



10 ORDERS FOR DISCLOSURE: POTENTIAL USE OF THE USA PATRIOT ACT IN CANADA

The first question posed in the Request for Submissions is whether the USA Patriot Act permits US authorities to access personal information of British Columbians that is, through the outsourcing of public services, in the custody or under the control of USA-linked private sector service providers and, if so, under what conditions that can occur. We have already noted that, if personal information is located outside British Columbia, it is subject to the law that applies where it is found, regardless of the terms of the outsourcing contract. Chapter 5 provides a summary of USA Patriot Act amendments to the Foreign Intelligence Surveillance Act (FISA). The question this report focuses on is whether an order under the amended FISA could reach directly into British Columbia without the intervention or protection of Canadian law or processes, including the Freedom of Information and Protection of Privacy Act (FOIPPA).

Submissions from the British Columbia government and some information technology corporations conclude that US authorities would use alternative avenues rather than seeking access to personal information in Canada using the powers conferred by the USA Patriot Act. The Information Technology Association of Canada (ITAC) summarizes its position this way:

[T]he Patriot Act simply does not provide an efficient

or effective method of obtaining that information. Rather, given all of the legal and practical obstacles, common sense suggests that pre-existing methods of international criminal investigation such as letters rogatory, the Canada-United States [Mutual Legal Assistance Treaty] and informal requests for assistance (all of which require the cooperation of the Canadian government and Canadian courts) are much more likely to be employed.

It is therefore important to avoid over-emphasizing the relevance of the Patriot Act to situations in which public bodies in British Columbia outsource certain functions to “USA-linked” partners. In a very real sense, the Patriot Act should not be a substantial concern at all in those circumstances.¹

We disagree. In Chapter 9, we explained that US authorities seeking access to personal information in Canada would be unlikely to make use of the Mutual Legal Assistance Treaty or letters of request to Canadian courts when the Foreign Intelligence Surveillance Act (FISA) provides an alternative avenue. As discussed in Chapter 6, USA Patriot Act amendments to FISA alter the requirements for applications for court orders compelling the disclosure of records held by US-linked companies in Canada. In this chapter we discuss the factors likely to be considered by the Foreign Intelligence Surveillance Court (FIS Court) when it reviews such applications. We conclude that, while there is no way of predicting with certainty what approach the FIS Court may take, there is evidence to

¹ Submission of Information Technology Association of Canada (28 May 2004) p. 23.



suggest that current arrangements for the protection of personal information in British Columbia are unlikely to act as a firm disincentive, in all cases, against the issuance of FIS Court orders compelling disclosure.

There is general consensus in the submissions that the FIS Court could, under FISA, order a US corporation to produce records held in Canada by its Canadian subsidiary. There is no general consensus, however, about whether the FIS Court would make such an order in the face of a Canadian law prohibiting disclosure. We will now discuss the existing US case law said to provide the closest analogies to such orders that could be made by the FIS Court, accepting the consensus that the FIS Court would likely apply the same principles. We will then consider the balancing test that US courts use in deciding whether to order disclosure of records held outside the US, including where foreign law prohibits disclosure.

Disclosure of Foreign-Located Records Where Control is Shown

US courts have frequently upheld subpoenas ordering a corporation to disclose records located outside the US but under the corporation's control, even where they compel disclosure of records located in countries whose law prohibits disclosure.² US courts have also been willing to order disclosure of records held outside the US for the purpose of US proceedings, as long as a person or corporation subject to the US court's jurisdiction has control of those records.

In such cases, the US-located corporation at

which the disclosure requirement is directed must, on penalty of being found in contempt of court, obtain the records from abroad and turn them over. Contempt fines for failing to comply have in some cases been in the millions of dollars.³

In these cases, the subpoena or court order has not been enforced through a foreign court or a treaty. It is enforced directly by the US court using its power to punish non-compliance through contempt of court proceedings in the US against persons in the US. It is the threat of contempt of court penalties that leads to compliance and results in the subpoena or order having effect outside the US. In the case of FISA orders, it is a felony not to comply with the order.

Control over records

As the British Columbia government's submission acknowledges, in these cases, control of the records located outside the US is the key.⁴ The government also contends, however, that a US court must have what is known in US law as "personal jurisdiction" over the person who has the records before disclosure can be ordered and that the FIS Court is not likely to assert jurisdiction over a Canadian corporation that is affiliated with a US-located corporation where the Canadian corporation operates and is located outside the US.⁵ The government says the FIS Court is unlikely to assert personal jurisdiction over a Canadian corporation that has only minimal contacts with the US and says that, if a US court on this basis decided it does not have personal jurisdiction over the Canadian company, a FISA order cannot be served or be effective.⁶

2 See, for example, *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984). The grand jury is a feature of the US justice system that has no current counterpart in Canada. A grand jury investigates possible criminal activity and has the power to issue subpoenas compelling individuals to testify or compelling production of records.

3 In the case of *In re Grand Jury Proceedings (Bank of Nova Scotia)*, *ibid.* the Bank was fined \$1 825 000 for contempt of court arising from its failure to comply with the grand jury subpoena.

4 Submission of Government of British Columbia (23 July 2004) pp. 11-12.

5 *Ibid.* pp. 12-13.

6 *Ibid.* pp. 12-13, 32-33. Although the BC Government submission does not mention it, the submission of the American Civil Liberties Union (10 August 2004) says that, if foreign actions cause harm in the US, the US may assert jurisdiction over the foreign conduct and foreign actors responsible (p. 8). The ACLU refers to, for example, US anti-trust enforcement cases in which US courts have asserted jurisdiction where actions abroad have caused harm in the US, citing *In re Investigations of World Arrangements with Relation to the Production, Transportation, Refining and Distribution of Petroleum*, 13 F.R.D. 280 (D.D.C. 1952). We have chosen not to focus on this issue for the purposes of this report.



The British Columbia government is correct to recognize that control of records located outside the US is the key. It is also true that a Canadian subsidiary of a US-located corporation may not be subject to the personal jurisdiction of a US court. However, if the US parent controls records in the Canadian subsidiary's possession, the US court may still compel the US parent to get the records and produce them.

There are many examples of law enforcement and civil litigation matters where US courts have required US corporations to obtain and produce, in the US, records that are held outside the US but are controlled by the US-located corporation. In such cases, the US courts consider their personal jurisdiction over the US-located corporation to be sufficient to require production regardless of whether the court has personal jurisdiction over the party outside the US. As one court has said,

personal jurisdiction and "control" of documents are distinct issues in that [the] court can compel discovery of documents in "control" of a party although in "possession" of a person over whom there is no personal jurisdiction.⁷

It is, therefore, clear that US courts do not order disclosure on the basis of jurisdiction over the foreign corporation itself. As long as the court has jurisdiction over a US corporation that controls records located

abroad, the court can order disclosure.⁸ Location of the records is not the issue⁹—a US court will not permit a US-located corporation to resist producing records simply because the records are located outside the US.¹⁰

When control is being determined by a US court, its meaning is an issue of US law.¹¹ US courts use a number of factors to determine whether a US corporation controls records located outside the US. Control is not limited to legal ownership or actual physical possession of records. In deciding whether to order a corporation to obtain records in the physical possession of a foreign affiliate and disclose them in the US, US courts have interpreted the concept of control "broadly as the legal right, authority or practical ability to obtain the materials sought upon demand".¹²

Whether a US-located corporation controls records held abroad by its subsidiary depends on a number of factors, including the degree of ownership and control the parent exercises over the subsidiary, whether the two corporations operate as one, demonstrated access to records in the ordinary course of business and an agency relationship.¹³ Courts have held that a US parent corporation will, unless it proves otherwise, be held to control records located abroad that it requires in the ordinary course of business.¹⁴ Similarly, US courts have found that

7 *Dietrich v. Bauer*, 2000 U.S. Dist. LEXIS 11729 (S.D.N.Y. 2000) at 10-11, citing *Afros S/PA. v. Krauss-Maffei Corp.*, 113 F.R.D. 127, 129 (D. Del. 1986).
 8 *Dietrich v. Bauer*, *ibid.* at 6-7. US federal rules of civil procedure expressly provide that a party or non-party to US litigation can be ordered to produce records in its possession, custody or control: Fed.R.Civ.P. 34 and 45. The test for control is the same regardless of whether the records are sought from a party or a non-party: *Alcan International Ltd. v. S.A. Day Mfg. Co., Inc.*, 176 F.R.D. 75 at 78 (W.D.N.Y. 1996).
 9 *In re Marc Rich & Co., A.G.*, 707 F.2d 663 at 667 (2nd Cir. 1983). Also see *In re Grand Jury Subpoenas duces tecum addressed to Canadian International Paper Company et al.*, 72 F.Supp. 1013 (S.D.N.Y. 1947).
 10 *United States v. Chase Manhattan Bank, N.A.*, 584 F. Supp. 1080 at 1085 (S.D.N.Y. 1984).
 11 *Ssanyong Corp. v. Vida Shoes Int'l, Inc.*, 2004 U.S. Dist. LEXIS 9101 at 4-5 (S.D.N.Y. 2004). Section 3(1) of FOIPPA provides that FOIPPA only applies to a record "in the custody or under the control of a public body". In light of US cases confirming that the issue of whether a US corporation has control of records located abroad is a question of US law, the FOIPPA control test is unlikely to be relevant for a US court making a control determination.
 12 *Bank of New York v. Meridien Biao Bank Tanzania*, 171 F.R.D. 135 at 146 (S.D.N.Y. 1977). See also, *Dietrich v. Bauer*, *supra* note 7 at 7, citing, among other decisions, *Asset Value Fund, Ltd. v. The Care Group, Inc.*, 1997 U.S. Dist. LEXIS 19768 at 9 (S.D.N.Y. 1997).
 13 *Dietrich v. Bauer*, *ibid.* at 7-8.
 14 *Cooper Industries, Inc. v. British Aerospace, Inc.*, 102 F.R.D. 918 at 920 (S.D.N.Y. 1984).



a parent corporation has a sufficient degree of ownership and control over a wholly-owned subsidiary that it must be deemed to have control of documents located with that subsidiary.¹⁵

It has even been said that a US corporation will control a foreign corporation if the US corporation can, directly or indirectly, through another corporation or corporations, elect a majority of the directors of the foreign corporation.¹⁶ The *Restatement (Third) of the Foreign Relations Law of the United States* says this:

Courts in the United States have generally held United States corporations responsible for production of documents located abroad in the possession of their foreign branches or subsidiaries, unless a defence, such as an effective blocking order, is applicable where the information is located.¹⁷

It is not possible, in the absence of details of specific outsourcing arrangements, to say whether personal information located in British Columbia is in the control of a US parent corporation on the basis of the ownership or other tests applied by some US courts. We consider, in any event, that the US federal court decisions in which control over foreign records has been found on the basis of the parent-subsidiary relationship alone must be given some weight. We adopt, therefore, the working assumption that control, as a matter of US law, may be found on the basis of corporate relationship alone, regardless of the contractual or practical arrangements between the public body and the service provider or the public body and US-located parent corporation.

Effect of contractual prohibitions and security arrangements

We do not suggest that public bodies cannot or should not implement contractual or practical arrangements relating to control. To the contrary, we recommend that such arrangements be put into place. This is because, despite the cases in which corporate ownership is enough to establish control over records, other cases suggest that such measures might influence the control issue.

For one thing, the US cases usually deal with business records of a foreign subsidiary. The courts have found that the parent company controls a subsidiary's business records that are accessible to the US-located parent in the ordinary course of business. In the case of outsourcing of public services, by contrast, personal information contained in records possessed by the US-linked service provider is third-party personal information. We are not prepared to say a US court would ignore outsourcing agreement provisions and practical arrangements that clearly preclude the US-located parent from having access to the personal information for any purpose at all. It is, again, difficult to predict how the FIS Court might approach the matter, but there is reason to believe that corporate ownership might not be the sole litmus test of control over records under US law.

