/dataoecd/47/48/1960522.pdf

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Declaration on the Protection of Privacy on Global Networks*, October 19, 1998, http://www.oecd.org/dataoecd/39/13/1840065.pdf (accessed on July 23, 2009)

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Declaration on Transborder Data Flows*, April 11, 1985, http://www.oecd.org/document/32/0,3343,en_2649_34255_1888153_1_1_1_1,00.html (accessed on May 11, 2010)

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *OECD Guidelines on the Protection of Privacy*

and Transborder Flows of Personal Data, September 23, 1980, http://www.oecd.org/document/57/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (accessed on May 11, 2010).

SPAIN, SPANISH DATA PROTECTION AGENCY (AEPD), information brochure, https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/AEPD_en.pdf

THOMAS, R. and M. WALPORT, *Data Sharing Review*, *Ministry of Justice*, report presented to the Prime Minister and Secretary of State for Justice of United Kingdom, 2008, http://www.justice.gov.uk/reviews/datasharing-intro.htm

THOMAS, R., *Evidence to the Justice Select Committee – January 2009*, United Kingdom, Information Commissioner's Office, 2009, http://www.ico.gov.uk/about_us/news_and_views/current_topics/ic_evidence_to_js_committee.aspx

UNITED KINGDOM, DEPARTMENT FOR CONSTITUTIONAL AFFAIRS, *Increasing penalties for deliberate and wilful misuse of personal data*, 2006, www.dca.gov.uk/consult/misuse_data/cp0906.htm

UNITED KINGDOM, HOUSE OF LORDS, *Surveillance: Citizens and the State*, February 6th, 2009, http://www.parliament.uk/hlconstitution/

UNITED KINGDOM, INFORMATION COMMISIONER'S OFFICE, *Coroners and Justice Bill, Part 8 – Data Protection*, Commentary from the Information Commissioner's Office, 2009, www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cj_bill_lords_2nd_reading_v2%200.pdf

UNITED KINGDOM, INFORMATION COMMISSIONER'S OFFICE, *Data breaches reported to the ICO*, February 9th, 2009, www.ico.gov.uk/upload/documents/pressreleases/2009/data_breaches_ico_statement20090209.pdf

UNITED KINGDOM, INFORMATION COMMISSIONER'S OFFICE, "Information Commissioner calls for prison sentences for illegal buying and selling of personal information," May 12, 2006, http://www.ico.gov.uk/global/search.aspx?collection=ico&keywords=prison

UNITED KINGDOM, INFORMATION COMMISSIONER'S OFFICE, *Minutes – Management board,* January 26, 2009, www.ico.gov.uk/upload/documents/library/corporate/notices/minutes_3_march_2008v1.8.pdf

UNITED KINGDOM, MINISTRY OF JUSTICE, *Response to the Data Sharing Review Report*, United Kingdom, Ministry of Justice, 2008, http://www.justice.gov.uk/publications/response-data-sharing-review.htm

UNITED KINGDOM, PARLIAMENT, *Coroners and Justice Bill 2008-09 United Kingdom Parliament* , http://services.parliament.uk/bills/2008-09/coronersandjustice.html

UNITED STATES OF AMERICA, COMMITTEE ON ENERGY AND COMMERCE, *Deception and Distrust: The Federal Communications Commission Under Chairman Kevin J. Martin*, 2009, http://energycommerce.house.gov/index.php?option=com_content&task=view&id=1455&Itemid=1

WORLD ANTI-DOPING AGENCY, *About WADA*, 2010, online: http://www.wada-ama.org/en/About-WADA/.

WORLD ANTI-DOPING AGENCY, *International Standard on the Protection of Privacy and Personal Information*, 2009, p. 1, online: http://www.wada-ama.org/Documents/World_Anti-Doping_Program/WADP-IS-PPPI/WADA_IS_PPPI_TC_EN.pdf.

WORLD ANTI-DOPING AGENCY, *FIFA Joins WADA's Say NO! to Doping Campaign During World Cup*, 2010, online: http://www.wada-ama.org/en/News-Center/Articles/FIFA-Joins-WADAs-Say-NO-to-Doping-Campaign-during-World-Cup-1/.

