FOCUS ON PRIVACY WINTER 2005

JURISDICTIONAL LIMITS ON CANADIAN PRIVACY LAW:

David T.S. Fraser*

Canada's federal privacy law is already hobbled by the country's constitutional division of powers. By relying upon the federal parliament's "general trade and commerce" powers, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") cannot apply to the provincially regulated workplace. Likewise, it cannot apply to the non-commercial operations of charities and the "MUSH" sector, meaning municipalities, universities, schools and hospitals. While there are sectors beyond PIPEDA's reach, the question of whether PIPEDA applies to commercial activities that take place outside Canada's borders remains.

Until recently, the putative position of officials from the Office of the Privacy Commissioner has been that PIPEDA can apply to the collection, use and disclosure of personal information about Canadians by foreign companies. The issue has ceased to be theoretical thanks to an unpublished finding of the Assistant Privacy Commissioner dealing with a complaint brought by the Canadian Internet Policy and Public Interest Clinic ("CIPPIC"), associated with the University of Ottawa Law School. In the Assistant Commissioner's letter to CIPPIC,[1] her office declined to initiate an investigation because the company involved had no presence in Canada. This represents a complete reversal from the previous (unofficial and hypothetical) position of the Office of the Privacy Commissioner.

The letter from the Assistant Commissioner was issued in response to a complaint under PIPEDA launched by CIPPIC against Abika.com, a U.S. company that harvests databases and public sources to produce reports that allegedly include personal information up to and including psychosexual profiles of individuals. This service provides information on Americans and Canadians. CIPPIC filed its complaint in June, claiming that Abika collects, uses, and discloses the personal information of Canadians without consent in violation of Canada's national privacy law.

In its response, the Office of the Privacy Commissioner noted that the company does not have a physical presence in Canada. This led to their conclusion that "while the organization may well be collecting information on Canadians, our legislation does not extend to investigating organizations located only in the United States. We are, therefore, unable to investigate this matter under PIPEDA." This conclusion came as a surprise to many

---

* David T.S. Fraser is the chairman of the Privacy Practice Group at McInnes Cooper, Atlantic Canada's largest single law partnership, principal legal advisor to National Privacy Services Inc. and the author of "PIPEDA and Canadian Privacy Law", a privacy law weblog found at http://pipeda.blogspot.com. The genesis of this article is a presentation given by the author to the Canadian Bar Association Annual Meeting and Conference, August 2004.

[1] Available online at http://www.cippic.ca/en/projects-cases/privacy/opcc_response_30nov04.pdf.

because of the unofficial position taken by the Office of the Privacy Commissioner when the question was merely theoretical.

At the risk of only minimal controversy, the Office of the Privacy Commissioner *could* have asserted jurisdiction to investigate and then dealt with the challenges of enforcement. Modern Canadian principles of conflict of laws, following such seminal cases as *Morguard Investments* v. *De Savoye*[2], *Tolofson* v. *Jensen*,[3] and *Hunt* v. *T & N PLC*[4] provide a strong basis to argue that Canada's privacy laws can reach beyond its borders where there is a clear and substantial connection with Canada. Such a decision would at least have left the complainant with the ability to take the finding to the Federal Court of Canada to explore whether the Court would fashion a remedy and whether the cooperation of U.S. authorities could be obtained. Declining to accept jurisdiction left the complainant with one option: to seek judicial review of this decision, completely separate from the merits of the original complaint.

At least in its origins, PIPEDA was designed to be a piece of an international system to protect the privacy of consumers and citizens. All privacy statutes in Canada trace their roots back to an initiative undertaken by the Organization for Economic Cooperation and Development ("OECD") to establish basic levels for the protection of personal information among member states.[5] The 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* was signed by Canada in 1984 but was never formally adopted into Canadian law, though they eventually found their way into the *Privacy Act*[6] that governs personal information in the custody of the federal government and certain crown agents. According to the former Canadian Privacy Commissioner:

> [a]mong the most influential modern formulations of the desire to protect against excessively curious governments and businesses has been the OECD's 1980 *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data*. In 1984, Canada joined 22 other industrialized nations by adhering to the guidelines. The guidelines were intended to harmonize data protection laws and practices among OECD member countries by establishing minimum standards for handling personal data. The guidelines were not themselves enforceable, but they became the starting point for data protection legislation in countries around the world, including Canada.[7]

The OECD guidelines contain eight fundamental principles of national application dealing with the collection, use, disclosure and retention of personal information.