Any contractual and practical measures to keep personal information out of the control of a US-located parent corporation would also speak to British Columbia public policy respecting the privacy of personal information. This is important because, even if a US court decides that records located outside the US are controlled by a US-located corporation, it will apply a balancing test to decide whether it

¹⁵ *Dietrich v. Bauer*, *supra* note 7 at 8-9, citing several decisions from various US federal courts. Also see, for example, *In re Uranium Antitrust Litigation*, 480 F.Supp. 1138 (N.D. Ill. 1979).

¹⁶ *In re Investigations of World Arrangements with Relation to the Production, Transportation, Refining and Distribution of Petroleum*, *supra* note 6 at 285.

¹⁷ *Restatement (Third) of the Foreign Relations Law of the United States* § 442 note 10 (1986).



should order disclosure in the face of foreign law that prohibits disclosure.

We discuss below the balancing test US courts apply in deciding whether to order disclosure of foreign records. Before doing so, however, we will address the contention in some submissions that, apart from the balancing test, other procedural or policy safeguards exist that make it unlikely that US authorities will seek to directly enforce a FISA order in Canada.

Are There Other Safeguards?

The British Columbia government, EDS Canada Inc. (EDS), the FBI and the US Department of Homeland Security (DHS) all contend that protections are in place to guard against inappropriate extraterritorial application of FISA orders. Neither the FBI nor the DHS provides details about these protections. The British Columbia government suggests that US government lawyers are required, before they seek to force disclosure of records abroad, to seek approval from the Office of International Affairs (OIA) of the US Department of Justice. The British Columbia government says this stems from recognition of the distaste expressed by other countries for extra-territorial application of US subpoenas. The British Columbia government adds that the US is now much more sensitive than it was to objections by other countries to extra-territorial application of US subpoenas and is less likely to use them than in the past. It says the use of FISA proceedings will be similarly constrained.¹⁸ EDS makes similar points in its submission.¹⁹

No basis is offered for the claim that the US

government and its institutions are, after September 11, more deferential to foreign sensibilities about extra-territorial application of US laws. In fact, US cases decided before September 11 show that, even then, any concerns about extra-territorial application of US law were often overcome. We see no reason to believe that US courts—including the FIS Court—will be more, not less, inclined after September 11 to shrink from using lawful means to obtain intelligence information from abroad. We also note that, since its enactment in 1978, FISA has specifically distinguished between the interests and rights of US persons and the interests of non-US persons.

Nor does the British Columbia government explain why it believes that the US government's policy to require federal prosecutors to work through the OIA applies to FISA processes and FISA orders. The government points to section 279 of the Criminal Resources Manual of the US Department of Justice and its controls on seeking records abroad. We note, however, that this 1997 version of the manual specifically relates to criminal prosecutions and not national security activities. We are aware of no reason to believe that the FBI and its lawyers may or must follow these rules in seeking a FISA order for intelligence purposes alone.

We have also considered Executive Order 12333,²⁰ to which the relevant FISA section refers, and the required guidelines approved in 2003 by the US Attorney General (National Security Investigations (NSI) Guidelines).²¹ Neither sets out procedural safeguards or policy requirements relating to use of FISA orders to obtain records located abroad, although we note that the published version of the Attorney General's guidelines has been heavily redacted on

18 Submission of Government of British Columbia (23 July 2004) pp. 11-15, 36-37.

19 Submission of EDS Canada Inc. (19 July 2004) pp. 31-35 (legal opinion of Steptoe & Johnson LLP).

20 Executive Order 12333—United States Intelligence Activities 46 FR 59941, 3 CFR, 1981 Comp. A copy of the Order is available on the US Central Intelligence Agency website: www.cia.gov

21 The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (31 October 2003) Reproduced on the website of the US Department of Justice, Office of Legal Policy: www.usdoj.gov/olp/



national security grounds. Nor are any safeguards offered in the rules governing the FIS Court's processes, which only recently came to public attention through a US access to information request. By their terms, the rules only allow specially designated US government lawyers and agents to appear or participate in hearings held in private before the court.²²

EDS contends that FBI officials are deterred from inappropriately obtaining FISA orders because they might be prosecuted under US law if they were to do so.²³ We do not question the good faith of FBI officials in exercising their power to seek FISA orders, but we note that the British Columbia government's submission indicates only one FISA application of the thousands that have been made to the FIS Court has ever been denied.²⁴ Although it appears the number of FISA applications increased substantially in 2003, according to the annual FISA report that the US Attorney General is required to make to Congress, only 4 of 1,727 FISA applications made in that year were rejected by the FIS Court.²⁵

We do not exclude the possibility that policy or procedural safeguards exist in respect of FISA applications for disclosure of records located outside the US. In the absence of evidence of such safeguards, however, this report proceeds on the basis that US authorities are unfettered in their ability to seek such an order and may do so in some circumstances. One of the recommendations we make in Chapter 11 is that the British Columbia government, in conjunction with the government of Canada as appropriate and necessary, should seek assurances from relevant US

government authorities that they will not seek a FISA order (or issue a national security letter) for access to personal information records in British Columbia.

We will now discuss the balancing test for disclosure of records located outside the US.

The Balancing Test for Compelling Disclosure

A number of the submissions referred to the balancing test that US courts apply in deciding whether to order disclosure from outside of US. The British Columbia government, for example, pledged in its submission to enact legislation precluding disclosure of records under FISA, recognizing that a US court will consider such a law as part of the balancing test.²⁶ The submission of EDS contends, without qualification, that a US court would honour a Canadian statutory prohibition against disclosure,²⁷ while the BCGEU and ACLU submissions express the opposite view.²⁸

A US order for foreign disclosure may or may not be enforced where foreign (including Canadian) law prohibits disclosure. In some cases US courts have been uneasy about enforcing disclosure abroad²⁹ because they acknowledge that the laws of a country do not generally extend beyond its borders. It is recognized that attempts to enforce laws outside a country are highly unpopular in the international community. As noted in the *Restatement (Third) of the Foreign Relations Law of the United States*:

22 US, Rules of the Foreign Intelligence Surveillance Court, r. 9; a copy of this document is available on the ACLU website: www.aclu.org and on the website of the Federation of American Scientists: www.fas.org.

23 Submission of EDS Canada Inc. (19 July 2004) p. 28 (legal opinion of Steptoe & Johnson LLP).

24 Submission of Government of British Columbia (23 July 2004) p. 29, note 38.

25 The Electronic Privacy and Information Center has published a summary of information taken from the annual FISA reports on its website: www.epic.org. A list of the annual FISA reports is available on the website of the Federation of American Scientists: www.fas.org.

26 We understand the proposed amendments to FOIPPA in Bill 73 to be blocking legislation in this regard: Freedom of Information and Protection of Privacy Amendment Act, 2004, 5th Sess., 37th Parl., BC, 2004 (3rd reading 19 October 2004).

27 Submission of EDS Canada Inc. (19 July 2004) pp. 31-32 (legal opinion of Steptoe & Johnson LLP).

28 Submissions of BCGEU (6 August 2004) p. 49 and American Civil Liberties Union (10 August 2004) pp. 9-11.

29 See, for example, *In re Sealed Case*, 825 F.2d 494 at 497-99; (D.C. Cir. 1987) 498-499.



No aspect of the extension of the American legal system beyond the territorial frontier of the United States has given rise to so much friction as the requests for documents in investigation and litigation in the United States. As of 1986, some 15 states had adopted legislation expressly designed to counter United States efforts to secure production of documents situated outside the United States....

The common theme of foreign responses to United States requests for discovery is that, whatever pre-trial or investigative techniques the United States adopts for itself, they may be applied to persons or documents located in another state only with permission of that state. The United States position, on the other hand, has been that persons who do business in the United States, or who otherwise bring themselves within United States jurisdiction to prescribe and to adjudicate, are subject to the burdens as well as the benefits of United States law, including the laws on discovery. This section [of the *Restatement (Third)*] generally supports the United States position, subject, however, to the principle of reasonableness.³⁰

Our review of US law leads us to conclude that US courts have been willing to enforce disclosure of foreign-located records sought for use in the US and in some cases have done so even where foreign law prohibits disclosure. In deciding whether to order disclosure from abroad, a US court balances a number of factors in deciding whether the US interest in disclosure outweighs the interest in avoiding extra-territorial application of US subpoenas or court orders.³¹ As one US court has observed,

[m]echanical or overbroad rules of thumb are of little value; what is required is a careful balancing of the interests involved and a precise understanding of the facts and circumstances of the particular case.³²

Among the various factors a court will consider are those described in the *Restatement (Third)* as follows:³³

§442. REQUESTS FOR DISCLOSURE: LAW OF THE UNITED STATES

(1) (a) A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.

(b) Failure to comply with an order to produce information may subject the person to whom the order is directed to sanctions, including finding of contempt, dismissal of a claim or defense, or default judgment, or may lead to a determination that the facts to which the order was addressed are as asserted by the opposing party.

(c) In deciding whether to issue an order directing production of information located abroad, and in framing such an order, a court or agency in the United States should take into account the importance to the investigation or litigation of the documents or other information requested; the degree of specificity of the request; whether the information originated in the United States; the availability of alternative means of securing the information; and the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.

(2) If disclosure of information located outside the United States is prohibited by a law, regulation, or order of a court or other authority of the state in which the information or prospective witness is located, or of the state of which a prospective witness is a national;

³⁰ *Restatement (Third) of the Foreign Relations Law of the United States*, supra note 17 at note 1.

³¹ See, for example, *First Am. Corp. v. Price Waterhouse LLP*, 154 F.3d 16 at 22 (2d Cir. 1998). In the case *In re Grand Jury Proceedings (Bank of Nova Scotia)*, supra note 2 at 26-27, the court considered similar factors as set out in the *Restatement (Second) of the Foreign Relations Law of the United States* § 40 (1965).

³² *United States v. First Nat'l City Bank*, 396 F.2d 897 at 901 (2d Cir. 1968).

³³ See, for example, *Volkswagen, A.G. v. Valdez*, 909 S.W.2d 900 at 902 (Tex. Sup. Ct. 1995).



- (a) a court or agency in the United States may require the person to whom the order is directed to make a good faith effort to secure permission from the foreign authorities to make the information available;
- (b) a court or agency should not ordinarily impose sanctions of contempt, dismissal, or default on a party that has failed to comply with the order for production, except in cases of deliberate concealment or removal of information or of failure to make a good faith effort in accordance with paragraph (a);
- (c) a court or agency may, in appropriate cases, make findings of fact adverse to a party that has failed to comply with the order for production, even if that party has made a good faith effort to secure permission from the foreign authorities to make the information available and that effort has been unsuccessful.³⁴

While a court may consider other factors, we are proceeding on the assumption that those set out in §442(1)(c) of the *Restatement (Third)* are the core factors.

It should be noted here that the factors set out in the *Restatement (Third)* have been fashioned for the purposes of US litigation or investigations where foreign subsidiaries of companies subject to the US court's jurisdiction hold relevant records abroad. These cases involve proceedings in ordinary US courts. We cannot say with certainty what approach the special FIS Court would apply to the extra-territorial enforcement issue in relation to personal information records located in British Columbia that are involved in the outsourcing of public services to US-linked service providers.