WORLD ANTI-DOPING AGENCY, Q&A on ADAMS, online: http://www.wada-ama.org/en/adams/qa-on-adams-/.

WORLD ANTI-DOPING AGENCY, *UNESCO Convention Reaches 140 Ratification Mark*, 2010, online: http://www.wada-ama.org/en/News-Center/Articles/UNESCO-Convention-Reaches-the-140-Ratification-Mark/.

WORLD ANTI-DOPING AGENCY, *WADA Statement About the Opinion of European Working Party on Data Protection*, 2009, p. 1–2, online: http://www.wada-ama.org/Documents/World_Anti-Doping_Program/WADP-IS-PPPI/WADA_Statement_WP29_EN.pdf

WORLD ANTI-DOPING AGENCY, *World Anti-Doping Code*, 2009, p. 14.

Various

COMSCORE, "June 2009 U.S. Search Engine Rankings", 2009, http://www.comscore.com/Press_Events/Press_Releases/2009/7/comScore_Releases_June_2009_U.S._Search_Engine_Rankings

D'ANGELO, C., "Committee Recommends Amendments to British Columbia's Private Sector Privacy Legislation," *McCarthy Tétrault*, August 8th, 2008, http://www.mccarthytetrault.ca/article_detail.aspx?id=4101

GEIST, M., "Facebook Settles Privacy Commissioner of Canada", 2009, http://www.michaelgeist.ca/content/view/4330/196/

GEIST, M., "Standing on Guard for Privacy – Before Facebook", Toronto, Toronto Star, September 14th, 2009 at http://www.thestar.com/business/article/695147

GOOGLE, "Google does not use the keywords meta tag in web ranking", 2009, http://googlewebmastercentral.blogspot.com/2009/09/google-does-not-use-keywords-meta-tag.html

LE TIGRE, "Marc L***", 2009, http://www.le-tigre.net/Marc-L.html

MOSTROUS, A., "UK citizens' private information being lost at record rate," *London Times*, February 9th, 2009, http://www.timesonline.co.uk/tol/news/politics/article5688347.ece

O'REILLY, T. and J. BATTELLE, "Web Squared: Web 2.0 Five Years On", 2009, http://www.web2summit.com/web2009/public/schedule/detail/10194

O'REILLY, T., "What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software", 2005, http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1, (2007) 65 International Journal of Digital Economics 17. A French version entitled, "Qu'est-ce que le web 2.0 : modèles de conception et d'affaires pour la prochaine génération de logiciels", 2006, is available at the following website: http://www.eutech-ssii.com/ressources/1.

SPIGELMAN, J., "Judicial Review and the Integrity Branch of Government", speech delivered at the *World Jurist Association Congress*", Shanghai, September 8, 2005, http://www.lawlink.nsw.gov.au/lawlink/supreme_court/ll_sc.nsf/pages/SCO_spigelman080905 (accessed on December 14, 2009)

SPIGELMAN, J., "The Integrity Branch of Government – The First Lecture in the 2004 National Lecture Series", lecture given as part of the *National Lecture Series of the Australian Institute of Administrative Law* , Sydney, April 29, 2004, http://www.lawlink.nsw.gov.au/lawlink/supreme_court/ll_sc.nsf/pages/SCO_speech_spigelman_290404 (accessed on December 14, 2009)

TURBIDE, Mathieu, "Street View est-il une atteinte à la vie privée?", 2009, http://www.infinit.net/techno/nouvelles/archives/2009/10/20091008-073509.html

WORLD PRIVACY FORUM, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, 2009, http://www.worldprivacyforum.org/cloudprivacy.html

Internet Sites

Canadian Radio-television and Telecommunications Commission, http://www.crtc.gc.ca/

Commission d'accès à l'information du Québec, http://www.cai.gouv.qc.ca/index-en.html

Competition Policy Review Panel, www.competitionreview.ca

European Data Protection Supervisor, http://www.edps.europa.eu

Facebook, http://www.facebook.com

Flickr, http://www.flickr.com/

Google, http://www.google.ca and http://www.google.fr

Google images, http://images.google.ca/

Google maps, http://maps.google.ca/

Grand Dictionnaire, www.granddictionnaire.com

Legislative Assembly of British Columbia, http://www.leg.bc.ca/

Myspace, www.myspace.com

New York University School of Law, Institute for International Law and Justice, Global Administrative Law Project, http://www.iilj.org/global_adlaw

