The Sedona Conference Journal

Volume 13 2012

Canada's Privacy Regime as It Relates to Litigation and Trans-Border Data Flows

Kelly Friedman

Recommended Citation: Kelly Friedman, *Canada's Privacy Regime as It Relates to Litigation and Trans-Border Data Flows*, 13 SEDONA CONF. J. 253 (2012).

For this and additional publications see:
https://thesedonaconference.org/publications

CANADA'S PRIVACY REGIME AS IT RELATES TO LITIGATION AND TRANS-BORDER DATA FLOWS

Kelly Friedman[1]
Davis LLP
Toronto, Ontario, Canada

Canadian courts have a long tradition of protecting individual privacy rights. Privacy rights are entrenched in Canada's Constitution[2] and are reinforced by the courts. In the context of litigation, Canadian courts strive to respect the privacy rights of litigants and third parties while ensuring parties adhere to document production obligations. More recently, the globalization of information processing, and the reality that personal information is "both here and there,"[3] has challenged the Canadian courts, as it has the rest of the global community, to consider the privacy implications of information being indifferent to national boundaries.

In this paper, I begin with an introduction to Canada's privacy regime. Next, I discuss how Canadian courts have reconciled production requirements with privacy concerns when the personal information remains within Canada's boundaries. Finally, I explore recent Canadian jurisprudence dealing with the management of privacy concerns regarding the flow of personal information across national boundaries.

Canada's Privacy Regime, in Brief

In the Canadian private sector, federal legislation, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"),[4] applies to federal works, undertakings and businesses, as well as to provincially regulated business in provinces that do not have adequately similar privacy legislation. To date, only three provinces have enacted private sector legislation which the Canadian government has recognized as being equivalent to PIPEDA: British Columbia, Alberta and Quebec.[5]

Privacy laws in Canada are based on two fundamental notions:

- An individual's personal information ought not to be used or disclosed without the person's consent or in contravention of the person's reasonable expectations; and

1 I am indebted to Sarah Willis, Summer Student in Davis LLP's Toronto office, for her assistance with the preparation of this paper.
2 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982 c 11, s 8, protects privacy rights against unreasonable intrusions from the State ("Everyone has the right to be secure against unreasonable search or seizure").
3 *Society of Composers, Authors and Music Publishers of Canada v Canadian Associations of Internet Providers*, 2004 SCR 45 at para 59, Binnie J [*SOCAN*].
4 SC 2000, c 5 [PIPEDA].
5 *Personal Information Protection Act,* SBC 2003, c 63; *Personal Information Protection Act*, SA 2003, c P-6.5; *An Act respecting the Protection of personal information in the private sector*, RSQ c P-39.

- A proper balance should be struck between the protection of privacy, on the one hand, and access to information or a commercial organization's need to collect, use and disclose personal information, on the other hand.

This balancing act was discussed by the Federal Court of Appeal in *Englander v TELUS Communications Inc*.[6] The court held that an individual's right to privacy is not absolute, and the provisions of PIPEDA are meant to establish the circumstances in which collection, use and disclosure of information can appropriately occur.[7] The court stated that the wording of the Act pointed to the application of an overarching standard of reasonableness in determining disputes.[8]

Personal information

Privacy laws protect an individual's "personal information." "Personal information" is defined similarly in most of the federal and provincial privacy statutes. In PIPEDA, personal information is defined as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."[9]

Canadian courts have given a generous interpretation to the definition of "personal information" in relation to privacy. In *Dagg v Canada (Minister of Finance)*,[10] the Supreme Court of Canada considered the definition of personal information in the context of the federal public sector privacy legislation. The court held that determining what constitutes personal information requires an analysis of the reasonable expectations of the individual. In this case, information regarding employee logs, specifically who was coming to work after hours, was found to be personal information for the purposes of the *Privacy Act*.[11] The Court found that it was a reasonable expectation of the employees that information regarding their whereabouts would be protected.[12]

Building off the *Dagg* decision, the Federal Court of Appeal further defined "personal information" in *Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)*.[13] The court focused mainly on whether it was personal information ***about*** an individual. The information at issue involved recordings of air traffic controllers. In determining that the communications at issue were of a professional nature, the court said that although they could help to identify an individual, they were not actually ***about*** the individual. The court also took into account that protection of this type of information was not consistent with the overall purpose of the *Privacy Act* and the values it was working to protect.[14]

A more recent case involving a Canadian furniture store, Leon's, had the Alberta courts interpreting "personal information" in the context of Alberta's private sector privacy legislation.[15] At issue in *Leon's* was the right of the company to record both driver's license and license plate numbers when third parties came to pick up furniture for a customer.