There is, however, some consensus in the

submissions that the FIS Court would find that it has the authority to order a US parent of a Canadian subsidiary to obtain and disclose records located in Canada but controlled by the US parent. We accept this view. We also accept the view expressed in a number of submissions that the FIS Court is likely to consider some or all of the factors in the *Restatement (Third)* in deciding whether to compel production of records located in Canada under a FISA order.

The fact that only two FISA decisions have ever been released—neither of which is relevant here—makes our assessment of how the FIS Court might apply the *Restatement (Third)* factors necessarily somewhat speculative. We can only suggest, applying the approach in cases decided under other US laws, how the FIS Court might apply them.

Specificity of the request for disclosure

The British Columbia government submission refers to cases in which the US court has said that the scope of a disclosure subpoena or order must be reasonable.³⁵ As we understand this, the British Columbia government is referring to cases in which US courts have restricted the scope of subpoenas to records reasonably related to the investigation or proceeding under way. The government appears to be suggesting that a comparable scope restriction, which depends on the facts of each case, will safeguard British Columbians' personal information in the context of outsourcing because any FISA order that might be issued with effect in British Columbia would be similarly limited.

The ACLU's submission also suggests that the FIS Court might require proposed orders for disclosure of records to be specific. It maintains that FISA allows for broad records requests, but

³⁴ *Restatement (Third) of the Foreign Relations Law of the United States*, *supra* note 17, § 442.

³⁵ Submission of Government of British Columbia (23 July 2004) p. 12; however, the BC Government acknowledges that it is uncertain whether the FIS court would apply the same legal principles in the context of FISA that an ordinary US court would apply in the context of a grand jury subpoena.



notes that “[c]ourts have struck down sweeping demands for information that could not meet the test of being ‘reasonably relevant’ to an actual, authorized investigation.”³⁶ We also acknowledge that the US Department of Justice rules governing FISA applications and its FISA minimization requirements, which speak to relevance and minimal collection, could influence the FIS Court to impose a comparable standard of specificity and reasonableness on FISA orders.

Origin of the information sought

We mentioned earlier the prospect that the FIS Court might account for the fact that a US-linked contractor possesses records for the limited purpose of performing services and has no control over the records. In some US cases, the court has considered whether the records in question originated in the US or abroad. It is reasonable to expect a US court to look unfavourably on any attempts to avoid disclosure by removing US records from the country. However, this would not be the case with personal information of British Columbians involved in outsourcing. The records would originate in British Columbia and be in the possession of the US-linked contractor only for the purposes of the outsourcing.

Importance of the records to the US investigation

US courts will consider the importance of the records to the litigation or proceeding for which they are sought. The more important the requested records are to the litigation or other proceeding, the more likely the court will issue an order for disclosure. For

example, in *Volkswagen, AG v. Valdez*, applying the balancing test in § 442 of the *Restatement (Third)*, the court held that the records sought were not important to the US litigation because the plaintiffs already had previous versions of the same information.³⁷ Similarly, in *Minipeco, SA v. ContiCommodity Services, Inc.*,³⁸ the court was influenced by the fact that much of the information in documents sought from Switzerland was not relevant to the litigation and noted that a great deal of commercial information of third parties not involved in the case would be revealed.

The FIS Court may decline to issue a FISA order for disclosure of personal information records in Canada if it views the records as only marginally relevant to the purpose for which they are sought. Although it has been a factor of influence in some conventional litigation cases, it might be difficult to apply to the more diffuse context of a FISA investigation where no investigation of a specific offence is involved.

Existence of alternative means of obtaining the information

The availability of adequate alternatives for obtaining the information sought can weigh against ordering disclosure in the face of a prohibition under foreign law.³⁹ We have already dealt with the contention that MLAT is the default information gathering mechanism for US authorities. MLAT provides for the continued use of other agreements, arrangements or practices and, in any event, is not available where US authorities seek to gather information for purposes other than an investigation or prosecution for an offence as defined by MLAT.

We have also noted that Canadian and US authorities can and do use other arrangements to share information for intelligence and national security

³⁶ Submission of American Civil Liberties Union (10 August 2004) p. 11.

³⁷ *Volkswagen, A.G. v. Valdez*, *supra* note 33.

³⁸ *Minipeco, SA v. ContiCommodity Services, Inc.*, 116 F.R.D. 517 (S.D.N.Y. 1987)

³⁹ See *Volkswagen, A.G. v. Valdez*, *supra* note 33.



purposes. It is possible that the FIS Court, assuming it was aware of such other arrangements, might decline to order disclosure from Canada where bilateral arrangements could be used to get the information.

Good faith of the person from whom disclosure is sought

US courts have considered the good faith of the US-located person resisting disclosure in trying to get the information being sought. Some courts address this factor only in deciding whether to enforce the disclosure order, while others consider it when deciding whether to order disclosure in the first place.

Good faith is a consideration where foreign law—such as a banking secrecy law—requires the party resisting disclosure to get consents from foreign parties whose information is affected. In *Société Internationale Pour Participations Industrielles Et Commerciales, S. A. v. Rogers*,⁴⁰ for example, the US Supreme Court found that the affected party had made extensive efforts to get records from Switzerland but faced criminal prosecution there if it turned the records over in response to the US court order. Similarly, in *Minipeco, SA v. ContiCommodity Services, Inc.*,⁴¹ the court noted that the affected party had made extensive efforts to obtain documents abroad, including by getting consents from third parties that allowed disclosure of their records. Its efforts clearly influenced the court's decision not to order further disclosure.

By contrast, in *Ssangyong Corp. v. Vida Shoes Int'l, Inc.*,⁴² the court noted that the party resisting disclosure had, for three months, made no attempt to comply with the disclosure requirement. This weighed in favour of requiring disclosure of banking records despite a common law rule in Hong Kong requiring banking confidentiality.

Competing interests of the US and Canada

As indicated above, the *Restatement (Third)* indicates the court should weigh the interests of the US and the foreign jurisdiction in deciding whether to order disclosure. The following passage from the comments on § 442(1)(c) of the *Restatement (Third)* is helpful in explaining how a US court should assess this factor:

In making the necessary determination of foreign interests under Subsection (1)(c), a court or agency in the United States should take into account not merely a general policy of the foreign state to resist “intrusion upon its sovereign interests,” or to prefer its own system of litigation, but whether producing the requested information would affect important substantive policies or interests of the foreign state. In making this determination, the court or agency will look, [among other things], to expressions of interest by the foreign state, as contrasted with expressions by the parties; to the significance of disclosure in the regulation by the foreign state of the activity in question; and to indications of the foreign state's concern for confidentiality prior to the controversy in connection with which the information is sought. ...

In making the necessary determination of the interests of the United States under Subsection (1)(c), the court or agency should take into account not merely the interest of the prosecuting or investigating agency in the particular case, but the long-term interests of the United States generally in international cooperation in law enforcement and judicial assistance, in joint approach to problems of common concern, in giving effect to formal or informal international agreements, and in orderly international relations. ...⁴³

As this passage indicates, the US court must balance US interests against foreign interests. A

40 *Société Internationale Pour Participations Industrielles Et Commerciales, S. A. v. Rogers*, 357 U.S. 197 (1958).

41 *Minipeco, SA v. ContiCommodity Services, Inc.*, *supra* note 38.

42 *Ssangyong Corp. v. Vida Shoes Int'l, Inc.*, *supra* note 11.

43 *Restatement (Third) of the Foreign Relations Law of the United States*, *supra* note 17, comment c.



significant issue is whether a foreign legal prohibition against disclosure of the requested records will overcome US interests in disclosure.

Canadian statutory restrictions on disclosure

As noted earlier, the submission of EDS says that where Canadian law restricts disclosure of personal information, a US court will honour that restriction.⁴⁴ As the BCGEU points out, however, the case EDS cites as the “closest case on point” in support of its proposition⁴⁵ was later disavowed by the same court.⁴⁶ Our research discloses that, where competing US interests favour disclosure, a US court may order it despite the existence of a foreign law prohibiting disclosure.⁴⁷ As one court put it, “The possibility of civil or criminal sanction [abroad] will not necessarily prevent enforcement of a subpoena.”⁴⁸

In fact, US courts have, in the face of foreign laws prohibiting disclosure, been willing to enforce disclosure of records for the purposes of enforcing US criminal fraud laws⁴⁹ and securities laws.⁵⁰ Even in purely private litigation, where no US government interest is directly involved, US courts have in some cases given more weight to the general US interest in resolving litigation in US courts than to foreign laws prohibiting disclosure of the records.⁵¹

We do agree, however, with the following statement from the submission of the ACLU:

The most important portion of the balancing test is the weighing of the interests of the two states involved. Courts have tended to be extremely deferential in cases where the state interest is a criminal prosecution. Because requests involving the Patriot Act apply not only to criminal acts but to terrorism (a crime that all nations have an important interest in resolving and that tends to be international in scope), it is likely that a U.S. court would give significant weight to this interest. Courts have also recognized that the other nations have a legitimate and important privacy interest in their citizens’ personal information, but have tended to be sceptical of secrecy laws (general in the context of bank records) when they interfere with criminal investigations or strong state interests.

...
As a practical matter, cases brought by the government (especially those involving violations of criminal law) have tended to favor the disclosure of records because courts accord them great weight under the “significant government interest” prong of the test. While it is difficult to predict the access that U.S. courts will grant to foreign records, it is likely that if the U.S. government claims that its interest lies in preventing terrorist activity and it attempts to limit the amount of the request, a court will find that it has satisfied the prongs of the balancing test and should be granted the records it seeks.⁵²

We agree that, although the facts of each case determine the outcome, particularly in the post-September 11 world, the amendments to FISA appear to demonstrate that the scope of what are considered to be vital US national interests in ensuring national security and protecting against terrorism has grown.

44 Submission of EDS Canada Inc. (19 July 2004) p. 31 (legal opinion of Steptoe & Johnson LLP).

45 *Ings v. Ferguson*, 282 F.2d 149 (2d Cir. 1960).

46 *United States v. First Nat’l City Bank*, *supra* note 31; also see *Minipeco, S.A. v. ContiCommodity Services, Inc.*, *supra* note 38.

47 *In re A Grand Jury Subpoena dated August 9, 2000*, 218 F. Supp. 2d 544 at 554 (S.D.N.Y. 2002). Also see *Compagnie Française d’Assurance Pour le Commerce Extérieur v. Phillips Petroleum Co.*, 105 F.R.D. 16 (S.D.N.Y. 1984).

48 *In re A Grand Jury Subpoena dated August 9, 2000*, 218 F. Supp. 2d 544; 2002 U.S. Dist. LEXIS 16800 (S.D.N.Y., 2002), at para. 23.

49 *United States v. Davis*, 767 F.2d 1025 (2d Cir.1985), where enforcing criminal laws against fraud overcame the Cayman Islands’ interest in bank secrecy.

50 *SEC v. Banca Della Svizzera Italiana*, 92 F.R.D. 111 (S.D.N.Y. 1981), compelling production in regulatory action to enjoin violations of US federal securities laws.

51 See, for example, *Ssangyong Corp. v. Vida Shoes Int’l, Inc.*, *supra* note 11.

52 Submission of American Civil Liberties Union (10 August 2004) pp. 10-11.



Since US courts have sometimes found lesser US interests to trump foreign statutes prohibiting disclosure, a Canadian statutory prohibition against disclosure, standing on its own may, but will not necessarily, overcome the vital US interests FISA investigations are said to be aimed at protecting.

