Co-operation Among Canadian Data Protection Authorities

by
David Loukidelis
Information and Privacy Commissioner for British Columbia
Victoria
British Columbia
Canada

September 2004

Introduction

This brief paper offers an overview of co-operation initiatives among Canadian data protection authorities, speculates about possible future initiatives and considers whether the Canadian situation speaks to international data protection challenges.[i]

It is first necessary to describe the constitutional and statutory context within which Canadian data protection authorities work, as this context is the source of legal and practical difficulties facing Canadian authorities as they try to co-operate better in enforcing Canada's data protection laws.

Context for Canada's Data Protection Laws

The Canadian constitution[ii] allocates authority to enact laws, and thus to regulate private sector activity, between the federal Parliament and the legislatures of the provinces. Parliament and the provincial legislatures have the authority to pass laws regulating their own privacy practices and subsidiary public bodies that they create or have authority over.

Private sector matters of a local nature and property and civil rights are within the legislative and thus regulatory authority of provincial legislatures. The federal Parliament, however, has the historically limited but perhaps growing power to regulate trade and commerce. It can also regulate inter-provincial and has authority to enter into international treaties.

Public sector data protection laws now exist across Canada. At the federal level, the *Privacy Act*[iii] regulates collection, use and disclosure of personal information by federal government institutions. All provinces and the three territories under federal authority have now passed data protection laws regulating collection, use and disclosure of personal information by their government ministries and other public bodies. These laws are similar in their important features to European laws and have benefited from the years of experience in Europe.[iv]

Although European data protection laws affecting the private sector have been around for over thirty years, such laws have only started to appear in Canada in the last five years.

The federally-enacted *Personal Information Protection and Electronic Documents Act* (PIPEDA), which has come into force in stages since January 1, 2001, regulates the collection, use and disclosure of personal information by the private sector in the course of commercial activities. Quebec, British Columbia and Alberta have all enacted their own laws that apply to the private sector[v] and are substantially similar to PIPEDA.[vi]

PIPEDA now governs private sector activity in the territories and provinces in which no substantially similar private sector law has been passed, including Ontario. This can raise enforcement challenges in at least two ways. First, until the federal Cabinet declares Ontario's recently-passed private sector health privacy law to be substantially similar to PIPEDA, the federal law will apply along with the Ontario law.[vii] This will engage both federal and provincial enforcement responsibility in the interim.

Second, there may be situations in which it is not clear whether the data protection rules under the recent Ontario health privacy law or those under PIPEDA apply.[viii] In such cases, the challenge for federal and provincial data protection authorities will be to identify the appropriate agency to pursue enforcement activity, and to do so expeditiously.

Even in respect of activities having some connection with a province that has enacted a substantially similar private sector data protection law, PIPEDA is likely to have a continued role in regulating trans-border transfers of personal information, especially where a transfer is part of a commercial activity.

Many Canadian organizations carry on business or are otherwise active across the country and internationally and many organizations active in Canada are foreign corporations. In the ordinary course of business, organizations are increasingly likely to transfer personal information across provincial and international borders for a broad range of purposes. These span the spectrum from ordinary-course processing, to emergency backup, to disclosures to third parties for a broad array of uses. Even where an organization operates in a province that has enacted a private sector data protection law, the organization may well transfer data across a border. In light of the federal Parliament's authority to legislate in respect of trans-border matters, transfer of data across a border means both the relevant provincial data protection law and PIPEDA may apply.[ix]

This is not necessarily problematic by any means. The substantial similarity of Canada's private sector data protection laws ensures that an organization's compliance with, for example, PIPEDA almost certainly means the organization will be in compliance with the counterpart provincial data protection law. This is because Canada has, as regards the private sector data protection laws that do exist, achieved an acceptable level of legislative similarity. The possible overlap of federal and provincial data protection jurisdiction in such cases does mean, however, that challenges exist in enforcement actions by Canadian data protection authorities.

A further area of challenge for Canada's data protection authorities arises in cases where the issue of whether an organization is a federal work, undertaking or business, and therefore subject to PIPEDA—which covers such organizations—and not the provincial private sector law, will not necessarily be clear at first sight. As noted earlier, federal and provincial data protection authorities must, where their jurisdiction is not clear on the surface, determine the appropriate enforcement agency quickly and efficiently.

These challenges, which are surmountable, have caused Canadian data protection authorities to move ahead with co-operative enforcement efforts. In forging ahead, data protection authorities will have to bear in mind their slightly different legislative mandates, powers and functions. Early signs are, however, that co-operation offers improvements in service to organizations and consumers alike, while promising to reduce enforcement costs for the participating data protection authorities.