Office of the Information & Privacy Commissioner for British Columbia, http://www.oipc.bc.ca/

Office of the Information And Privacy Commissioner of Alberta, http://www.oipc.ab.ca/pages/About/Commissioner.aspx

Office of the Privacy Commissioner of Canada, http://www.priv.gc.ca/

Reforming the FCC, http://fcc-reform.org/

Wikipedia, www.wikipedia.org

Yahoo maps, http://ca.maps.yahoo.com/

YouTube, www.youtube.com

APPENDIX A

Employment Equity Act*, S.C. 1995, c. 44, Part III (Assessment of Monetary Penalties), ss. 35 *et seq.

PART III – ASSESSMENT OF MONETARY PENALTIES

Violations

Violation

35. (1) Every private sector employer commits a violation of this Act who

(*a*) without reasonable excuse, fails to file an employment equity report as required by section 18;
(*b*) without reasonable excuse, fails to include in the employment equity report any information that is required, by section 18 and the regulations, to be included; or
(*c*) provides any information in the employment equity report that the employer knows to be false or misleading.

Continuing violations

(2) A violation that is committed or continued on more than one day constitutes a separate violation for each day on which it is committed or continued.

Violations not offences

(3) A violation is not an offence and accordingly the Criminal Code does not apply in respect of a violation.

Assessment of monetary penalty

36. (1) The Minister may, within two years after the day on which the Minister becomes aware of a violation, issue a notice of assessment of a monetary penalty in respect of the violation and send it by registered mail to the private sector employer.

Limit

(2) The amount of a monetary penalty shall not exceed
(*a*) $10,000 for a single violation; and
(*b*) $50,000 for repeated or continued violations.

Factors to be considered

(3) In assessing the amount of a monetary penalty, the Minister shall take into account
(*a*) the nature, circumstances, extent and gravity of the violation; and
(*b*) the wilfulness or intent of the private sector employer and the employer's history of prior violations.

Notice of assessment of monetary penalty

37. A notice of the assessment of a monetary penalty shall
(*a*) identify the alleged violation;
(*b*) specify the amount of the monetary penalty; and
(*c*) specify the place where the employer may pay the monetary penalty.

Options

Employer's options

38. (1) An employer may, no later than thirty days after receiving a notice of assessment of a monetary penalty,
(*a*) comply with the notice; or
(*b*) contest the assessment of the monetary penalty by making a written application to the Minister for a review, by a Tribunal, of that assessment.

Copy of application

(2) If the Minister receives a written application, the Minister shall send a copy of it to the Chairperson.

Copy of notice of assessment

(3) If an employer who is issued a notice of assessment of a monetary penalty fails to exercise one of the options set out in subsection (1) within the period referred to in that subsection, the Minister shall send a copy of the notice to the Chairperson.

1995, c. 44, s. 38; 1998, c. 9, s. 40.

Assignation

39. (1) On receipt of a copy of a written application or a copy of a notice of assessment, the Chairperson shall establish a Tribunal consisting of one member selected from the Canadian Human Rights Tribunal to review the assessment and shall
(*a*) send, by registered mail, a request that the employer appear before the Tribunal at the time and place set out in the request to hear the allegations against the employer in respect of the alleged violation; and
(*b*) in writing, advise the Minister who issued the notice of assessment of the time and place set out in the request.

Failure to appear before the tribunal

(2) Where an employer to whom a request is sent fails to appear before a Tribunal at the time and place set out in the request, the Tribunal shall consider all the information that is presented to it by the Minister in relation to the alleged violation.

Opportunity to make representations

(3) In conducting its review, a Tribunal shall provide the Minister and the employer with a full opportunity consistent with procedural fairness and natural justice to present evidence and make representations to it with respect to the alleged violation.

Determination of Tribunal

(4) Where at the conclusion of its proceedings a Tribunal determines that the employer
(*a*) has not committed the alleged violation, the Tribunal shall immediately inform the employer and the Minister of its determination and no further proceedings shall be taken against the employer in respect of the alleged violation; or
(*b*) has committed the alleged violation, the Tribunal shall immediately
(i) issue to the Minister a certificate, in the prescribed form, of its determination that sets out an amount, not exceeding the applicable amount set out in subsection 36(2), determined by the Tribunal to be payable by the employer in respect of the violation, and
(ii) send a copy of the certificate to the employer by registered mail.