Following the OECD guidelines, the European community decided to implement and harmonize private sector privacy legislation throughout the continent. The result of this initiative was the European Data Protection Directive[8] which required all member countries of the European Union to implement legislation protecting personal information, hopefully to provide a seamless privacy regime throughout Europe. Most notably, the European Directive included a provision that prevented the transmission of any personal information outside of the European Union unless the recipient country had legislation in place that would offer substantially similar protections. While this provision does not purport to operate extraterritorially, it is

[2] [1990] 3 S.C.R. 1077.
[3] [1994] 3 S.C.R. 1022.
[4] [1993] 4 S.C.R. 289.
[5] Organization for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (adopted 23 September 1980).
[6] *Privacy Act*, R.S.C. 1985, c. P-21.
[7] Speech by Bruce Phillips to the Canadian Bar Association, "The Evolution of Canada's Privacy Laws" (January 28, 2000). Available online http://www.privcom.gc.ca/speech/archive/02_05_a_000128_e.asp.
[8] 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.

demonstrative of an attempt to specifically regulate the cross-border movement of personal information. There is also little doubt that it had an extraterritorial effect.

In the absence of similar and recognized legislation in Canada, the European Data Protection Directive would have prevented the free flow of personal information between Canada and member states of the European Union. The modern economy is predicated on the flow of personal information, either as a good in and of itself or ancillary to other transactions. The prohibitions contained in the European Directive would have amounted to a non-tariff trade barrier between Europe and Canada.

In response to the European Directive and a perceived need to boost electronic commerce, the Canadian government introduced legislation that, it was hoped, would be considered by Europe to be sufficiently similar to the Directive. Both the OECD Guidelines and the European Directive provide the international context in which PIPEDA was born.

In disposing of questions such as the one considered by the Office of the Privacy Commissioner, Canadian courts consider whether there is a "real and substantial" connection between the matter at issue and Canada. If the answer is "yes", the courts may assume jurisdiction. The "real and substantial connection" test has been more recently used by the Supreme Court of Canada in *Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Providers*.[9] In the SOCAN decision, Justice Binnie reviewed the general principles of the extraterritoriality of Canadian laws and concluded that the Canadian *Copyright Act*[10] may apply to cross-border activities where there is a "real and substantial connection" with Canada:

> ¶54 While the Parliament of Canada, unlike the legislatures of the Provinces, has the legislative competence to enact laws having extraterritorial effect, it is presumed not to intend to do so, in the absence of clear words or necessary implication to the contrary. This is because "[i]n our modern world of easy travel and with the emergence of a global economic order, chaotic situations would often result if the principle of territorial jurisdiction were not, at least generally, respected"; see *Tolofson v. Jensen*, [1994] 3 S.C.R. 1022, at p. 1051, per La Forest J.
>
> ¶55 While the notion of comity among independent nation States lacks the constitutional status it enjoys among the provinces of the Canadian federation (*Morguard Investments Ltd. v. De Savoye*, [1990] 3 S.C.R. 1077, at p. 1098), and does not operate as a limitation on Parliament's legislative competence, the courts nevertheless presume, in the absence of clear words to the contrary, that Parliament did not intend its legislation to receive extraterritorial application.
> ¶56 Copyright law respects the territorial principle, reflecting the implementation of a "web of interlinking international treaties" based on the principle of national treatment (see D. Vaver, *Copyright Law* (2000), at p. 14).
>
> ¶57 The applicability of our *Copyright Act* to communications that have international participants will depend on whether there is a sufficient connection between this country and the communication in question for Canada to apply its law consistent with the "principles of order and fairness ... that ensure security of [cross-border] transactions with justice"; see *Morguard Investments Ltd., supra*, at p. 1097; see also *Unifund Assurance Co. v. Insurance Corp. of British Columbia*, [2003] 2 S.C.R. 63, 2003 SCC 40, at para. 56; R. Sullivan, *Sullivan and Driedger on the Construction of Statutes* (4th ed. 2002), at pp. 601-602.
>
> ¶58 Helpful guidance on the jurisdictional point is offered by La Forest J. in *Libman v. The Queen*, [1985] 2 S.C.R. 178. That case involved a fraudulent stock scheme. U.S. purchasers were