6 2004 FCA 387 [*Englander*].
7 *Ibid* at paras 38-40.
8 *Ibid* at para 102.
9 PIPEDA, *supra* note 4, s 2.
10 (1997), 2 SCR 403 [*Dagg*].
11 RSC 1985, c P-21.
12 *Dagg, supra* note 10 at paras 71-73.
13 2006 FCA 157 [*Transportation Accident Investigation and Safety Board*].
14 *Ibid* at para 54.
15 *Leon's Furniture Limited v Alberta (Information Privacy Commissioner)*, 2011 ABCA 94 [*Leon's*].

The court's decision arose out of two main issues: first, the definition of personal information and, second, the reasonableness of Leon's practices. Not unlike the courts in *Dagg* and *Transportation Accident Investigation and Safety Board*, the Alberta Court of Appeal in *Leon's* focused on whether the information at issue was about an individual. The court found that driver's license numbers fell under the definition of "personal information" because they are unique to each individual. With respect to license plates, the court determined that although license plates can be traced to individuals, they do not constitute information ***about*** the individual. The analysis addressed the reasonableness of Leon's decision to record driver's license and license plate numbers as a method of fraud prevention. The court felt that, when balancing between privacy and access, neither principle should be awarded paramountcy. As long as Leon's was acting reasonably, their actions were not contrary to the purpose of the statute.[16]

A recent Ontario Court of Appeal case can be contrasted with the *Leon's* decision. In *Citi Cards Canada v Pleasance*,[17] the Ontario Court of Appeal declined to order the production of a mortgage discharge statement. The court first held that information involving the amount owing on a mortgage constitutes information about an identifiable individual and, therefore, falls under the definition set out in PIPEDA. In coming to this determination, the court commented that the definition of personal information is an "elastic definition" and should be interpreted as such.[18] In *Citi Cards*, the court held that information about property owned by an individual constituted personal information. In *Leon's*, the court came to the opposite conclusion. The difference might be attributable to the nature of the property at issue. The balance owing on a mortgage is more intimately tied to the private affairs of an individual than the numbers attached to an individual's driving privileges.

Commercial activity

PIPEDA applies to organizations which collect, use or disclose personal information in the course of "commercial activities" in all provinces, except organizations that collect, use or disclose personal information entirely within the provinces of Alberta, British Columbia or Quebec, as such organizations are governed by their provincial private sector privacy legislation.[19] Accordingly, an important determination in many privacy related disputes is the definition of "commercial activity."

PIPEDA defines "commercial activity" as follows:

> Any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.[20]

The leading case on the interpretation of "commercial activity" involved a dispute over informal notes made by a doctor during an independent medical examination (IME) performed at the request of an insurance company.[21] The insured person, Mr. Rousseau,

16 *Ibid* at para 39.
17 2011 ONCA 3 [*Citi Cards*].
18 *Ibid* at paras 21-22.
19 See footnote 5, *supra*. Further, Health information collected, used or disclosed by health information custodians in Ontario is also not governed by PIPEDA, as it is governed by specific legislation, the *Personal Health Information Protection Act, 2004*, SO 2004, c 3.
20 *Supra* note 4 at s 2(1).
21 *Wyndowe v Rousseau,* 2008 FCA 39 [*Rousseau*].

was seeking access to the written notes after his insurance company terminated his long-term benefits. Whether the information collected by the doctor constituted personal information was not seriously disputed, therefore, one of the main issues was whether it was collected in the course of a commercial activity; in other words, was the IME transaction of a sufficient commercial nature to trigger PIPEDA? The Federal Court of Appeal found that the doctor was acting as an agent of the insurance company, which was engaged in a commercial relationship with Mr. Rousseau. This relationship established on the basis that it was governed by a contract whereby Mr. Rousseau paid the insurance company premiums.[22] Furthermore, the court found that it was the intention of Parliament to include transactions by insurance companies.[23]

With that brief introduction to some of the primary concepts in Canada's privacy regime, I turn to the special context of civil litigation.