Factors to be considered

(5) In determining an amount under subparagraph (4)(*b*)(i), a Tribunal shall take into account the factors set out in subsection 36(3).

Burden of proof

(6) In proceedings under this section, the Minister has the burden of proving, on a balance of probabilities, that an employer has committed the alleged violation.

Certificate

(7) A certificate that purports to have been issued by a Tribunal under subparagraph (4)(*b*)(i) is evidence of the facts stated in the certificate, without proof of the signature or official character of the person appearing to have signed the certificate.

Determinations are final

(8) A determination of a Tribunal under this section is final and, except for judicial review under the *Federal Courts Act*, is not subject to appeal or review by any court.

1995, c. 44, s. 39; 1998, c. 9, s. 41; 2002, c. 8, s. 182.

Enforcement of monetary penalties

Registration of certificate

40. (1) A certificate issued under subparagraph 39(4)(*b*)(i) may be registered in the Federal Court and when registered has the same force and effect, and all proceedings may be taken on the certificate, as if the certificate were a judgment in that Court obtained by Her Majesty in right of Canada against the employer named in the certificate for a debt in the amount set out in the certificate.

Recovery of costs and charges

(2) All reasonable costs and charges associated with registration of the certificate are recoverable in like manner as if they were part of the amount determined by the Tribunal under subparagraph 39(4)(*b*)(i).

APPENDIX B

Telecommunications Act (1993, c. 38)

Administrative monetary penalties

Violation

72.01 Every contravention of a prohibition or requirement of the Commission under section 41 constitutes a violation and the person who commits the violation is liable
(*a*) in the case of an individual, to an administrative monetary penalty of up to $1,500; or
(*b*) in the case of a corporation, to an administrative monetary penalty of up to $15,000.

2005, c. 50, s. 2.

Vicarious liability — acts of employees, agents and mandataries

72.02 A person is liable for a violation that is committed by an employee, or an agent or mandatary, of the person acting in the course of the employee's employment or the scope of the agent's or mandatary's authority, whether or not the employee, agent or mandatary who actually committed the violation is identified or proceeded against in accordance with this Act.

2005, c. 50, s. 2.

Continuing violation

72.03 A violation that is continued on more than one day constitutes a separate violation in respect of each day during which it is continued.

Power of Commission re notices of violation

72.04 (1) The Commission may
(*a*) designate persons, or classes of persons, who are authorized to issue notices of violation; and
(*b*) establish, in respect of each violation, a short-form description to be used in notices of violation.

Certificate

(2) A person designated under paragraph (1)(a) shall be provided with a certificate of designation, which certificate must be presented at the request of any person appearing to be in charge of any place entered by the designated person.

Information requirement

72.05 A person authorized to issue notices of violation who believes that a person is in possession of information that the authorized person considers necessary for the administration of section 41 may require that person to submit the information to the authorized person in periodic reports or in any other form and manner that the authorized person specifies.

Inspections

72.06 (1) A person authorized to issue notices of violation may
(*a*) subject to subsection (2), enter and inspect, at any reasonable time, any place in which he or she believes on reasonable grounds there is any document, information or thing relevant to the enforcement of section 41, and examine the document, information or thing or remove it for examination or reproduction;
(*b*) make use of or cause to be made use of any data processing system at the place to examine any data contained in or available to the system;
(*c*) reproduce any record or cause it to be reproduced from the data in the form of a print-out or other intelligible output and take the print-out or other output for examination or copying; and
(*d*) make use of any copying equipment or means of communication located at the place.

Warrant required to enter dwelling-place

(2) A person authorized to issue notices of violation may not enter a dwelling-place except with the consent of the occupant or under the authority of a warrant issued under subsection (3).