Co-operation Efforts by Canadian Data Protection Authorities

In May of 2003, in advance of the enactment of the Alberta and British Columbia private sector data protection laws, the data protection commissioners of those provinces met with Jennifer Stoddart, at the time president of the Quebec data protection authority, to discuss how the three jurisdictions could co-operate in enforcement of the data protection laws for which they are responsible. Late in 2003, Jennifer Stoddart, by then the newly-appointed Privacy Commissioner of Canada, expressed interest in co-operation with British Columbia and Alberta her new capacity.

Discussions among the three commissioners followed quickly and, in March 2004 a letter from Jennifer Stoddart to the others confirmed their mutual commitment to ongoing co-operation in overseeing implementation of their data protection laws. Since then, the three offices have continued their work on co-operation, yielding both procedural and substantive products. This work has continued to the present and is of course ongoing.

Regarding processes for communication, the three authorities have arranged the following:

- The three commissioners meet at least twice a year, and communicate regularly between personal meetings, to discuss co-operation among their offices and to make decisions and give direction to their offices where appropriate.
- Each commissioner has designated a senior official to serve as the sole point of contact for joint initiatives and staff-level communications.
- The designated senior officials meet by conference call on a regular schedule and in person at least twice a year. These meetings serve several purposes. They ensure timely three-way discussion of information about enforcement experience and emerging issues, with a view to formulating recommendations to the commissioners for joint action where appropriate. These meetings also enable each office to keep current on emerging complaint trends and best practices as they develop in each office. The meetings also reduce the possibility that more than one of the offices is

working on the same matter without the other knowing—the sharing of information reduces the risk that resources will be wasted by re-inventing the wheel.

- Staff in all three offices, along with staff in other Canadian data protection authority offices, participate in a list-serve administered by the Saskatchewan Information and Privacy Commissioner. This list-serve enables real-time sharing by staff of information about practices and experiences, without disclosing case-specific information.

As for substantive matters, the three offices have been working on the following matters among others:

- Tools to permit the three offices to determine case by case, on a co-operative basis, which of them has or should assume jurisdiction to investigate a particular complaint that may fall under the jurisdiction of more than one of them.
- Arrangements to share the contents of complaints files where circumstances warrant and consistent with their legal authorities and obligations.[x]
- Harmonization, or consistency, of approaches to the processing of complaints made to the respective offices. This reflects the fact that all three offices employ mediation where possible to resolve complaints.
- Development of joint position statements, frequently-asked questions publications and jurisdictional tools. An example of this work is the jointly prepared document, "Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's *Personal Information Protection Acts* (PIPAs)", a web-published resource for organizations and consumers who are trying to decide which law applies to their situation.[xi] Other support materials for organizations and consumers can be developed, and can perhaps build on work already done by any one of the three offices.[xii]
- Harmonization of statistical reporting and language for such reporting where possible.

Another way to promote consistency of interpretation and application of the three private sector data protection laws would be to issue joint decisions in significant matters involving systemic issues for all three laws. Specifically, we have discussed whether, in such cases, the commissioner who has jurisdiction over the complaint should delegate authority to one or more of the other commissioners, with the formal hearing and decision being handled by all of them jointly. No decision has been taken on this, but the issuance of a joint decision in such matters could at the very least signal a commitment to consistency of approach by the participating offices.

Moreover, the federal, Alberta and British Columbia commissioners are all committed to, wherever possible, giving respect and weight to each others' formal rulings. They recognize that, while the common law principle of precedent would not be appropriate in the Canadian data protection setting, consistency of interpretation and application of data protection principles is desirable, wherever feasible, given the inter-provincial character of Canadian business activity.

It should be said that the ongoing co-operation of the Alberta, British Columbia and federal data protection authorities respecting their private sector data protection laws occurs against the backdrop of a long history of co-operation between and among Canadian data protection authorities in fulfilling their responsibilities. Canadian data protection authorities have, over the years, often communicated about emerging policy challenges and have taken joint, or at least co-ordinated, public positions on pressing privacy challenges.[xiii] Canadian data protection authorities over the years have also borrowed material from each other, a practice that, as noted earlier, promotes consistency while reducing the demand on public funds.[xiv]

Canadian Experience and International Challenges

The challenge for the three commissioners who are most closely working together is to find ways to co-operate efficiently and effectively without miring their offices in rigid, overly-bureaucratic structures for co-operation. One thing is certain. The challenges to data protection in Canada are multiplying on many fronts and will continue to do so, requiring all of us to adapt and evolve in our work.