Privacy Rights in Civil Litigation

Consent to the collection, use and disclosure of one's personal information is a cornerstone of privacy law in Canada. Express or implied consent, or a prescribed exception to the consent requirement, must always be present in respect of any collection, use or disclosure of personal information in the course of commercial activities.[24]

Exceptions to the consent requirement

The provincial private sector privacy Acts in Alberta, British Columbia and Quebec, as well as Ontario's *Personal Health Information Protection Act, 2004*, each include a provision specifically providing that nothing in the respective Acts shall be construed to interfere with information that is otherwise available by law to a party to a proceeding. PIPEDA does not contain a general exemption to the consent requirement in respect of litigation. Instead, PIPEDA contains several exceptions permitting the non-consensual collection, use or disclosure of personal information which may apply in the context of litigation proceedings. The most relevant exceptions in the litigation context are the following:

- An organization may collect personal information without consent if consent would compromise the availability or accuracy of the information and the collection is reasonable for purposes relating to investigating a breach of an agreement or a contravention of the laws of Canada or a province, including the common law.[25]

- An organization may use information without consent if it has reasonable grounds to believe the information could be useful in the investigation of a contravention of the laws of Canada and the information is used for the purpose of investigation.[26]

22 *Ibid* at para 35.
23 *Ibid* at para 37.
24 PIPEDA, *supra* note 4, sch 1, provides that "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate" (ss 4.3), and further that, "Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law" (ss 4.5).
25 *Ibid,* s 7(1)(b).
26 *Ibid,* s 7(2)(a).

- Disclosure without consent is permitted if the disclosure is made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization.[27]

Disclosure without consent is permitted for the purpose of collecting a debt owned by an individual, where required to comply with a subpoena, warrant, court order or the rules of court relating to the production of records or when made to an investigative body on reasonable grounds to believe that the personal information relates to a breach of an agreement or contravention of the laws of Canada or of a province or a foreign jurisdiction.[28]

In *Lisozzi v Bell Distribution Inc.*,[29] the Ontario Supreme Court discussed these exceptions and stated as follows:

> Section 7[(3)](c) in no way precludes the inspection of document No. 24 but instead mandates that the document can be produced or ordered to be produced to comply with the rules of court relating to inspection of documents. Section 7[(3)](a) complements that requirement by ensuring that disclosure can be made to the lawyer representing the party which then permits the solicitor to fulfill his or her duty vis-a-vis the necessity of full disclosure of all documents relating to any matter in issue in the action as required by Rule 30.03(4).[30]

Publicly available information

Publicly available information is also exempt from the consent requirement so long as the collection, use or disclosure relates directly to the purpose for which the personal information appears in the public record, document or registry, namely telephone books, professional or business directories, statutory registries, and documents of a judicial or quasi-judicial body that are available to the public.[31] In *Citi Cards*, the appellant argued that mortgage information fell under this exception because the amount of a mortgage is available from the Registry Office and the balance may be accessible from credit bureaus. The court rejected this argument, noting that mortgage information was not mentioned in the regulations, nor is the balance owing on a mortgage publicly available anywhere. The court clarified some aspects of section 7, saying that in order for information to fall under this exclusion, it must have been ***collected*** from a publically available source.[32]

Implied consent

Implied consent is also important in the litigation context. Not surprisingly, if one commences a lawsuit, he or she must expect to have some intrusions into their personal information. In *Ferenczy v MCI Medical Clinics*,[33] the court emphasized that a party

27 *Ibid*, s 7(3)(a).
28 *Ibid,* s 7(3)(c).
29 [2001] OJ No 2378.
30 *Ibid* at para 11.
31 PIPEDA, *supra* note 4, s 7(3)(h.1); *Regulations Specifying Publicly Available Information*, SOR/2001-7 s 1.
32 *Supra* note 17 at para 27.
33 [2004] OJ No 1775 [*Ferenczy*].

