703 The Extra-Jurisdictional Reach of the US Patriot Act & Its Effect on Cross-Border Transactions

Michel E. Belec
Associate General Counsel
Telus Communications Inc.

Frank Giblon
Legal Consultant
Sun Microsystems, Inc.

Micheal Tolfree
Manager, Information and Privacy
Calgary Health Region

Garry B. Watzke
Senior Vice President, General Counsel
Iron Mountain, Incorporated

Faculty Biographies

Michel E. Belec

Michel E. Belec is associate general counsel to TELUS responsible for legal services to all of TELUS' customer facing groups. He leads a team of lawyers responsible for various outsourcing and multi-service transactions with national and public sector clients. His primary areas of practice include corporate commercial law, telecommunications, and intellectual property law, joint ventures as well as bankruptcy and insolvency matters.

Prior to joining TELUS, Mr. Belec was counsel to Rogers Communications, a diversified Canadian communications and media company, where he provided support on a wide range of corporate, commercial, and municipal relations matters. Mr. Belec commenced the practice of law at Fasken Martineau, a leading national business and litigation law firm in Canada.

Mr. Belec obtained his B.A. from Simon Fraser University and his L.L.B. from Osgoode Hall Law School. Mr. Belec completed executive training with the University of British Columbia and the University of Western Ontario.

Frank Giblon

Frank Giblon is a legal consultant for Sun Microsystems, Inc. in Thornhill, Ontario.

He was called to the Ontario Bar for specializing in the areas of information technology, telecommunications contracts, and related intellectual property matters, he also has extensive contracts administration and dispute resolution experience, both domestically and internationally.

Mr. Giblon is a member of the board of directors of the Canadian Corporate Counsel Association and the Toronto CCCA chapter executive.

He obtained his LL.B. from Osgoode Hall Law School and his M.B.A. from York University.

Garry B. Watzke
Senior Vice President, General Counsel
Iron Mountain, Incorporated

The Extraterritorial Implications of the USA PATRIOT Act for Canadian Corporations

Frank G. Giblon, Legal Consultant

Introduction

It comes as no surprise in this post 9/11, post-Bali, post-Madrid, post-London era in which we live that, increasingly, security trumps privacy and other less visceral concerns. With every new terrorist attack, or failed plot, the public, particularly in the United States, becomes more inured to the erosion of civil liberties and other niceties.[1] Of course, it doesn't help that the terrorists themselves don't play by the same rules that govern 'civilized' nations.

It is against this backdrop that the U.S. government enacted, and recently extended, the USA PATRIOT Act, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (herein the "Patriot Act")[2]. This paper will address the implications of this legislation for Canadian companies and their information security practices.

Keeping Information Private in an Interconnected World

Even as our nations struggle to keep up with the proliferation of threats to national security and personal safety, our companies and agencies struggle to protect the sensitive personal information they collect in the course of their operations. With the Patriot Act and other legislation[3], corporate counsel need to be cognizant of the risk that sensitive information may be accessed or intercepted by U.S. and Canadian governmental agencies, with or without notice, and provide guidance to their clients on how to mitigate that risk.

As the North American economy becomes increasingly integrated, so too do our companies through cross-border outsourcing, subcontracting, and other commercial transactions. Arguably, although our citizens and customers are aware of the big picture, they are nevertheless queasy about the thought that their personal privacy is being

[1] Only this past week (August 10, 2006), with the revelations concerning the alleged plot in the U.K. to blow up several airplanes over the Atlantic, the public has stoically accepted new limitations on what may be brought onboard a commercial aircraft. The new normal now includes a ban on shampoo. As Canadian songwriter Bruce Cockburn wryly observed, "The trouble with normal is it always gets worse." Bruce Cockburn, "The Trouble With Normal", True North Records, 1983.
[2] Pub. L. No. 107-56, 115 Stat 272 (2001). Enacted on October 26, 2001.
[3] The Canadian federal Personal Information Protection and Electronic Documents Act contains provisions authorizing access to information by Canadian authorities similar to those in the Patriot Act.

compromised on a daily, if not transactional, basis, with every phone call, email, or purchase potentially under surveillance.[4] It is therefore incumbent on those who gather and process information to ensure that sensitive personal information is protected to the maximum extent possible through appropriate means.

For Canadian companies, that means finding the right balance between the need to conduct business, including outsourcing downstream activities in order to remain competitive, and the need to comply with applicable federal and provincial privacy laws, not to mention customer expectations of privacy. What follows is intended to help counsel analyze the particular facts confronting his or her company or agency in this context.