Conclusions

We conclude that, although the FIS Court may consider a Canadian statutory prohibition against disclosure, there are no guarantees that the prohibition alone would move the court to decline to issue an order under FISA, particularly when the grounds for the application are cast as vital US interests. Nevertheless, at a minimum, enactment of such statutory provisions in Canada provides US courts with a clear statement of public policy respecting the importance we attach to the privacy of personal information in British Columbia, particularly when it has been generated through necessary use by the public of the many services provided to them by public bodies in British Columbia.⁵³

The probability of a Canadian statutory prohibition against disclosure having persuasive effect on decisions of the FIS Court, or any foreign court, could be increased, in our view, if the prohibition were made specific to orders issued by a foreign court, or other foreign authority, and carried considerable penalties for breach, including large fines and imprisonment. Of course, the secrecy of the FIS Court and the fact that only US government lawyers appear before it lessen the probability that British Columbia law and policy will be brought to

the court's attention.⁵⁴

Despite any persuasive effect this type of legislation may have on decisions made by foreign courts such as the FIS Court, the most significant value of this legislation could be its practical and legal effect within British Columbia. Regardless of a decision by a US court that records are in the control of a US-linked organization are required for US litigation or relate to a vital US interest, if the records are subject to FOIPPA then, as a matter of law in British Columbia, they cannot be disclosed in response to a US court order. Compliance with FOIPPA must, of course, be a term of all outsourcing contracts and meaningful contractual terms respecting breach of contract would have to complement the direct statutory prohibitions.

Direct statutory prohibitions against disclosure in response to any form of order or request made by a foreign court or foreign authority, accompanied by considerable penalties for breach, provide a substantial incentive for compliance with British Columbia law by a person served with a foreign order for disclosure of personal information records in British Columbia. The threat of prosecution accompanied by a substantial fine or even imprisonment could be expected to be a factor in deterring a person or public body from abiding by the terms of a foreign order and failing to comply with British Columbia law in this regard. Such provisions also provide a defence to the person served with the foreign order and obligate them to notify the public body that it has been made. This is of particular importance in the context of FISA orders (and national security letters), the existence of which would otherwise remain shielded from

⁵³ Statutory provisions intended to counter the effect of foreign orders may be enacted at the provincial or federal level and are not unknown in Canadian law. For example, Canada has occasionally used the Foreign Extraterritorial Measures Act (FEMA), R.S.C. 1985, c. F-29, to block foreign laws, such as the US Helms-Burton Act, that purport to reach into Canadian law in violation of principles of international law and comity.

⁵⁴ In this respect, there is some suggestion that, in ordinary court proceedings, a US court might be influenced by the fact that the foreign government whose laws are implicated has made the effort to appear as a friend of the court and has resisted disclosure in defence of its laws. See, for example, *Volkswagen, A.G. v. Valdez*, *supra* note 33, and *In re Uranium Antitrust Litigation*, *supra* note 15.



attention.

In Chapter 9, we concluded that US authorities engaged in foreign intelligence gathering would not be likely to use the MLAT for a number of reasons. We also concluded that a ban on outsourcing would not be a practical or effective way of ensuring the protection of personal information of British Columbians. In this chapter, we have concluded

that there are no assurances that the FIS Court will not grant orders compelling US-linked companies to disclose personal information records located in Canada, particularly when vital US interests are considered to be at stake. The existence of that reasonable possibility warrants other mitigating steps being taken, such as direct statutory prohibitions on disclosure and contractual remedies.



11

CONCLUSIONS AND RECOMMENDATIONS

This chapter builds on conclusions reached in earlier chapters by making recommendations for action. We will begin with a short review of the process undertaken by the Office of the Information and Privacy Commissioner (OIPC) leading up to this report.

The possible implications of the USA Patriot Act for the security of personal information of British Columbians in light of British Columbia government outsourcing initiatives have in recent months been of considerable interest and concern to the public, business and government. The Information and Privacy Commissioner's Request for Submissions, published in late May 2004, therefore initiated a short-term and open process for assessing the privacy issues raised by the USA Patriot Act.

The Information and Privacy Commissioner's objective was to elicit the views of governments, members of the public, businesses, labour organizations and other interest groups and then prepare an advisory report that would be a point of departure for further discussion and action. The number, complexity and intensity of response of submissions received in July and August 2004 was astonishing¹ and clearly demanded an examination of the matter within the larger context of globalization, privacy and national security. In keeping with the openness of the process, some 60 submissions from governments, businesses,

interest groups and academics have been posted on the OIPC website (www.oipc.bc.ca).

We studied the submissions and prepared this report over a period of ten weeks. It can only be a step on the road, not an endpoint. The British Columbia government has, since its submission to the OIPC, introduced the FOIPPA amendments² that it promised to address the USA Patriot Act. A number of our recommendations below further illustrate the ongoing nature of the dialogue of which this report is a part.

The OIPC will monitor progress in implementation of these recommendations and will report publicly on progress within 12 months of the release of this report.

Questions and Answers

We will now recall the specific questions posed in the Request for Submissions and briefly summarize our answers to them:

1. Does the USA Patriot Act permit US authorities to access personal information of British Columbians that is, through the outsourcing of public services, in the custody or under the control of US-linked private sector service providers? If it does, under what conditions can this occur?

¹ The OIPC received over 500 written responses to the Request for Submissions.

² Freedom of Information and Protection of Privacy Amendment Act, 2004, 5th Sess., 37th Parl., BC, 2004 (3rd reading 19 October 2004).



2. If it does, what are the implications for public body compliance with the personal privacy protections in the Freedom of Information and Protection of Privacy Act (FOIPPA)? What measures can be suggested to eliminate or appropriately mitigate privacy risks affecting compliance with FOIPPA?

Access to British Columbians' personal information through the USA Patriot Act

On the first question, we have concluded that, if information is located outside British Columbia, it will be subject to the law that applies where it is found, regardless of the terms of an outsourcing contract. Therefore, if an outsourcing arrangement calls for personal information to be sent to the US, that information would be subject to the USA Patriot Act while in the US. The applicability of US law would not be limited to Foreign Intelligence Surveillance Act (FISA) orders for the production of “tangible things”. It would also include provisions respecting physical search orders under FISA, national security letters³ under various US statutes, and other laws that apply to records or information in the US.

Further, we have concluded that it is a reasonable possibility that the US Foreign Intelligence Surveillance Court (FIS Court) would issue a FISA order requiring a US-located corporation to produce records held in Canada by its Canadian subsidiary or, indeed, require any person or corporation within the jurisdiction of that court to disclose records held outside the US that they control because they have the legal or practical ability to obtain the records. It has also been said by some US courts that a US-located corporation will

control a foreign corporation if the US corporation can, directly or indirectly, elect a majority of the directors of the foreign corporation. Accordingly, it would not be prudent, in our view, to ignore the fact that control, as a matter of US law, has been found on the basis of corporate relationship alone and there is a reasonable possibility that the FIS Court would take this view regardless of contractual relationships or practical arrangements between a public body, its contractor and corporations related to the contractor.

Some in the information technology industry, notably the Information Technology Association of Canada, have argued that a FISA order is not a concern because Canada and the US have similar anti-terrorism laws. As discussed in Chapters 6 and 7, we agree that the two countries have anti-terrorism laws that share many features. This would not make the application of FISA orders to personal information in British Columbia acceptable or any less invasive.

Others in the information technology industry say a FISA order is not a concern because there is a ‘vanishingly small’ risk of one ever being made in relation to bulk collections of information or information located in British Columbia. However, US courts and grand juries have over many years made orders in relation to records located in Canada or other countries. This has been a source of friction between the US and Canada and the US and other countries. There is no indication that an extra-territorial FISA order will not be sought by the FBI and issued by a FIS Court or that this has not already happened in relation to personal information in Canada.

We are inclined to the view, for the reasons described in Chapter 10, that there is a reasonable possibility of the FIS Court issuing a FISA order affecting personal information of British Columbians

³ This presupposes that provisions for the issuance of national security letters will continue to exist in US statutes. As discussed in Chapter 6, the decision of Marrero J. in *Doe and ACLU v. Ashcroft*, No. 04-CIV-2614; 2004 U.S. Dist. Lexis 19343 (S.D.N.Y. 2004) has struck down one provision authorizing the issuance of National Security Letters (18 U.S.C. § 2709, relating to electronic communication subscriber, billing and transaction records typically held by Internet service providers) on the ground that it contravenes the First Amendment of the US Constitution. The US government is appealing this decision.



located in British Columbia—a possibility that has increased as a result of the USA Patriot Act amendments to FISA. Section 215 of the USA Patriot Act removed the limits to the types of organizations that can be investigated under FISA orders. Further, ongoing concerns about terrorism increase the likelihood that, when the FIS Court applies a ‘balancing test’ in reviewing applications for FISA orders, it may give greater weight to US national security concerns than to Canadian concerns about privacy protection.

The FBI, through the US Department of Justice, and the US Department of Homeland Security⁴ responded to the Request for Submissions. However, their submissions did not directly address, much less counter, the proposition that the USA Patriot Act might, through US persons or service providers, be used to reach personal information of British Columbians that is located in British Columbia.⁵ In the absence of evidence to the contrary—which could take various forms, including unequivocal written assurances from or a formal agreement with the US government—we cannot ignore the history of US courts issuing extra-territorial orders in some circumstances and the evident present day risk with respect to FISA orders (or national security letters that can be issued directly by the FBI under various US statutes).

Implications for compliance with FOIPPA and mitigation of privacy risks

As for the second question posed in the Request for Submissions, we concluded in Chapter 9 that disclosure by a public body or a contractor for the purpose of complying with a FISA order (or a

national security letter) is unauthorized disclosure under sections 30 and 33 of FOIPPA. FOIPPA, as we discussed, requires public bodies, directly and through their contractors, to implement reasonable, but not absolute, security arrangements to protect personal information against risks, including risk of unauthorized disclosure in response to an order made under foreign law.

Some submissions to us suggested that unauthorized disclosure in response to an extra-territorial FISA order (or a national security letter) is of little concern because extensive information transfer mechanisms that are recognized by FOIPPA would make an extra-territorial foreign order unnecessary. In our view, US authorities engaged in foreign intelligence gathering would not be likely to use the Canada-US treaty for mutual legal assistance in criminal matters (MLAT) for practical and legal reasons. We also concluded that it is not clear that US authorities would have available to them, or would necessarily use, other information transfer methods—such as information sharing agreements—that are recognized in MLAT and in section 33 of FOIPPA. This raises parallel issues about government transfers of personal information about Canadians to other countries that are important and warrant rigorous study and national dialogue in their own right.

We concluded in Chapter 9 that a ban on British Columbia government outsourcing of the management of sensitive personal information would not be a practical or effective plan of action, but that other measures should be implemented at legislative, contractual and practical levels to mitigate, though probably not eliminate, the risk of unauthorized disclosure in response to a FISA order or national security letter.

⁴ Submissions of the US Department of Justice, Federal Bureau of Investigation (18 August 2004) and the US Department of Homeland Security (6 August 2004).

⁵ The Submission of the FBI, *ibid.*, alludes to the US Privacy Act prohibiting the FBI from collecting and retaining personal information except for valid law enforcement purposes “which, as a general rule, are established by guidelines issued by the Attorney General”. There is no indication that this connotes any restriction on the collection or retention of information located outside US borders and, in the preceding paragraph, the submission refers to the FBI seeking information about a Canadian citizen from a US service provider, without qualification as to the location of that information.



Recommendations

We will now make recommendations with respect to the risks we have identified and just summarized. Some of the recommendations respond directly to the questions in the Request for Submissions. We readily acknowledge that other recommendations are not directly in response to those questions. They flow from suggested answers or justifications in the submissions received in response to the Request for Submissions that, in our view, raise other serious issues about government transfers of personal information in the context of globalization.