provides implied consent to the collection and use of relevant personal information when she commences a law suit:

> The plaintiff has given implied consent to the defendant to collect, record and use her personal information insofar as it is related to defending himself against her lawsuit. A plaintiff must know that by commencing action against a defendant, rights and obligations will be accorded to the parties to both prosecute and defend.[34]

In *M(A) v Ryan*,[35] the Supreme Court of Canada grappled with whether to order the disclosure of notes taken during a counseling session between a sexual assault victim and a psychiatrist. In determining whether an order for disclosure should be made, the Court noted that a balance between the proper administration of justice and the protection of individual privacy was needed in the litigation context.[36] In that case, the Court ordered the disclosure of the notes, but only the necessary parts and only to a very limited number of individuals. The Court emphasized that implied consent is given to the use of a plaintiff's personal information only to the extent necessary to bring to light information necessary to the determination of the dispute:

> …by commencing proceedings against the respondent Dr. Ryan, the appellant has forfeited her right to confidentiality. I accept that a litigant must accept such intrusions upon her privacy as necessary to enable the judge or jury to get to the truth….But I do not accept that by claiming such damages as the law allows, a litigant grants her opponent a license to delve into private aspects of her life which need not be probed for the proper disposition of the litigation.[37]

What if no exception applies, and no consent, implied or otherwise has been given?

Admissibility of personal information without consent in litigation

While a violation of PIPEDA during litigation will not necessarily render information inadmissible in civil litigation, disregarding individual privacy can be a factor considered by the courts in awarding costs and in determining whether to remove counsel from the record.[38] The court in *Ferenczy* dealt with the admissibility of videotape evidence in a medical malpractice claim. The plaintiff argued that the making and disclosure of the video were in contravention of PIPEDA. The court found that the evidence contained in the video was relevant and its probative value exceeded any prejudicial effects.[39] On the issue of privacy, the court provided valuable clarification on the applicability of PIPEDA in the litigation context. The defendant doctor had hired a private investigator to collect video evidence for use in the lawsuit. The plaintiff argued that the relationship was of a commercial nature and thus should be governed by PIPEDA. The court disagreed with this

34 *Ibid* at para 31.
35 (1997), 1 SCR 157 [*Ryan*].
36 *Ibid* at para 10.
37 *Ibid* at para 38.
38 *Supra* note 31.
39 *Ibid* at para 16.

argument, stating that the private investigator was simply acting as an agent for the doctor. The doctor was collecting the video evidence for a personal purpose – namely defending himself in a lawsuit, which is allowed under PIPEDA.[40] The presiding judge determined that the video tape evidence was not collected, used or disclosed in contravention of PIPEDA, but even if it had been, the evidence is relevant and admissible as a result of its probative value.[41]

A 2005 Ontario Superior Court decision further addressed admissibility of evidence when privacy concerns are raised.[42] The court stated that procedures for bringing complaints under PIPEDA are outlined in that Act, and therefore the court could not bypass these procedures and effectively override the Privacy Commissioner's jurisdiction to make an order regarding admissibility. The appropriate procedure would be for a complaint to be made under PIPEDA, and a report made by the Commissioner, and then potentially a hearing to be conducted in Federal court.[43]

Despite the requisite procedures, the Privacy Commissioner's report will not always govern. *Eastmond v Canadian Pacific Railway*[44] dealt with surveillance cameras placed around the worksite by Canadian Pacific Railway (CP). In that case, the Federal Court overruled the Privacy Commissioner's decision that the cameras were unreasonable and thus violated PIPEDA. In *Eastmond*, the court took a contextual approach saying that Parliament intended PIPEDA to be applied in a way that looks at why, how, when and where personal information is collected. Accordingly, in making a determination, the court should look at the appropriate circumstances surrounding collection, use and disclosure, noting that what is appropriate for collection may not be for use or disclosure and vice-versa.[45] The decision of the court turned, in part, on the fact that the recordings were never viewed unless there was a triggering event such as a theft. The court agreed with CP's argument that the collection of personal information did not actually occur until there was a triggering event, and at that point they were protected by the exemption under section 7(1)(b) of PIPEDA, which provides an exception if asking for consent would compromise the availability of the information for the purpose of an investigation.[46]