[9] 2004 SCC 45 ("SOCAN").
[10] Copyright Act, R.S.C. 1985, c. C-42.

solicited by telephone from Toronto, and their investment monies (which the Toronto accused caused to be routed through Central America) wound up in Canada. The accused contended that the crime, if any, had occurred in the United States, but La Forest J. took the view that "[t]his kind of thinking has, perhaps not altogether fairly, given rise to the reproach that a lawyer is a person who can look at a thing connected with another as not being so connected. For everyone knows that the transaction in the present case is both here and there" (at p. 208 (emphasis added)). Speaking for the Court, he stated the relevant territorial principle as follows (at pp. 212-13):

> I might summarize my approach to the limits of territoriality in this way. As I see it, all that is necessary to make an offence subject to the jurisdiction of our courts is that a significant portion of the activities constituting that offence took place in Canada. As it is put by modern academics, it is sufficient that there be a "real and substantial link" between an offence and this country ... [Emphasis added.]

¶59 So also, in my view, a telecommunication from a foreign state to Canada, or a telecommunication from Canada to a foreign state, "is both here and there". Receipt may be no less "significant" a connecting factor than the point of origin (not to mention the physical location of the host server, which may be in a third country). To the same effect, see *Canada (Human Rights Commission) v. Canadian Liberty Net*, [1998] 1 S.C.R. 626, at para. 52; *Kitakufe v. Oloya*, [1998] O.J. No. 2537 (QL) (Gen. Div.). In the factual situation at issue in *Citron v. Zundel, supra*, for example, the fact that the host server was located in California was scarcely conclusive in a situation where both the content provider (Zundel) and a major part of his target audience were located in Canada. The *Zundel* case was decided on grounds related to the provisions of the *Canadian Human Rights Act*, but for present purposes the object lesson of those facts is nevertheless instructive.

¶60 … From the outset, the real and substantial connection test has been viewed as an appropriate way to "prevent overreaching ... and [to restrict] the exercise of jurisdiction over extraterritorial and transnational transactions" (La Forest J. in *Tolofson, supra*, at p. 1049). The test reflects the underlying reality of "the territorial limits of law under the international legal order" and respect for the legitimate actions of other states inherent in the principle of international comity (*Tolofson*, at p. 1047). A real and substantial connection to Canada is sufficient to support the application of our *Copyright Act* to international Internet transmissions in a way that will accord with international comity and be consistent with the objectives of order and fairness.

…

¶62 Canada clearly has a significant interest in the flow of information in and out of the country. Canada regulates the reception of broadcasting signals in Canada wherever originated; see *Bell ExpressVu Limited Partnership v. Rex*, [2002] 2 S.C.R. 559, 2002 SCC 42. Our courts and tribunals regularly take jurisdiction in matters of civil liability arising out of foreign transmissions which are received and have their impact here; see *WIC Premium Television Ltd. v. General Instrument Corp.* (2000), 8 C.P.R. (4th) 1 (Alta. C.A.); *Re World Stock Exchange* (2000), 9 A.S.C.S. 658.

¶63 Generally speaking, this Court has recognized as a sufficient "connection" for taking jurisdiction, situations where Canada is the country of transmission (*Libman, supra*) *or* the country of reception (*Canada v. Liberty Net, supra*). This jurisdictional posture is consistent with international copyright practice.

…

¶76 Accordingly, the conclusion that Canada *could* exercise copyright jurisdiction in respect both of transmissions originating here and transmissions originating abroad but received here is

not only consistent with our general law (*Libman, supra*, and *Canada (HRC)* v. *Canadian Liberty Net, supra*) but with both national and international copyright practice.