Analyzing the Proposed Outsourcing, Subcontract or Other Transaction

The first step in the analysis is to determine what information is being collected, processed, stored and potentially outsourced or subcontracted to another company, organization or individual service provider (the "outsourcer"). Consider whether all of the information needs to be transmitted to the outsourcer, and whether it is appropriate to employ encryption or other technical means to protect especially sensitive information[5]. This also means that the CIO or other responsible executive needs to ensure that appropriate identity management software and other similar protective measures are in place to permit only specific authorized individuals to access sensitive information, and only for specific purposes, at every step of the supply chain, whether internal or external. This will also provide an information security audit trail which can help identify and correct vulnerabilities, as well as bolster the company's or agency's due diligence defense should there be an unauthorized disclosure.

Next, consider which data elements contain the most sensitive information, likely those relating to personally identifiable health records, financial transactions etc. It may be possible to accomplish the company's business purpose without necessarily disclosing or making available to the outsourcer, all of the sensitive information contained in the business records. Should, however, it be necessary to transmit all of the information to the outsourcer, and should the outsourcer be a U.S. corporation, or a subsidiary thereof operating in Canada or elsewhere, counsel should focus on ensuring that appropriate physical and contractual safeguards are included in the outsourcing contract, subcontract or other agreement. Of course, the information may still be accessed or intercepted, but the Canadian company will be in a position to demonstrate that it took all appropriate measures within its control to minimize that possibility.

[4] It was an attempt to purchase a large quantity of fertilizer, allegedly for bomb-making purposes, which led to the recent arrests in Toronto.

[5] It is probably prudent to assume that such techniques as encryption will not prevent access or interception by governmental agencies. Nevertheless, using such techniques should minimize the chance of casual interception by the curious or devious.

Protective Measures Checklist

1. What information is being outsourced? Does it include sensitive personally identifiable information?
2. Does all of the information need to be transmitted to the outsourcer? Can the information be processed on an anonymous basis and then matched internally with the personal identifiers?
3. What technical protective measures have been taken, e.g. data encryption, identity management etc.? Have these measures been extended to the entire business process supply chain?
4. Does the outsourcing contract contain appropriate physical and contractual safeguards?
5. Are other safeguards warranted? For example, the establishment of a separate Canadian entity whose shares are held in trust as in the BC Union[6] case.

Conclusion

The Patriot Act authorizes access to and interception of information in order to fight terrorism. Corporate counsel should use this opportunity to educate themselves on the details of their company or agency's supply chain, and information security practices, to minimize the risk of disclosure of their customers' or citizens' sensitive personally identifiable information and the attendant consequences.

[6] BC Govt. Serv. Empl. Union v. British Columbia (Minister of Health Services), 2005 BCSC 446 [BC Union]. In that case, the BC government contractually required that a trust be created to hold the shares of the BC subsidiary performing the outsourcing services. In the event of a threatened disclosure, ownership of the shares would transfer to the province. The outsourcing contract contained other contractual protections, including a requirement for employee training on the outsourcer's privacy and data handling obligations.

The USA Patriot Act
Pub.L.No. 107-56, 115 Stat. 272

Introduction.

Under Section 1861 of the Foreign Intelligence Surveillance Act (50 USC 1861), as amended by the USA Patriot Act, the FBI may apply for a court order requiring from any type of business the production "of any tangible things (including books, records, papers, documents and other items)" for an investigation to obtain foreign intelligence information or to protect against international terrorism. The FBI's application need assert only that the order is sought for an investigation to obtain foreign intelligence information or to protect against international terrorism or spying, so long as if an investigation relates to a United States person, it is not based solely on protected First Amendment activity. The authority granted in Section 1861 has raised concerns among foreign businesses, governments and citizens regarding the ability of the United States government to access information regarding foreign persons or entities. This paper explores briefly the history of the USA Patriot Act and summarizes its principal provisions that touch on this subject.

1. A Brief History. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the "USA Patriot Act" or the "Act") was passed by the House on October 24 (vote of 357-66), passed the Senate on October 25 (vote of 98-1) and signed into law on October 26, 2001, about six weeks after the September 11 attacks. Consideration of the Act was obviously rushed compared to the pace at which most legislation moves through Congress, especially given the fact that Congress' ability to focus during this period was disrupted by threats of anthrax contamination in congressional offices. However, the Act did not spring full-blown from the Administration's mind after September 11; after adopting two antiterrorist statutes in 1996, Congressional committees considered additional legislation toward the end of the nineties, and three blue-ribbon committees issued recommendations after concluding that the United States was poorly prepared for a terrorist attack. Concerns expressed by civil liberties groups effectively prevented adoption of new legislation until September 11, but concepts that were the subject of legislative debate in the years prior to the attacks were incorporated into the Anti-terrorism Act presented to Congress by Attorney General John Ashcroft on September 19. Despite the push to adopt legislation, civil liberties interests were able to modify the Administration's proposals in various ways, including a sunset provision requiring that many features of the Act be revisited before December 31, 2005.