Implied undertaking rule

Prior to legislative protections for privacy interests in litigation, the "deemed undertaking rule", also known as the "implied undertaking rule", protected these interests, and continues to be invoked in the Canadian courtroom as a counterbalance to claims of intrusion on individual privacy. The implied undertaking rule is a common law rule developed as a response to concerns regarding the invasion of litigants' privacy that occurs in the course of a legal proceeding. The rule protects information obtained on discovery, preventing it from being used for purposes collateral to the proceedings in which it is disclosed.[47]

40 *Ibid* at paras 25-30.
41 *Ibid* at para 35.
42 *Osiris Inc v 1444707 Ontario Ltd* (2005), OJ No 5527 [*Osiris*].
43 *Ibid* at paras 83-84.
44 *Eastmond v Canadian Pacific Railway* (2004), 2004 FC 852.
45 *Ibid* at para 131.
46 *Ibid* at paras 187-190.
47 *Halsbury's Laws of Canada*, 1st ed, vol 2 (Markham, Ont: LexisNexis Canada, 2008) "Civil Procedure", VIII.3(9). The common law deemed undertaking rule has been codified in many Canadian rules of court. See, for example, Ontario Rules of Civil Procedure, RRO 1990, reg 194, r 30.1.

A 2008 Ontario Court of Appeal case provided an extensive analysis of the deemed undertaking rule as it applied to videotape disclosure.[48] At issue in *Kitchenham* was whether a plaintiff was under an obligation to produce a surveillance video received through the disclosure process in a prior civil case. In the reasoning, the court quoted the following excerpt from a leading English discovery text addressing the implied undertaking rule:

> The primary rationale…is the protection of privacy. Discovery is an invasion of the right of the individual to keep his own documents to himself. It is a matter of public interest to safeguard that right… it is in general wrong that one who is compelled by law to produce documents for the purpose of particular proceedings should be in peril of having those documents used by the other party for some purpose other than the purpose of the particular legal proceedings.…[49]

The court then went on to conclude that the documents at issue were protected by the implied undertaking rule and therefore could only be produced upon consent of the affected party or a court order under the *Rules of Civil Procedure*.[50]

Relevance and proportionality

The concepts of relevance and proportionality are also be used to protect privacy interests in Canada. *The Sedona Canada Principles*[51] emphasize taking a broad, holistic approach to discovery, specifically stating that proceedings in a discovery process should focus on proportionality, taking into account:

> (i) the nature and scope of the litigation, including the importance and complexity of the issues, interest and amounts at stake; (ii) the relevance of the available electronically stored information; (iii) its importance to the court's adjudication in a given case; and (iv) the costs, burden and delay that may be imposed on the parties to deal with electronically stored information.[52]

The Sedona Canada Commentary on Proportionality in Electronic Disclosure and Discovery[53] elaborates further by emphasizing the importance of considering non-monetary factors when analyzing the proportionality of evidence. Non-monetary costs, such as the invasion of privacy, are to be considered by judges when determining whether production of evidence should be restricted.[54] In making a determination, judges look to balance the relevance and importance of the requested information with the protection of privacy interests of the litigant or non-party.

---

48 *Kitchenham v AXA Insurance Canada* (2008), 94 OR (3d) 276 [*Kitchenham*].
49 Paul Matthews & Hodge Malek, *Discovery* (London: Sweet & Maxwell, 1992) at 253, cited in *Kitchenham. ibid* at para 31.
50 RRO 1990, reg 194, r 30.1.01(8).
51 *The Sedona Canada Principles Addressing Electronic Discovery*, 2008 at 11 [*The Sedona Canada Principles*], online: Sedona Conference <https://thesedonaconference.org/>.
52 *Ibid*.
53 *The Sedona Canada Commentary on Proportionality in Electronic Disclosure & Discovery*, 2010, online: Sedona Conference <https://thesedonaconference.org/>.
54 The *Sedona Canada Principles*, and the concept of proportionality, have explicitly been incorporated into the Rules of Civil Procedure in Ontario.