In the case of audits of information sharing agreements, our recommendations flow from submissions that the wide extent of authorized information transfer mechanisms in FOIPPA—an important aspect of which is authority to disclose pursuant to sharing agreements—would make an extraterritorial US order unnecessary.

In the case of audits of the data mining activities of governments and government agencies in Canada, our recommendations flow from concerns that data mining is a use to which databases of personal information of Canadians could be expected to be put if they are transferred, unconditionally, into the hands of US government authorities or business organizations. Although data mining technologies are as available to Canadian governments as to their US counterparts, it became clear to us that, unlike the US, where the federal Government Accountability Office has published audit reports in this area, we really have little or no reporting or studies on the incidence of data mining by governments in Canada.

Provincial actions alone are not sufficient to address risks posed by transfers of personal information across national borders, whether as a result of FISA orders or other information sharing mechanisms. National dialogue and action are

required. Some of our recommendations in that regard are inspired by the government of British Columbia submission or by recommendations proposed by the Privacy Commissioner of Canada in her submission to us and in her office's earlier communications with the government of Canada.

Our recommendations also reflect the fact that the risk of USA Patriot Act access is not just an issue for the public sector or for this country. It is also an issue for the private sector and an issue that will have to be addressed by all jurisdictions across Canada, by other countries and at an international level.

Amendments to FOIPPA

On October 7, 2004, the serious government introduced Bill 73, the Freedom of Information and Protection of Privacy Amendment Act, 2004, in the Legislative Assembly of British Columbia.⁶ Bill 73 is in general a welcome development, insofar as we understand it is aimed at implementing the government's commitment to introduce legislative amendments to address the USA Patriot Act. We endorse the enactment of direct prohibitions and penal sanctions in FOIPPA against disclosure in response to an order by a foreign court or other foreign authority. A comment letter respecting Bill 73, including whether it adequately meets that objective, will be forthcoming from the Information and Privacy Commissioner.

Recommendation 1

The government of British Columbia should amend the Freedom of Information and Protection of Privacy Act (FOIPPA) to:

- (a) pending nation-to-nation agreement, as contemplated by Recommendation 16, prohibit personal information in the custody or under the control of a public body from being temporarily or permanently sent outside Canada for management, storage or safekeeping and**

⁶ Freedom of Information and Protection of Privacy Amendment Act, 2004, *supra* note 2.



- from being accessed outside Canada;
- (b) expressly provide that a public body may only disclose personal information in response to a subpoena, warrant, order, demand or request by a court or other authority if it is a Canadian court, or other Canadian authority, that has jurisdiction to compel the disclosure;
 - (c) impose direct responsibility on a contractor to a public body to ensure that personal information provided to the contractor by the public body, or collected or generated by the contractor on behalf of the public body, is used and disclosed only in accordance with FOIPPA;
 - (d) require a contractor to a public body to notify the public body of any subpoena, warrant, order, demand or request made by a foreign court or other foreign authority for the disclosure of personal information to which FOIPPA applies;
 - (e) require a contractor to a public body to notify the public body of any unauthorized disclosure of personal information under FOIPPA;
 - (f) ensure that the Information and Privacy Commissioner has the powers necessary to fully and effectively investigate contractors' compliance with FOIPPA and to require compliance with FOIPPA by contractors to public bodies, including powers to enter contractor premises, obtain and copy records, and order compliance; and
 - (g) make it an offence under FOIPPA for a public body or a contractor to a public body to use or disclose personal information, or send it outside Canada, in contravention of FOIPPA, punishable by a fine of up to \$1 million or a significant term of imprisonment, or both.

Provincial litigation policy

The next recommendation addresses the fact that US courts, when considering whether to require disclosure of records located outside the US, have been influenced by case-specific opposition from the foreign jurisdiction to disclosure in defiance of a law of the foreign jurisdiction. A published litigation policy

for opposition by the British Columbia government to a FISA order or national security letter in respect of personal information in British Columbia may, the US jurisprudence indicates, carry some weight with a US court as an expression of BC public policy respecting privacy of personal information in this province.⁷

Recommendation 2

The government of British Columbia should create a published litigation policy under which it would, as necessary, participate in or commence legal proceedings in Canada or abroad to resist a subpoena, warrant, order, demand or request made by a foreign court or other foreign authority for disclosure of personal information in British Columbia that is in the custody or under the control of a public body.

Acknowledging that FISA orders and national security letters are issued in secret, express statutory prohibitions against disclosure in FOIPPA, coupled with a requirement to notify the British Columbia government and meaningful penalties for breach, will create new legal and practical incentives for persons in British Columbia to refuse to comply with the foreign order and instead report it to the British Columbia government.

Further protection of personal information from FISA orders

Submissions to us from the US FBI and the US Department of Homeland Security have provided no assurance that FISA orders will not be sought from the FIS Court, or that national security letters will not be issued by the FBI, for access to personal information records in British Columbia. This assurance should be sought to complement the amendments to FOIPPA in Recommendation 1.

⁷ Doe and ACLU v. Ashcroft, *ibid.*, note 3, a lawsuit brought by the American Civil Liberties Union respecting national security letters, demonstrates that the secret nature of FISA proceedings and national security letter processes does not preclude intervention as contemplated by this recommendation.



Recommendation 3

The government of British Columbia, in conjunction with the government of Canada as appropriate and necessary, should seek assurances from relevant US government authorities that they will not seek a FISA order or issue a national security letter for access to personal information records in British Columbia.

Outsourcing contract privacy protection measures

As discussed in Chapter 9, a public body cannot, by contracting out, relieve itself of its privacy obligations under FOIPPA. This was the case before the USA Patriot Act with respect to all situations, whether or not foreign linked contractors were involved, and it continues to be the case. When a public body contracts out functions, it must ensure there are reasonable security arrangements for the personal information disclosed to the contractor and that the contractor collects or generates in fulfilling the outsourced function. The required standard of security under section 30 is a constant, with or without outsourcing.

OIPC Guideline 01-02 was issued in 2001, and updated in 2003, to assist public bodies in meeting FOIPPA privacy obligations with respect to data services contracts. The OIPC will be updating this guideline again to reflect the new FOIPPA provisions in Bill 73.

The OIPC will also be reviewing the British Columbia government's Privacy Protection Measures announced on October 5, 2004, which is a compilation of technology and business processes, employee strategies, contractual measures and corporate structure considerations for public bodies that are contemplating outsourcing to US linked contractors.

As noted earlier, the Information and Privacy Commissioner wrote in early 2002 to British Columbia government ministers to mark the need for public bodies that outsource functions to ensure they have the expert staff and other resources necessary to actively and

diligently monitor contract performance and to punish any discovered breaches. This is particularly important in relation to USA Patriot Act risks. Bearing that in mind, and also that many existing outsource contracts could be subject to USA Patriot Act risk but will not be subject to the new FOIPPA provisions in Bill 73 by virtue of its transitional provisions, we are prompted to make the following recommendations at this time:

Recommendation 4

All public bodies should ensure that they commit, for the duration of all relevant contracts, the financial and other resources necessary to actively and diligently monitor contract performance, punish any breaches and detect and defend against actual or potential disclosure of personal information to a foreign court or other foreign authority.

Recommendation 5

Recognizing that it is not enough to rely on contractors to self-report their breaches, a public body that has entered into an outsourcing contract should create and implement a program of regular, thorough compliance audits. Such audits should be performed by a third party auditor, selected by the public body, that has the necessary expertise to perform the audit and recommend any necessary changes and mitigation measures. Consideration should be given to providing that the contractor must pay for any audit that uncovers material noncompliance with the contract.

Recommendation 6

Treasury Board should direct all ministries, agencies and organizations covered by the Budget Transparency and Accountability Act to include the activities in Recommendations 4 and 5 in their annual service plans and to ensure that service plans include all financial resources necessary to perform these functions. The government of British Columbia should consider also requiring all public bodies to plan and budget for such financial resources.



Federal protection of personal information from foreign orders

In Chapter 9, we analyzed the status under FOIPPA of the disclosure of personal information in the custody or under the control of a public body, in response to an order of a foreign court or other foreign authority. Disclosure on that basis would be unauthorized under FOIPPA. We also analyzed, in Chapter 10, the role of direct statutory prohibitions against disclosure in the balancing test that might be expected to be applied by a FIS Court were it asked to issue an extraterritorial FISA order, and the importance, practically and legally, of making unauthorized disclosure under FOIPPA an offence punishable by significant deterrent penalties. The British Columbia government has now proceeded with the introduction of legislation extending FOIPPA to address the USA Patriot Act, in the form of Bill 73.

The next recommendation affirms that it is in the interest of protecting the privacy of British Columbians—whose personal information the government of Canada and its agencies collect directly or indirectly through sharing by public bodies in this province—for these issues also to be considered, and acted on where necessary, at the federal level.

Recommendation 7

The government of Canada should consider whether federal legislation protects adequately the personal information of Canadians that is in the custody or under the control of the government of Canada or its agencies (directly or through contractors) from disclosure in response to a subpoena, warrant, order demand or request made by a foreign court or other foreign authority. This should include a thorough review of the federal Privacy Act, as earlier urged by the Privacy Commissioner of Canada, with particular attention to the fact that the federal statute contains no equivalent to the reasonable security requirement in section 30 of FOIPPA.

Recommendation 8

The government of Canada should review British Columbia's Freedom of Information and Protection of Privacy Amendment Act, 2004 (Bill 73) and consider enacting provisions to protect personal information in Canada from disclosure in response to a subpoena, warrant, order, demand or request made by a foreign court or other foreign authority.

Audits of information sharing agreements and data mining activities

We received submissions that US authorities would not resort to extra-territorial FISA orders or national security letters because information sharing under treaties, agreements and arrangements is extensively authorized under FOIPPA and the federal Privacy Act. This raises important parallel issues about government transfers of personal information (issues that have also surfaced, in the context of national security, in the ongoing federal Arar Inquiry referred to in Chapter 9). The extent of information sharing by public bodies under FOIPPA has not been sufficiently or transparently studied and documented and, in our view, this needs to be remedied at the earliest practicable opportunity.

Advanced technologies have enabled the merging of databases into massive banks of information about identifiable individuals. This, in turn, enables data mining—the application of database technology and techniques to uncover patterns and relationships in data and predict future results or behaviour. When personal information is involved, the hidden patterns and subtle relationships that data mining detects are recorded and become new personal information of the individual whose characteristics or habits are being searched and analyzed. A recent audit by the US federal Government Accountability Office (referred to in Chapters 4 and 9) has studied the extent of data mining by US federal agencies. It has



confirmed that this practice is increasingly common and that many data mining efforts involve the use of personal information. The extent of data mining by governments in Canada has not been the subject of sufficient or transparent study and documentation and this too needs to be remedied at the earliest practicable opportunity.

The adequacy and appropriateness of information sharing and data mining practices at the federal level are important to British Columbians, whose personal information, as already noted, the government of Canada or its agencies collect directly or indirectly through sharing by public bodies in this province. Personal information practices in national security matters, a field in the exclusive jurisdiction of the federal government, are of particular significance in the context of this report on the implications for the privacy of British Columbians of foreign intelligence gathering under the USA Patriot Act.

We commend the Privacy Commissioner of Canada's efforts to date regarding information sharing audits (referred in Chapter 9) and support her recommendation for further work in this area. Audits and ongoing reporting and transparency in respect of information sharing agreements and arrangements and data mining activities are as necessary at the federal level as at the provincial level.