Over twenty years after publication of the OECD guidelines, the trans-border character of data flows continues to present challenges to data protection authorities and legislatures in Europe as well as Canada.[xv] Through the forum of the Article 29 Working Party and other means, Europe and its data protection commissioners have shown interest in co-operating. In the Asia Pacific region, work on an APEC privacy framework illustrates the understanding within APEC of the need to harmonize data protection laws, while recognizing the challenges in trans-border enforcement. Whether the modest Canadian experience to date with enforcement of our belated private sector laws can offer anything to our European and other colleagues abroad is for the reader to decide.

---

[i] This text of this paper summarizes my remarks on a panel at the 26th Annual Conference of International Data Protection and Privacy Commissioners, held in Wroclaw, Poland, in September 2004. While I am grateful to my colleagues, Jennifer Stoddart (Privacy Commissioner of Canada), and Frank Work, Q.C., (Information and Privacy Commissioner for Alberta), for their earlier comments on my draft remarks for the panel, any errors in my remarks or this paper are of course my sole responsibility.

[ii] *Constitution Act, 1867*, enacted by *Constitution Act, 1982*, being Schedule B to *Canada Act 1982* (U.K.) 1982, c. 11.

[iii] R.S.C. 1985, c. P-21.

[iv] Canadian data protection laws, both public and private sector, reflect the strong influence of the OECD's Guidelines.

[v] A number of provinces have enacted special-purpose data protection laws applying to health information in both the public and private sectors. The provinces of Alberta, Saskatchewan, Manitoba and, most recently, Ontario, have passed such laws.

[vi] In a development since the author's participation on the above-noted conference panel, the federal Cabinet has, as PIPEDA permits, declared the laws of Alberta and British Columbia to be substantially similar to PIPEDA. A similar declaration had already been made for Quebec's law. This means PIPEDA does not apply to activity covered by one of these provincial laws. The Alberta law is the *Personal Information Protection Act*, S.A. 2003, P-6.5. The British Columbia law is also called the *Personal Information Protection Act*, S.B.C. 2003, c. 63.

[vii] *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, in force November 1, 2004.

[viii] *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31.

[ix] There is no comparable issue, really, as regards the practices of public bodies covered by public sector data protection laws in Canada. For one thing, the federal Parliament has not purported to legislate in relation to the practices of provincial governments and other local public bodies, even assuming Parliament could constitutionally do so.

[x] To facilitate this initiative, amendments to the *Personal Information Protection Act* to facilitate information-sharing among offices were passed this autumn in British Columbia and are expected for Alberta's *Personal Information Protection Act* in the coming months.

[xi] This document was published by the Privacy Commissioner of Canada on November 19, 2004, but was in preparation at the time of my remarks at the September 2004 conference.

[xii] For example, my office has web-published support documents for compliance with British Columbia's *Personal Information Protection Act*, including "What are my organization's responsibilities under PIPA?", "How do I develop a privacy policy?" and "What are the OIPC's policies and procedures?". Alberta's Information and Privacy Commissioner, working with the Alberta government, published a comprehensive guide to that province's *Personal Information Protection Act*. My office used that guide, with permission, to produce a comprehensive guide for our own, very similar, law. This is an example of how co-operation by our offices can promote consistent interpretation of similar laws while reducing the demand on public funds. Another example is the in-progress work my office is doing on support materials for employers and employees on selected common employment privacy issues. This work will be shared with my Alberta and federal colleagues, and other Canadian commissioners who wish it, to support their work in employment privacy matters.

[xiii] As an example of this, in 2002, seven commissioners signed a letter to the federal government expressing opposition to federal *Customs Act* amendments permitting certain collection, use and disclosure of personal information for national security and other purposes.

[xiv] For example, my office's 2001 "Guidelines for Data Services Contracts" benefited from work by the office of the Information and Privacy Commissioner of Ontario, Ann Cavoukian, while her office made use of my office's 2000 "Public Surveillance System Privacy Guidelines" in creating similar materials for Ontario.

[xv] The same challenges are presented to non-governmental organizations in Europe and elsewhere who work in data protection. These organizations doubtless recognize the need to co-operate amongst themselves. There is also, in my view, a clear and pressing need for the international data protection authority community to more extensively and regularly engage non-governmental organizations, whose experts have much to offer commissioners.