There are many examples in the Canadian courts of balancing production obligations with privacy concerns using the twin concepts of relevance and proportionality. In *Desgagne v Yuen*,[55] the plaintiff was severely injured in a collision while she was riding a bicycle. The defendants applied to the court for access to her hard drive, palm pilot, photos and video game console in the hopes that there would be evidence that she was exaggerating her injuries. The court likened disclosure of all of these documents to an electronic monitoring bracelet, noting that the former amounts to an even greater intrusion than the latter.[56] The court offered a valuable analysis on electronic discovery issues dealing with hard drives and metadata. The main concerns for the court were regarding the over-breadth of disclosure of this kind and the fact that potentially relevant data was only speculative in nature. There was no guarantee that production of the documents would end in relevant evidence. In this case, the intrusion far outweighed the probative value.[57]

The court in *Baldwin Janzen Insurance Services (2004) Ltd. v. Janzen* similarly dismissed an application to have a hard drive produced due to a lack of compelling reasons as to why it should be produced. There was nothing to suggest the defendant was lying or failing to disclose relevant documents, and so the court was loath to make the order.[58]

The court in *Vector Transportation Services Inc v Traffic Tech Inc*[59] came to a different conclusion than in the previous two cases, upholding an order for the production of the defendant's laptop to search for e-mails relevant to the claim. In coming to its conclusion, the court distinguished the facts from those in *Baldwin Janzen* and *Yuen*, saying that the former was a case where the plaintiff "simply did not justify the court making the intrusive order,"[60] and the latter involved a situation where the value of disclosure did not outweigh the values of privacy and the efficient use of judicial resources.[61] In *Vector Transport*, the documents to be produced were more carefully defined and there appeared to be evidence suggesting that relevant documents were in the defendant's possession.[62]

Redaction

Finally, redaction and de-identification of personal information are recognized by Canadian courts as useful tools to balance privacy concerns with production needs. If the personal information is contained in a document that otherwise meets the thresholds of relevance and proportionality so as to be producible, but the personal information itself is not relevant and proportional, it might be possible for the personal information to be removed or neutralized. In *Andersen v. St. Jude Medical, Inc.*,[63] Master MacLeod of the Ontario Superior Court considered the production of a database containing personal health information. He set out a useful test for when personal information could be redacted from an otherwise producible dataset:

a) The data produced must be substantially the same data as that which has been reviewed by the producing party's own experts. If not, then the parties' experts are being asked to draw conclusions based on different information.

55 2006 BCSC 955 [*Desgagne*].
56 *Ibid* at para 14.
57 *Ibid* at para 20-23.
58 2006 BCSC 554 [*Baldwin Janzen*].
59 (2008), OJ No 1020 (Ont SCJ) [*Vector Transportation*].
60 *Ibid* at para 17.
61 *Ibid* at para 24.
62 *Ibid* at para 27.
63 (2008), OJ No 430 [*Anderson*].

b) The forensic continuity of the data must be demonstrable such that any issues about authenticity or accuracy can be readily answered.

c) The process of redaction must not leave the data less meaningful or useful.

d) The process of redaction must not unduly delay production.[64]

As illustrate by the cases cited, the Canadian courts have much experience balancing production obligations with privacy rights as purely domestic issues.

International transfers and trans-border data flows

Developments in data processing have resulted in a novel set of privacy-related issues for the international community. Protection of personal data has gone from a domestic issue, to one that transcends national and geographical boundaries. In 1980, the Organisation for Economic Co-operation and Development (OECD) was the first international organization to tackle the issue. The OECD's 1980 guidelines established a set of governing principles that numerous countries utilized in developing domestic laws addressing these issues.[65] Many other organizations continue to address the implications of, and best practices for, international data transfers, including Working Group 6 of The Sedona Conference®, which released in December 2011 a public comment version of its *International Principles of Discovery, Disclosure & Data Protection: Best Practices, Recommendation & Principles for Addressing the Preservation and Discovery of Protected Data in US Litigation (European Union Edition)*.[66]

PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing.[67] Under PIPEDA, a "transfer" of personal information is a use by the organization. When personal information is transferred, it can only be used for the purposes for which the information was originally created (and no additional consent for the transfer will be required).[68] "Processing" is interpreted to include any use of the information by the third party for a purpose for which the transferring organization can use it.[69] Under Canadian law, organizations are held accountable for the protection of personal information "transfers" under each individual outsourcing agreement. PIPEDA requires the organization to use contractual or other means to "provide a comparable level of protection while the information is being processed by the third party."[70]