Recommendation 9

The government of British Columbia should:

- (a) undertake a comprehensive and independent audit of interprovincial, national and transnational information sharing agreements affecting all public bodies in British Columbia;
- (b) use the audit to identify and describe operational and planned information sharing activities, including in each case: the kinds of personal information involved, the purposes for which it is shared, the authority for sharing it, the public bodies or private sector organizations involved, and the conditions in place to control the use and security of the information shared;

- (c) publicly release the audit report (including timely posting on a readily accessible government of British Columbia website);
- (d) act on deficiencies or other problems indicated by the audit;
- (e) conduct and publish periodic follow-up audits and reports to ensure ongoing transparency and accountability in this area; and
- (f) require information sharing agreements entered into by all public bodies to be generally available to the public (including timely consolidated posting on a readily accessible government of British Columbia website).

Recommendation 10

The government of British Columbia should

- (a) undertake a comprehensive and independent audit of data mining efforts by all public bodies;
- (b) use the audit to identify and describe operational and planned data mining activities, including in each case: the kinds of personal information involved, the purposes of the data mining, and the authority and conditions for doing so;
- (c) ensure that the audit report also proposes an effective legislated mechanism to regulate data mining activities by public bodies and effective guidelines for the application of fair information practices to data mining by public bodies; and
- (d) publicly release the audit report (including timely posting on a readily accessible government of British Columbia website).

Recommendation 11

The government of Canada should implement Recommendations 9 and 10 at the federal level.

Section 69 of FOIPPA

In Chapter 9, we described how a disturbing number of British Columbia government ministries do not appear to be living up to the reporting requirements about information sharing agreements



found in section 69 of FOIPPA. This also needs to be corrected promptly.

Recommendation 12

The government of British Columbia should:

- (a) ensure that, within 60 days after the date of release of this report, all ministries are fully compliant with the reporting requirements of section 69 of FOIPPA;
- (b) make the section 69 reporting requirements regarding information sharing agreements applicable to all public bodies (this can be done under section 69(7) by the minister responsible for FOIPPA); and
- (c) in conjunction with Recommendations 9 and 10, review the utility of section 69 in its present form, noting our view that section 69 needs to be amended to require more complete, transparent, ongoing and effective reporting about the information sharing agreements and data mining activities of all public bodies.

Private sector issues

This report has focussed on the implications of the USA Patriot Act for the security of personal information of British Columbians in light of public body outsourcing. However, many submissions to us—including those of the British Columbia government, the Privacy Commissioner of Canada, Professor Michael Geist and Milana Homsy, and the American Civil Liberties Union—observed, and we agree, that transnational personal information transfer issues in respect of government operations are at least as significant in respect of private sector activities.

Recommendation 13

The government of British Columbia and the government of Canada should consider and address the implications of the USA Patriot Act for the security of personal information that is entrusted to private sector custody or control in British Columbia or elsewhere in Canada.

Trends in information gathering and use for state purposes

The heightened fear of terrorism provided a catalyst for increased surveillance in North America and elsewhere. The resulting trend appears to be broadened state powers for collection of information for national security purposes (including border and public transportation security), which is then in some cases disclosed for enforcement of unconnected criminal and regulatory laws. The traditional distinction between intelligence gathering for the general purpose of ensuring national security, and policing for the specific purpose of enforcing ordinary laws, is increasingly blurred.

More generous allowances are made for the collection and use of information for security purposes. A more relaxed understanding of the distinction between security and law enforcement purposes then creates risk that traditional law enforcement restraints we rely upon to protect our civil liberties will be eroded. Advancing technology for surveillance and data manipulation compounds that risk. We do not question the importance of national security, but we are concerned that in the implementation of state security initiatives, insufficient attention may be afforded to maintaining necessary distinctions for protecting civil liberties of fundamental importance.

As we noted in Chapter 7, the Attorney General of Canada has said there is no contradiction between the protection of security and the protection of human rights, which we take to include privacy rights. We agree. The task for governments is to ensure that state initiatives reflect as much concern for protection of privacy as for the efficiency of security and law enforcement measures.



Recommendation 14

The Parliamentary review of the Anti-terrorism Act provides an important opportunity for the government of Canada to renew its commitment to ensure that human rights and freedoms are not unnecessarily infringed by national security and law enforcement measures. As part of this renewed commitment, we recommend that the public be permitted to participate in the review in a meaningful way.

International trade and investment agreements

As discussed in Chapter 4, there is an increasingly complex set of rules and agreements regarding international trade of goods and services. Canada has a stake in ensuring that those rules not only promote international trade but also protect the right of all countries to make independent policy choices. Canada needs to be careful when negotiating international trade obligations that relate to or may affect the delivery of public services to ensure that privacy protections are maintained in accordance with Canadian values.

Recommendation 15

The government of Canada should, in consultation with the provincial and territorial governments, negotiate with foreign trade partners (including members of the World

Trade Organization) to ensure that trade agreements and other treaties do not impair the ability of Canadian provinces, territories and the federal government to maintain and enhance personal information protections in accordance with Canadian values.

Other international agreements

North America appears to be moving towards a continent wide customs free zone with common approaches to trade, energy, immigration and security. The privacy implications of transnational data flows must be taken into account in this process. Privacy values must be given full weight in the multilateral legal, regulatory and administrative solutions that emerge. Rigorous, well-considered privacy protections must be established and must be accompanied by effective continental oversight and accountability mechanisms.

Recommendation 16

In moving towards a North American trade, energy, immigration and security zone, the government of Canada should, in consultation with the provincial and territorial governments, advocate to the US and Mexico for comprehensive transnational data protection standards and for multilateral agreements respecting continental control and oversight of transnational information sharing for government purposes, including national security and public safety purposes.



BIBLIOGRAPHY

Canadian Statutory Material and Treaties

- Access to Information and Protection of Privacy Act, (Nunavut), R.S.N.W.T. 1994, c. 20.
- Access to Information and Protection of Privacy Act, R.S.Y. 2002, c. 1.
- Access to Information and Protection of Privacy Act, S.N.L. 2002, c. A-11.
- Access to Information and Protection of Privacy Act, S.N.W.T. 1994, c. 20.
- Aeronautics Act, R.S.C. 1985, c. A-2.
- Anti-terrorism Act, S.C. 2001, c. 41.
- Bill 73, Freedom of Information and Protection of Privacy Amendment Act, 2004, 5th Sess., 37th Parl., BC, 2004 (3rd reading 19 October 2004).
- Canada Evidence Act, R.S.C. 1985, c. C-5.
- Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23.
- Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11.
- Criminal Code, R.S.C. 1985, c. 41.
- Customs Act, R.S.C. 1985 (2d Supp.) c.1.
- Document Disposal Act, R.S.B.C. 1996, c. 99.
- Evidence Act, R.S.B.C. 1996, c. 124.
- Foreign Extraterritorial Measures Act, R.S.C. 1985, c. F-29.
- Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175.
- Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25.
- Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165.
- Freedom of Information and Protection of Privacy Act, R.S.P.E.I. 2002, c. F-15.01.
- Freedom of Information and Protection of Privacy Act, S.N.S. 1993, c. 5.
- Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. F-22.01.
- Inquiries Act, R.S.C. 1985, c. I-11.
- Mutual Legal Assistance in Criminal Matters Act, R.S.C. 1985 (4th Supp.), c. 30.
- National Defence Act, R.S.C. 1985, c. N-5.
- Personal Information Protection Act, S.B.C. 2003, c. 63.
- Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.
- Privacy Act, R.S.C. 1985, c. P-21.



Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17
Public Safety Act, 2002, S.C. 2004, c. 15.
Rules of Court, B.C. Reg. 221/90, as amended.
Security of Information Act, R.S.C. 1985, c. O-5.
Treaty between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters (18 March 1985) 1990, Can. T.S. No. 19 (in force 24 January 1990; C.Gaz. 1990.1.953).

Canadian Case Law

Application Under s. 83.28 of the Criminal Code (Re), 2004, S.C.J. No. 40, SCC 42.
Atwal v. Canada, [1988] 1 F.C. 107 (C.A.).
Bell ExpressVu Limited Partnership v. Rex, [2002] 2 S.C.R. 559.
Blencoe v. British Columbia (Human Rights Commission), [2000] 2 S.C.R. 307.
Canada (Information Commissioner) v. Canada (Immigration and Refugee Board), [1997] 4 Admin L.R. (3d) 96 (F.C.T.D.).
Canada (Information Commissioner) v. Canada (Minister of Citizenship and Immigration), [2003] 1 F.C. 219 (C.A.).
Canadian AIDS Society v. Ontario, [1995] O.J. No. 2361 (Gen. Div.); aff'd [1996] O.J. No. 4184 (C.A.); leave to appeal refused [1997] S.C.C.A. No. 33.
Germany (Federal Republic) v. Canadian Imperial Bank of Commerce, [1997] 31 O.R. (3d) 684 (Gen. Div.).
Germany (Federal Republic) v. Ebke, [2001] 159 C.C.C. (3d) 253 (N.W.T.S.C.); aff'd [2003] N.W.T.J. No. 49 (N.W.T.C.A.); leave to appeal refused [2003] S.C.C.A. No. 178.
Gulf Oil Corp. v. Gulf Canada Ltd., [1980] 2 S.C.R. 39.
Hunter v. Southam Inc., [1984] 2 S.C.R. 145.
Morguard Investments Ltd. v. De Savoye, [1990] 3 S.C.R. 1077.
Ontario (Criminal Code Review Board) v. Ontario (Information and Privacy Commissioner) (1999), 180 D.L.R. (4th) 657 (Ont. C.A.).
Purdy v. Canada (Attorney General) (2003), 230 D.L.R. (4th) 361 (B.C.C.A.).
R. v. Colarusso, [1994] 1 S.C.R. 20.
R. v. Collins, [1987] 1 S.C.R. 265.
R. v. Cook, [1998] 2 S.C.R. 597.
R. v. Dersch, [1993] 3 S.C.R. 769.
R. v. Dyment, [1988] 2 S.C.R. 417.
R. v. Evans, [1996] 1 S.C.R. 8.
R. v. Harrer, [1995] 3 S.C.R. 562.
R. v. Jarvis, [2002] 3 S.C.R. 757.
R. v. Ling, [2002] 3 S.C.R. 814.
R. v. Mills, [1999] 3 S.C.R. 668.



- R. v. O'Connor*, [1995] 4 S.C.R. 411.
R. v. Plant, [1993] 3 S.C.R. 281.
R. v. Terry, [1996] 2 S.C.R. 207.
R. v. Tessling (2003), 171 C.C.C. (3d) 361 (Ont. C.A.).
R. v. Wise, [1992] 1 S.C.R. 527.
R. v. Zingre, [1981] 2 S.C.R. 392.
Re Republic of France and De Havilland Aircraft of Canada Ltd. (1991), 65 C.C.C. (3d) 449 (Ont. C.A.).
Re Vancouver Sun, [2004] S.C.J. No. 41, 2004 SCC 43.
Re Westinghouse Electric Corp. and Duquesne Light Co. (1977), 78 D.L.R. (3d) 3 (Ont. H.C.J.).
Rodriguez v. British Columbia (Attorney General), [1993] 3 S.C.R. 519.
Ruby v. Canada (Solicitor General), [2000] 3 F.C. 589 (C.A.); varied [2002] 4 S.C.R. 519.
Schreiber v. Canada (Attorney General), [1998] 1 S.C.R. 841.
Slaight Communications Inc. v. Davidson, [1989] 1 S.C.R. 1039.
Smith v. Canada (Attorney General), [2001] 3 S.C.R. 902.
Tolofson v. Jensen, [1994] 3 S.C.R. 1022.
U.S.A. v. Orphanou, [2004] O.J. No. 622 (S.C.).
U.S.A. v. Ross, [1994] B.C.J. No. 971 (C.A.).
U.S.A. v. Ross, [1995] Q.J. No. 506 (C.A.), leave to appeal refused [1995] C.S.C.R. No. 410.
U.S.A. v. Schneider, [2002] B.C.J. No. 1561 (S.C.).