¶77 This conclusion does not, of course, imply imposition of automatic copyright liability on foreign content providers whose music is telecommunicated to a Canadian end user. Whether or not a real and substantial connection exists will turn on the facts of a particular transmission (*Braintech, supra*). It is unnecessary to say more on this point because the Canadian copyright liability of foreign content providers is not an issue that arises for determination in this appeal, although, as stated, the Board itself intimated that where a foreign transmission is aimed at Canada, copyright liability might attach.

PIPEDA is not explicit about whether it is intended to apply extraterritorially, but there is some guidance in Section 4, the basis of the law's application:

Application
4. (1) This Part applies to every organization in respect of personal information that

(a) the organization collects, uses or discloses in the course of commercial activities; or

(b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

The application section is entirely silent with respect to its intended territorial application. The only reference to specific jurisdictions are contained in the transitional provisions and the definition of "federal work, undertaking or business". The transition provisions begin with Section 30:

DIVISION 5
TRANSITIONAL PROVISIONS

Application
30. (1) This Part does not apply to any organization in respect of personal information that it collects, uses or discloses within a province whose legislature has the power to regulate the collection, use or disclosure of the information, unless the organization does it in connection with the operation of a federal work, undertaking or business or the organization discloses the information outside the province for consideration.

Application
(1.1) This Part does not apply to any organization in respect of personal health information that it collects, uses or discloses.

Expiry date
*(2) Subsection (1) ceases to have effect three years after the day on which this section comes into force.

*[Note: Section 30 in force January 1, 2001, see SI/2000-29.]

Expiry date
*(2.1) Subsection (1.1) ceases to have effect one year after the day on which this section comes into force.

*[Note: Section 30 in force January 1, 2001, see SI/2000-29.]

These provisions were temporary (and expired on January 1, 2004), as part of the gradual implementation of PIPEDA, providing individual provinces with the ability to put in place substantially similar legislation during the period in which the law only applied to the federally regulated private sector and cross-border sales of information. It may be notable that the cross-border reference says "outside the province" and not "to another province".

In the absence of clear guidance from the statute, one can interpret it to apply in all circumstances where there exists a "real and substantial link" to Canada, following the Supreme Court's guidance in *SOCAN* and the cases to which Binnie J. refers. In any event, there is nothing in the statute that would prevent the Office of the Privacy Commissioner from assuming jurisdiction in the circumstances set out above if one takes the more modern and progressive view of jurisdiction that is currently being applied by the Canadian courts.

In the past, Officials with the Office of the Privacy Commissioner have advised that the Commissioner likely would assume jurisdiction where the collection of personal information is about Canadian residents or where the collection originates in Canada. This appears to no longer be the case. The Commissioner's office used to be of the view that PIPEDA is part of an international scheme of privacy protection that could reach over borders. The Privacy Commissioner has an arguable basis to make this second assertion and assume jurisdiction. As mentioned above, Canada implemented PIPEDA following the OECD Guidelines and in light of threatened restrictions on cross-border data flows caused by the European Directive.

While Canada is not bound by either the European Directive or the OECD Guidelines, it appears to be the spirit of PIPEDA that the Canadian law fit within this general scheme of international data protection. This, in and of itself, would give support for investigating the complaint brought by CIPPIC. Nevertheless, modern Canadian conflict of law jurisprudence clearly gives a Canadian adjudicative body, tribunal or investigator jurisdiction over activities that take place outside of our frontiers if there is a "real and substantial" connection to Canada. Whether that connection exists in the CIPPIC's complaint is both a question of law and a question of fact, two questions that the Assistant Commissioner appears not to have pursued. Unless CIPPIC seeks judicial review of the Assistant Commissioner's decision not to investigate, it may be some time before the question in judicially considered.

THE MCINNES COOPER PRIVACY TEAM

McInnes Cooper's Privacy Law Group has extensive experience in advising business on PIPEDA. If you have any questions, please contact any of the following:

Nova Scotia David T.S. Fraser 902 424 1347 david.fraser@mcinnescooper.com	**New Brunswick** Jaime Connolly 506 458 1544 jaime.connolly@mcinnescooper.com
Newfoundland Jackie Penney 709 724 8239 jackie.penney@mcinnescooper.com	