Aside from contractual terms, the Office of the Privacy Commissioner of Canada requires organizations to take into account the nature of the foreign regime, including

64 *Ibid* at para 31.
65 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), online: OECD <http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html>.
66 (2011), online: The Sedona Conference® <https://thesedonaconference.org/>.
67 Canada's public sector privacy law, the *Privacy Act*, RSC 1985, c P-21, also does not prohibit transfers of personal information. Note, however, that British Columbia and Nova Scotia have enacted legislation that limit a public body's ability to outsource the processing of personal information outside of Canada. However, even in these provinces, there are no restrictions on third party service providers accessing the information in Canada. See *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 and *Personal Information International Disclosure Protection Act*, SNS 2006, c 3.
68 PIPEDA, *supra* note 4, sch 1, ss 4.5; see also Office of the Privacy Commissioner of Canada, *Processing Personal Data Across Borders: Guidelines* (2009) at 5, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp> [*Guidelines*].
69 PIPEDA, *ibid*, ss 4.1.3; see also *Guidelines, ibid* at 5; see also Office of the Privacy Commissioner, *Bank's notification to customers triggers Patriot Act concerns* (2005), online: Office of the Privacy Commissioner <http:// 29717.vws.primus.ca/cf-dc/2005/313_20051019_e.cfm>.
70 PIPEDA, *ibid*, ss 4.1.3.

economic and social conditions to assess the risk to the integrity, security and confidentiality or customer personal information. In other words, an organization must ask itself "how likely is it that there will be access to the personal information by foreign courts, law enforcement and national security organizations?"[71]

While transfers of Canadian personal information outside the country is not prohibited, it is clear in Canada that the Office of the Privacy Commissioner of Canada has jurisdiction to regulate the transfers of personal data from Canada to other jurisdictions. This was confirmed in the 2007 case of *Lawson v Accusearch Inc.*[72] *Lawson* involved a judicial review of the Privacy Commissioner's decision concerning the collection, use and disclosure of Canadian personal information by a US company. The Privacy Commissioner said that she had no extraterritorial effect and, therefore, lacked jurisdiction to compel the respondent to produce evidence necessary to conduct the investigation. The Federal Court disagreed and stated that the destination of the information was irrelevant, because the information had to have come from Canada at some point. Therefore, although the inability to identify the Canadian sources may frustrate the investigation, it does not mean the Privacy Commissioner has no jurisdiction to act.[73] In *Lawson*, the Federal Court relied on the Supreme Court of Canada decision in *SOCAN*.[74] The question on appeal before the Supreme Court of Canada was "who should compensate musical composers and artists for their Canadian copyright in music downloaded in Canada from a foreign country via the Internet?"[75] The court began by stating that the capacity of the internet to disseminate information and art around the world is highly valued, but it should not be facilitated unfairly at the expense of the creator of the works.[76] The Court then concluded that there was a sufficient connection for taking jurisdiction when Canada was either the country of transmission or reception.[77]

A complaint by a Canadian regarding cloud computing likely also comes under PIPEDA and under the jurisdiction of the Privacy Commissioner of Canada. The Privacy Commissioner has taken the position that where the Privacy Commissioner has jurisdiction over the subject matter of the complaint (i.e. collection, use, disclosure of Canadian personal information) but the complaint deals with cloud computing infrastructure that is not obviously located in Canada, "current jurisprudence is clear that the Privacy Commissioner may exert jurisdiction when assessment indicates that a real and substantial connection to Canada exists".[78]

The case of *DataTreasury Corporation v Royal Bank of Canada*,[79] illustrates the Canadian courts' approach to data transfers from Canada to the United States, and highlights key aspects of the Canadian privacy regime, including the implied undertaking rule and the specific exemptions to consent which allow for international transfers. *DataTreasury* took the form of a motion before a Prothonotary of the Federal Court of Canada to settle the terms of a protective order. DataTreasury and certain banks, the "Banking Group", were engaged in patent infringement and patent impeachment proceedings. The parties contemplated a protective order to maintain the confidential aspects of the patented technology and other confidential information of the parties.