Orders of the Information and Privacy Commissioner for British Columbia

- Order 00-47, [2000] B.C.I.P.C.D. No. 51.
 Order 04-19, [2004] B.C.I.P.C.D. No. 19.

Canadian Governmental Documents and Reports

- Final Report of the Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada*, Roy J. Romanow, Commissioner, (November 2002).
 Government of Canada, *Securing an Open Society: Canada's National Security Policy*, (Privy Council Office, April 2004).
 Office of the Information and Privacy Commissioner for British Columbia, Guideline 01-01, *Guidelines for Audits of Automated Personal Information Systems*.
 Office of the Information and Privacy Commissioner for British Columbia, Investigation Report 01-01, "Investigation into BC Nurses Union Complaint about Telus-VGH LastWord Contract", (5 October 2001).
 Smith, D. and B. Barnard. "Consultations on British Columbia's Information Structure" prepared for the BC Ministry of Employment and Investment (9 November 1994).



US Statutory Material

Department of Homeland Security Appropriations Act, 2005, HR 4567, 108th Congr.
Foreign Intelligence Surveillance Act, 1978, 50 U.S.C. 1801 *et seq.*
Intelligence Authorization Act for Fiscal Year 2004, HR 2417, 108th Cong.
Personal Data Offshoring Protection Act, 2004, HR 4366, 108th Cong.
The Homeland Security Act, 2002, Pub. L. No. 107-296, 116 Stat. 2135.
USA Patriot Act, 2001, Pub. L. No. 107-56, 115 Stat. 272.
US, Rules of the Foreign Intelligence Surveillance Court.

US Case Law

Afros S/P.A. v. Krauss-Maffei Corp., 113 F.R.D. 127, 131 (D. Del. 1986).
Alcan International Ltd. v. S.A. Day Mfg. Co., Inc., 176 F.R.D. 75 (W.D.N.Y. 1996).
Asset Value Fund Ltd. v. The Care Group, Inc., U.S. Dist. LEXIS 19768 (S.D.N.Y. 1997).
Bank of New York v. Meridien Biao Bank Tanzania, 171 F.R.D. 135 (S.D.N.Y. 1977).
Compagnie Française d'Assurance Pour le Commerce Extérieur v. Phillips Petroleum Co., 105 F.R.D. 16 (S.D.N.Y. 1984).
Cooper Indus., Inc. v. British Aerospace, Inc., 102 F.R.D. 918 (S.D.N.Y. 1984).
Dietrich v. Bauer, U.S. Dist. Lexis 11729 (S.D.N.Y. 2000).
Doe and ACLU v. Ashcroft, No. 04-CIV-2614, 2004 U.S. Dist. LEXIS 19343 (S.D.N.Y. 2004).
First Am. Corp. v. Price Waterhouse LLP, 154 F.3d 16 (2d Cir. 1998).
Griswold v. Connecticut, 381 U.S. 479 (1965).
In re A Grand Jury Subpoena dated August 9, 2000, 218 F. Supp. 2d 544 (S.D.N.Y. 2002).
In re Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984).
In re Grand Jury Subpoenas duces tecum addressed to Canadian International Paper Company et al., 72 F.Supp. 1013 (S.D.N.Y. 1947).
In re Investigations of World Arrangements with Relation to the Production, Transportation, Refining and Distribution of Petroleum, 13 F.R.D. 280 (D.D.C. 1952).
In re Marc Rich & Co., A.G., 707 F.2d 663 (2nd Cir. 1983).
In re Sealed Case, 310 F.3d 717 (Foreign Intell. Surv. Ct. Rev. 2002).
In re Sealed Case, 825 F.2d 494; (D.C.C. 1987).
In re Uranium Antitrust Litigation, 480 F.Supp. 1138 (N.D. Ill. 1979).
Ings v. Ferguson, 282 F.2d 149 (2d Cir. 1960).
Katz v. United States, 389 U.S. 347 (1967).
Kyllo v. United States, 533 U.S. 27 (2001).
Lawrence v. Texas, 539 U.S. 558 (2003).
Lopez v. United States, 373 U.S. 427 (1963).
Minipeco, S.A. v. ContiCommodity Services, Inc., 116 F.R.D. 517 (S.D.N.Y. 1987).
Olmstead v. United States, 277 U.S. 438 (1928).



- Planned Parenthood of Southeastern Pa. v. Casey*, 505 U. S. 833 (1992).
SEC v. Banca Della Svizzera Italiana, 92 F.R.D. 111 (S.D.N.Y. 1981).
Société Internationale Pour Participations Industrielles Et Commerciales, S.A. v. Rogers, 357 U.S. 197 (1958).
Ssangyong Corp. v. Vida Shoes Int’l, Inc., 2004 U.S. Dist. LEXIS 9101 (S.D.N.Y. 2004).
United States v. Chase Manhattan Bank, N.A. and F.D.C. Co. Ltd., 584 F. Supp. 1080 (S.D.N.Y. 1984).
United States v. Davis, 767 F.2d 1025 (2d Cir. 1985).
United States v. First Nat’l City Bank, 396 F.2d 897 (2d Cir. 1968).
United States v. United States District Court, 407 U.S. 297 (1972).
Volkswagen, A.G. v. Valdez, 909 S.W.2d 900 (Tex. Sup. Ct. 1995).

Other Governmental Documents and Reports

- Report of the Secretary’s Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, US Secretary of Health, Education and Welfare (June, 1973).
- Bazan, Elizabeth B. “The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions” (Congressional Research Service Report for Congress, 2003).
- Council of Europe Convention for the Protection for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108 (Strasbourg: Jan 1981).
- Doyle, Charles. “The USA Patriot Act: A Legal Analysis” (Congressional Research Service Report for Congress, 2002).
- EC, European Parliament and Council Directive 95/46/EC 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, [1995] O.J.L. 281/31.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).
- Technical Analysis, Mutual Legal Assistance Treaty Between the United States and Canada, reprinted in S. Treaty Doc. 100-14, 100th Cong., 2d Sess (1988).
- UK Report of a Committee of Privy Counsellors, *Review of Intelligence on Weapons of Mass Destruction (Return to an Address of the Honourable the House of Commons)*, Chairman, the Rt Hon the Lord Butler of Brockwell (London: The Stationery Office, 14 July 2004).
- UN Conference on Trade and Development, *World Investment Report 2004: The Shift Towards Services* (United Nations: New York and Geneva, 2004).
- UN Universal Declaration of Human Rights, G.A. Res 217A(III), UNGAOR, 3d Sess. Supp. No. 13, UN Doc. A/810 (1948).
- US Department of Justice, Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (31 October 2003).
- US Department of Justice. “Report from the Field: The USA Patriot Act at Work” (July 2004).
- US Executive Order 12333—United States Intelligence Activities 46 FR 59941, 3 CFR, 1981 Comp., p. 200.
- US General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*, Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Committee on Governmental Affairs, U.S. Senate. (May 2004).



US Privacy Protection Study Commission. *Personal Privacy in an Information Society* (July 1977).

US Senate Judiciary Committee, Senators Patrick Leahy, Charles Grassley and Arlen Specter. *FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures* (Interim Report, February 2003).

Books

6, Perri. *The Future of Privacy*, vol. 1 (London: Demos, 1998).

American Law Institute. *Restatement (Third) of the Foreign Relations Law of the United States* (St. Paul, MN: American Law Institute Publishers, 1987).

Ash, Timothy Garton. *The File* (New York: Random House, 1997).

Bennett, Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992).

Bennett, Colin J. and Rebecca Grant, eds., *Vision of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999).

Bennett, Colin J. and Charles D. Raab. *The Governance of Privacy* (Aldershot: Ashgate, 2003).

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Reading, MA: Addison-Wesley, 1998).

Cavoukian, Ann and Don Tapscott. *Who Knows: Safeguarding Your Privacy in a Networked World* (Toronto: Vintage Canada, 1995).

Diffie, Whitfield and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, MA: The MIT Press, 1998).

Etzioni, Amitai. *The Limits of Privacy* (New York: Basic Books, 1999).

Flaherty, David H. *Privacy in Colonial New England* (Charlottesville: University Press of Virginia, 1967).

Flaherty, David H. *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989).

Hogg, Peter W. *Constitutional Law of Canada* (Toronto: Thomson-Carswell, 2004).

Kindred, H.M. et al., *International Law Chiefly as Interpreted and Applied in Canada*, 5th ed. (Toronto: Emond Montgomery, 1993).

Krivel, E.F., Beveridge, T. and J.W. Hayward. *A Practical Guide to Canadian Extradition* (Toronto: Carswell, 2002).

Roach, Kent. *September 11: Consequences for Canada* (Québec: McGill-Queen's University Press, 2003).

Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Vintage Books, 2001).

Sieghart, Paul. *Privacy and Computers* (London: Latimer, 1976).

Solzhenitsyn, Alexander. *Cancer Ward* (New York: Farrar, Straus & Giroux, 1969).

Sullivan, R. *Driedger on Construction of Statutes*, 3d ed. (Vancouver: Butterworths, 1994).

Sykes, Charles J. *The End of Privacy* (New York: St. Martin's Press, 1999).

Westin, Alan. *Privacy and Freedom* (New York: Atheneum, 1967).

Whitaker, Reg. *The End of Privacy: How Total Surveillance Is Becoming A Reality* (New York: New Press, 1999).



Journal Articles and Commentaries

- Brown, Christopher. "Experts Debate Uses, Privacy Concerns Raised by Vast Databases of Personal Info" (2004) 3:13 *Privacy and Security Law*.
- Cockfield, Arthur J. "The State of Privacy Laws and Privacy-encroaching Technologies after September 11: A Two-year Report Card on the Canadian Government", *University of Ottawa Law and Technology Journal* 1 (2003-2004).
- Cotler, the Hon. Irwin, Minister of Justice and Attorney-General of Canada. (Address to the Canadian Bar Association Annual Conference, Winnipeg, 16 August 2004).
- Currie, Robert J. "Peace and Public Order: "International Mutual Legal Assistance 'The Canadian Way'" [1998] 7 *Dal. J. Leg. Stud.* 91.
- Feinberg, Joe. "Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?" [1982] 58 *Notre Dame L. Rev.*
- Freedman, Bradley J. & Gregory N. Harney. "Obtaining Evidence from Canada: The Enforcement of Letters Rogatory by Canadian Courts" [1987] Vol. 21:2 *UBCL Rev.* 351.
- Goldstein, Robert & Nancy, Dennison. "Mutual Legal Assistance in Canadian Criminal Courts" [2002] 45 *Crim. L.Q.* 126.
- La Forest, the Hon. Gérard V., C.C., Q.C., retired Supreme Court of Canada Justice, Legal Opinion for the Privacy Commissioner of Canada (12 November 2002).
- Loukidelis, David, Information and Privacy Commissioner for British Columbia "Alternative Service Delivery—Privacy Issues" (Letter to all Ministers, 21 January 2002).
- Loukidelis, David, Information and Privacy Commissioner for British Columbia. "Identity, Privacy & Security—Can Technology Really Reconcile Them?" (Speech, Victoria, British Columbia, February 2004).
- Rankin, M.T. "The Supreme Court of Canada and the International Uranium Cartel: Gulf Oil and Canadian Sovereignty" [1980] 2 *Sup. Ct. L. Rev.* 410.
- Regan, Priscilla. "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics" in Colin Bennett and Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999).
- Schulhofer, Stephen J. "No Checks, No Balances: Discarding Bedrock Constitutional Principles" in Richard C. Leone and Greg Anrig, Jr., eds., *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* (New York: PublicAffairs, 2003).
- Stanley, Jay. "The Surveillance-Industrial Complex: How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society" (New York: American Civil Liberties Union, 2004).
- Tassé, Roger, O.C., Q.C., Legal Opinion for the Privacy Commissioner of Canada (21 November 2002).