Authority to issue warrant

(3) On *ex parte* application, a justice, as defined in section 2 of the *Criminal Code*, may issue a warrant authorizing a person authorized to issue notices of violation and who is named in the warrant to enter and inspect a dwelling-

place, subject to any conditions specified in the warrant, if the justice is satisfied by information on oath
(*a*) that the dwelling-place is a place described in paragraph (1)(*a*);
(*b*) that entry to the dwelling-place is necessary for the enforcement of section 41; and
(*c*) that entry has been refused, there are reasonable grounds for believing that entry will be refused, or consent to entry cannot be obtained from the occupant.

Use of force

(4) A person executing a warrant issued under subsection (3) shall not use force unless he or she is accompanied by a peace officer and the use of force has been specifically authorized in the warrant.

Notice of violation

72.07 (1) A person authorized to issue notices of violation who believes on reasonable grounds that a person has committed a violation may issue, and shall cause to be served on that person, a notice of violation.

Contents of notice

(2) The notice of violation must name the person believed to have committed a violation, identify the violation and set out
(*a*) the penalty for the violation as set out in section 72.01;
(*b*) the right of the person, within 30 days after the notice is served, or within any longer period that the Commission specifies, to pay the penalty or to make representations to the Commission with respect to the violation, and the manner for doing so; and
(*c*) the fact that, if the person does not pay the penalty or make representations in accordance with the notice, the person will be deemed to have committed the violation and the Commission may impose the penalty.

Payment

72.08 (1) If the person pays the penalty set out in the notice of violation, the person is deemed to have committed the violation and proceedings in respect of it are ended.

Representations to Commission

(2) If the person makes representations in accordance with the notice, the Commission must decide, on a balance of probabilities, whether the person committed the violation and, if it so decides, it may impose the penalty.

Failure to pay or make representations

(3) A person who neither pays the penalty nor makes representations in accordance with the notice is deemed to have committed the violation and the Commission may impose the penalty.

Copy of the decision and notice of rights

(4) The Commission must cause a copy of any decision made under subsection (2) or (3) to be issued and served on the person together with a notice of the person's right to apply for a review under section 62 and to appeal under section 64.

Debts to her Majesty

72.09 (1) An administrative monetary penalty constitutes a debt due to Her Majesty in right of Canada that may be recovered as such in the Federal Court.

Time limit

(2) No proceedings to recover a debt referred to in subsection (1) may be commenced later than five years after the debt became payable.

Proceeds payable to Receiver General

(3) An administrative monetary penalty paid or recovered in relation to a violation is payable to and shall be remitted to the Receiver General.

Certificate of default

(4) The unpaid amount of any debt referred to in subsection (1) may be certified by the Commission.

Registration in Federal Court

(5) Registration in the Federal Court of a certificate made under subsection (4) has the same effect as a judgment of that Court for a debt of the amount specified in the certificate and all related registration costs.

Defences

72.1 (1) It is a defence for a person in a proceeding in relation to a violation to establish that the person exercised due diligence to prevent the violation.

Common law principles

(2) Every rule and principle of the common law that renders any circumstance a justification or excuse in relation to a charge for an offence in relation to a contravention of a prohibition or requirement of the Commission under section 41 applies in respect of a violation to the extent that the rule or principle is not inconsistent with this Act.

Evidence

72.11 In a proceeding in respect of a violation, a notice purporting to be served under subsection 72.07(1) or a copy of a decision purported to be served under subsection 72.08(4) is admissible in evidence without proof of the signature or official character of the person appearing to have signed it.

Time limit

72.12 (1) No proceedings in respect of a violation may be commenced later than two years after the day on which the subject-matter of the proceedings became known to the Commission.

Certificate of secretary to the Commission

(2) A document appearing to have been issued by the secretary to the Commission, certifying the day on which the subject-matter of any proceedings became known to the Commission, is admissible in evidence without proof of the signature or official character of the person appearing to have signed the document and is, in the absence of evidence to the contrary, proof of the matter asserted in it.

Publication

72.13 The Commission may make public the nature of a violation, the name of the person who committed it, and the amount of the administrative monetary penalty.

How act or omission may be proceeded with

72.14 If a contravention of a prohibition or a requirement of the Commission under section 41 can be proceeded with either as a violation or as an offence, proceeding in one manner precludes proceeding in the other.

Section 12 does not apply

72.15 Section 12 does not apply in respect of any decision of the Commission under subsection 72.08(2) or (3).