71 *Guidelines*, *supra* note 66 at 6-7.
72 (2007), 4 FCR 314 [*Lawson*].
73 *Ibid.*
74 *SOCAN, supra* note 3.
75 *Ibid* at para 1.
76 *Ibid* at para 40.
77 *Ibid* at paras 44-45 (This conclusion differed from the lower court's views that only transmission amounted to a sufficient connection).
78 Office of the Privacy Commissioner, *Reaching for the Cloud(s):Privacy Issues Related to Cloud Computing* (2010), online: Office of the Privacy Commissioner <http://www.priv.gc.ca/information/pub/cc_201003_e.asp>.
79 (2008), 2008 FC 955 [*DataTreasury*].

DataTreasury was headquartered in the United States and insisted that productions in the course of the proceedings would need to be sent to the United States because its central document database, document management consultants, United States counsel, witnesses and experts were all centralized in the United States. The Banking Group wanted a "Canada Only Clause" in the protective order that would have allowed the party producing information to serve and file a notice of motion to request an order preventing disclosure of the information outside of Canada. The receiving party would then be precluded from sending the information outside of Canada until after the final disposition of the motion, including any appeals.

The Banking Group expressed concerns about the transfer of its data to the United States which necessitated the "Canada Only Clause", as follows:

a) Canadian banks have been the subject of highly publicized privacy complaints relating to counter-terrorism laws;

b) The potential that these proceedings could prompt similar complaints and cause serious harm to the goodwill of the Banking Group;

c) The absence of the implied undertaking rule in the United States; and

d) That the security of the Canadian banking system could be needlessly compromised if detailed information relating to the networks used by the Banking Group for processing financial documents were permitted to leave the country.[80]

The Federal Court acknowledged that once the information had left Canada, it could be subject to production in ways not contemplated by the parties. However, the court also found that the Canada Only Clause would result in endless motions and could limit the ability of counsel to show relevant documentation to its client located in the United States and to receive instructions. In its decision, the court attempted to address the Banking Group's concerns. The court noted that section 7(3) of PIPEDA specifically permits disclosure of personal information in these circumstances. That is, the knowledge or consent of the individual to whom the information relates is not required where disclosure is required to comply with rules of court relating to the production of records, in this case, the Federal Court Rules. Further, it stated that the personal information of customers of the Banking Group need not be produced and could be redacted. With respect to the use of the documents once they were in the United States, the court noted that the documents disclosed in this proceeding were in fact impressed with the implied undertaking that the documents and information would not be used for purposes other than these proceedings. As a precaution, the court ordered that the implied undertaking rule be explicitly set out in the protective order. While the Banking Group raised a concern about seizure of the productions by the U.S. Government under the PATRIOT Act, the court noted that this seizure concern was raised "as a possibility not an absolute reality" and that several members of the Banking Group routinely engage in outsourcing activities which permit personal information of customers to be sent to the United States.[81]

80 *Ibid* at para 4.
81 *Ibid* at para 22.

The *DataTreasury* case illustrates several tools which the parties and the courts can use in the context of Canada-U.S. data transfers to maintain privacy rights and ensure production obligations are satisfied. A protective order can be used to limit access to documents and require those obtaining access to execute confidentiality agreements and to explicitly state the implied undertaking rule for the benefit of those U.S. parties who are unfamiliar with the implied undertaking rule. Further, redaction should always be considered as a means of ensuring irrelevant personal information does not get disclosed.

At The Sedona Conference® "4th Annual International Programme on Cross-Border Discovery and Data Privacy" held in Toronto in June 2012, the participants will consider whether such traditional tools to protect the privacy of Canadians, coupled with The Sedona Conference's *International Principles of Discovery, Disclosure & Data Protection: Best Practices, Recommendation & Principles for Addressing the Preservation and Discovery of Protected Data in U.S. Litigation (European Union Edition)*, are appropriate and sufficient for protecting privacy in the context of Canada-U.S. transfers. It is hoped that a consensus will emerge as to best practices for managing data flows across the Canadian border for use in U.S. litigation.