Magazine and News Articles

- Baron, Madeleine. "Welcome to the Matrix: Inside the Government's Secret, Corporate-run Mega-database" *The*



New Standard (9 July 2004).

- Berrington, Craig. "Privacy, Insurance and the Transparent Society" *Privacy in Focus* (February 2001).
- Boo, Katherine. "The Best Job in Town: The Americanization of Chennai" *The New Yorker* (5 July 2004).
- Bridge, Maurice. "Police Want More Access to Your E-mail" *Vancouver Sun* (24 August 2004) A03.
- Bridge, Maurice. "World Is Less Safe Now, Says RCMP's Top Boss" *The Vancouver Sun* (26 August 2004) A05.
- Canadian Press, "Census Deal with U.S. Firm Goes Through" *The Globe and Mail* (9 October 2004).
- Chester, Simon. "Outsourcing Threat to Privacy Overblown" *Financial Post* (16 August 2004).
- Clark, Drew. "Senate Votes for Privacy Study on Agencies' Data-mining Use" *National Journal's Technology Daily* (16 September 2004).
- Clarke, Roger. "The Digital Persona and Its Application to Data Surveillance" *The Information Society* 10:2 (June 1994).
- Cole, David. "Scalia's Kind of Privacy" *The Nation* (12 July 2001).
- Janzen, Leah. "Florida Firm Hawking Stolen St. B. Net Drug List" *Winnipeg Free Press* (5 August 2004).
- Kehaulani Goo, Sara. "No Fly List's 'T. Kennedy' irks senator" *The Washington Post* (20 August 2004).
- McGregor, Glen. "Biometric Passports Approved" *Victoria Times-Colonist* (6 October 2004) A-1.
- McKenna, Barrie. "Offshoring of Jobs Big Benefit for Canada" *The Globe and Mail* (23 September 2004).
- Morgan, Dan and Babington, Charles. "Push by GOP Ends Attempt to Scale Back Patriot Act" *The Seattle Times* (9 July 2004).
- Recalde, Maria. "Seeking Safe Harbor from European Union Privacy Laws" *New England In-House, Lawyers Weekly USA* (July 2003).
- Sallot, Jeff. "Mounties Bungled Arar File" *The Globe and Mail* (25 September 2004) A-1, A-4.
- Schechter, Barbara. "Visa Accounts Open to U.S. Law Enforcement Agencies, CIBC Warns" *The National Post* (24 September 2004).
- Taber, Jane. "Ottawa Compiles 'No-fly' List of Banned Passengers" *The Globe and Mail* (3 September 2004) A-1.
- Ticol, David. "U.S. Patriot Act's Reach Is a Concern for Canadians" *The Globe and Mail* (14 October 2004) B13.
- "U.S. Patriot Act Used in Pot Case" *CBC News, British Columbia News Online* (5 August 2004).

Other

- Canadian Bar Association Resolution 04-05-A, "Privacy Rights in Canada" (August 2004).
- Canadian Bar Association Resolution 04-06-A, "Limiting State Access to Private Information" (August 2004).
- Canadian Imperial Bank of Commerce Notice, "Changes to the CIBC VISA Cardholder Agreement" (September 2004).
- Public Policy Forum and ITAC Roundtable, "IT Offshore Outsourcing Practices in Canada," (Ottawa, 20 May 2004).



APPENDIX

List of Submissions from Organizations

The following submissions will remain posted on the Information and Privacy Commission website at www.oipc.bc.ca until October 2005. In addition to these, we received about 450 submissions from individuals.

- American Civil Liberties Union, (10 Aug 2004), 14 pages.
- BC Association of Pregnancy Outreach Programs, "Submission on the USA Patriot Act", (7 Aug 2004), 2 pages.
- BC Citizens for Public Power, "Submission on the USA Patriot Act", (Aug 2004), 9 pages.
- BC Federation of Labour, "Examination of the *USA Patriot Act* Implications for Personal Information of BC Residents", (20 July 2004), 30 pages.
- BC Federation of Retired Union Members, "Submission on the USA Patriot Act", (9 July 2004), 1 page.
- BC Ferry and Marine Workers' Union, "Right to Privacy", (5 Aug 2004), 3 pages.
- BC Freedom of Information and Privacy Association & BC Coalition of People with Disabilities, "Is Government Outsourcing a Threat to Privacy?", (6 Aug 2004), 19 pages.
- BC Government and Service Employees' Union – Part 1, "Submission on the USA Patriot Act", (6 Aug 2004), 42 pages.
- BC Government and Service Employees' Union – Part 2, "Submission on the USA Patriot Act", (6 Aug 2004), 50 pages.
- BC Health Coalition, "Outsourcing MSP and Pharmacare and the Impact on British Columbians' Privacy Rights", (6 Aug 2004), 5 pages.
- BC Hydro, "Examination of USA Patriot Act Implications for Personal Information of British Columbia Residents Involved in Outsourcing of Government Services to US-linked Service Providers", (6 Aug 2004), 2 pages.
- BC Library Association, "Submission on the USA Patriot Act and its Impact on the Privacy of BC Citizens' Personal Information in the Context of Government Outsourcing of Data Administration", (6 Aug 2004), 24 pages.
- BC Medical Association, (12 July 2004), 3 pages.
- BC Nurses' Union, "Submission to the Information and Privacy Commissioner for British Columbia regarding the *USA Patriot Act*", (6 Aug 2004), 10 pages.
- BC Persons with AIDS Society, "Submission on the USA Patriot Act", (14 July 2004), 18 pages.
- Bearing Point Inc., "Assessing USA Patriot Act Implications", (6 Aug 2004), 3 pages.



- British Columbia Civil Liberties Association, "Implications of the USA Patriot Act on Government Outsourcing", (6 Aug 2004), 10 pages.
- Canadian Advanced Technology *Alliance*, (6 Aug 2004), 2 pages.
- Canadian Internet Policy and Public Interest Clinic, "Submission on the *USA Patriot Act* and its Impact on the Privacy of BC Citizens' Personal Information in the Context of Government Outsourcing of Data Administration", (2 Aug 2004), 27 pages.
- Canadian Union of Public Employees, BC Division, "Addendum to the Submission on the USA Patriot Act", (6 Aug 2004), 1 page.
- Canadian Union of Public Employees, BC Division, "Submission on the USA Patriot Act", (4 Aug 2004), 22 pages.
- Canadian Vehicle Manufacturers' Association, "Submission on the USA Patriot Act", (6 Aug 2004), 2 pages.
- Carpenters Union Local 1995, (3 Aug 2004), 1 page.
- Comox Valley Chapter Council of Canadians, "Submission to the Privacy Commissioner from the Comox Valley Chapter Council of Canadians", (1 Aug 2004), 1 page.
- Council of Canadians, "A Submission on the USA Patriot Act to the Information and Privacy Commissioner for British Columbia", (6 Aug 2004), 6 pages.
- Council of Senior Citizens' Organizations of BC, (4 Aug 2004), 2 pages.
- Credit Union Central BC, "Submission on the USA Patriot Act", (22 July 2004), 2 pages.
- Dutch Data Protection Authority, "Examination of USA Patriot Act Implications", (9 Aug 2004), 2 pages.
- EDS Canada Inc., "USA Patriot Act Implications for Privacy Compliance under British Columbia's *Freedom of Information and Protection of Privacy Act*", (19 July 2004), 46 pages.
- Fasken Martineau DuMoulin LLP, "Submission on the USA Patriot Act", (5 Aug 2004), 40 pages.
- Federal Bureau of Investigation, "Implications of USA Patriot Act on Information Pertaining to British Columbia Residents", (18 Aug 2004), 3 pages.
- Fraser Valley / White Rock Chapter CARP, "Submission on the USA Patriot Act", (5 Aug 2004), 6 pages.
- Green Party of BC, "Submission on the USA Patriot Act", (6 Aug 2004), 1 page.
- Information and Privacy Commissioner for PEI, "Submission on the USA Patriot Act", (5 Aug 2004), 5 pages.
- Information Technology Association of Canada, "Submissions of the Information Technology Association of Canada Regarding the *USA Patriot Act*", (5 Aug 2004), 65 pages.
- INTRIA Items Inc., "Submission on the USA Patriot Act", (6 Aug 2004), 2 pages.
- MAXIMUS, "MAXIMUS Response to Request for Submissions Assessing USA Patriot Act Implications for Privacy Compliance", (23 July 2004), 32 pages.
- Microsoft Canada Co., "Submission on USA Patriot Act", (5 Aug 2004), 2 pages.
- MYRA Systems Corp., "MYRA Systems Submission on the USA Patriot Act", (6 Aug 2004), 8 pages.
- New Brunswick Ombudsman, (4 Aug 2004), 3 pages.
- Office of the Privacy Commissioner of Canada, "Transferring Personal Information about Canadians Across Borders", (16 Aug 2004), 15 pages.
- Party of Citizens, "The Patriot Act in a Psychopolitical Context", (31 July 2004), 3 pages.
- Privacy International, "Response to British Columbia Information and Privacy Commissioner", (Aug 2004), 7 pages.



- Prof. Michael Geist & Milana Homs, LL.B., “The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy?” (26 July 2004), 34 pages.
- Prof. Reg Whitaker, “Implications of *USA Patriot Act* for Outsourcing of Public Services to US-linked Service Providers”, (5 Aug 2004), 7 pages.
- Professional Employees Association, “Submission on the USA Patriot Act”, (16 July 2004), 2 pages.
- Province of British Columbia, “Examination of USA Patriot Act Implications for Personal Information of British Columbia Residents Involved in Outsourcing of Government Services to US-Linked Services Providers”, (23 July 2004), 102 pages.
- Province of British Columbia (further submission), “Examination of the USA PATRIOT ACT Implications for Personal Information of British Columbia Residents Involved in Outsourcing of Government Services to US-linked Service Providers”, (9 Sep 2004), 6 pages.
- Public Services International, “Submission on the USA Patriot Act”, (14 July 2004), 2 pages.
- REACH Community Health Care, “Submission on the USA PATRIOT Act”, (6 Aug 2004), 2 pages.
- Retail Council of Canada, Canadian Chamber of Commerce and BC Chamber of Commerce, “Submission on the USA Patriot Act”, (5 Aug 2004), 4 pages.
- Seniors Network of BC, “Submission on the USA Patriot Act”, (6 July 2004), 1 page.
- Tenough Coalition, “Assessing *USA Patriot Act* Implications for Privacy Compliance”, (6 Aug 2004), 12 pages.
- The British Columbia Public Interest Advocacy Group, “Assessing ‘USA Patriot Act’ Implications for Privacy Compliance under British Columbia’s *Freedom of Information and Protection of Privacy Act*”, (June 2004), 6 pages.
- US Department of Homeland Securities, “(6 Aug 2004), 3 pages.
- Vancouver Coastal Health Authority & Providence Health Care, “Submission on the USA Patriot Act”, (6 Aug 2004), 11 pages.
- Vancouver Public Library, “Examination of the *USA Patriot Act* Implications for Personal Information of British Columbia Residents Involved in Outsourcing of Government Services to US-linked Service Providers”, (6 Aug 2004), 6 pages.
- Vancouver Women’s Health Collective, (6 Aug 2004), 1 page.
- Women Elders in Action, “A Submission to the Privacy Commissioner From Senior Women in BC”, (28 July 2004), 4 pages.