2. Principal Features of the USA Patriot Act. The Act sought to correct a number of the problems that became painfully apparent in the aftermath of the September 11 attacks. The Act amended, among others, the Right to Financial Privacy Act, the Bank Secrecy Act, and the Fair Credit Reporting Act, as well as the Foreign Intelligence Surveillance Act. The following are the Act's principal features:

(a) The Act eliminated legal barriers to information sharing between law enforcement and intelligence agencies that previously existed:

  (i) it amended a grand jury secrecy rule to permit grand jury information to be disclosed to federal officials without a court order;
  (ii) it permitted sharing of law enforcement and intelligence information among law enforcement, intelligence, protective, immigration, national defense and national security officials.

(b) The Act authorized espionage warrants to investigate terrorism:

  (i) warrants in federal criminal investigations are obtained by the FBI under Title III of the Omnibus Crime Control Act of 1968, but warrants in national security investigations are obtained under the Foreign Intelligence Surveillance Act of 1978 ("FISA").

  (ii) prior to the Act, the FISA warrant provision provided that warrants for electronic surveillance could be issued if the government could show "probable cause" that the primary purpose of the surveillance was intelligence gathering, and that the target of the warrant was a foreign power or an agent of a foreign power (including terrorist groups);

  (iii) Section 215 of the Act changed the requirement for FISA warrants so that the requirement became only to show that foreign intelligence gathering is a "significant purpose" of the activity.

  (iv) under the Act, the government is not required to reveal the warrant to the target upon completion;

(c) The Act authorized government monitoring of addressing information in e-mails:

  (i) the Act authorized pen registers, trap and trace devices and roving wiretaps, and modified traditional definitions of pen registers and trap and trace devices to include devices that track dialing, routing, addressing or signaling information, thus permitting tracking of internet usage (although not message content)

(d) the Act created new anti-money laundering provisions, allowing for asset seizure:

  (i) the Act required banks and financial institutions to monitor account activity and report suspicious transactions;

(ii) the Act permitted the Treasury Department to share reports with intelligence agencies, and authorized sharing of surveillance information between law enforcement and intelligence agencies;

(iii) the Act allowed government access to credit records without notifying the target.

(e) the Act granted authority to the Attorney General to detain non-citizens suspected of terrorism.

(i) the Act authorized detention of non-citizens for up to seven days, after which the government must bring immigration or criminal charges (the Administration had asked for rights of indefinite detention of non-citizens);

(ii) under the Act, the Attorney General can detain indefinitely not only those convicted of crimes or immigration offenses (as was possible prior to the Act), but also any non-citizen the Attorney General has reasonable grounds to believe is a terrorist or is engaged in any other activity that endangers the national security of the U.S. The Attorney General's decisions are reviewable only through habeas corpus proceedings.

3. Section 215 of the Act. Section 215 of the USA Patriot Act modified provisions of existing law related to the court established under FISA (the "FISA Court"), to make FISA warrants easier to obtain, and to make FISA warrants more broadly applicable.

Prior to the adoption of the Act, the FBI was authorized under FISA to apply for ex parte orders from the FISA court to obtain records from four categories of businesses: (i) common carriers, (ii) public accommodation facilities, (iii) physical storage facilities, and (iv) car rental agencies. In its applications, the FBI had to show that (i) the records sought were relevant to an investigation to gather foreign intelligence information or concerned international terrorism, and (ii) there were specific and articulable facts leading the FBI to believe the person to whom the record pertained was foreign power or an agent of a foreign power.

The Act relaxed the requirements for obtaining FISA warrants in two ways. First, the Act eliminated the limitation of FISA warrants to the four categories of entities; now FISA orders can be used to obtain access to any records or tangible things, provided the items are for an investigation to protect against international terrorism or clandestine intelligence activities (and if the target is a U.S. person, the investigation is not conducted solely upon the basis of First Amendment-protected activities). Secondly, the Act eliminated the requirement that the records relate to a foreign power or an agent thereof, so that now the FBI can obtain records of associates of such targets when those records are relevant to an investigation to protect against international terrorism or clandestine intelligence activities, or to obtain foreign intelligence information about non-U.S. persons. In addition, the Act eliminated the specific and articulable acts requirement. Now, FISA court orders are available if they are sought for an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that if an investigation relates to a U.S. person, the investigation of the U.S. person must not be based solely on protected First Amendment activity.

A person who has received a FISA-approved order seeking tangible things for an investigation may not disclose to any other person (other than those persons necessary to produce the tangible things) that the FBI has sought to obtain the tangible things. However, authorities apparently agree that the recipient of a FISA order can bring a motion to quash in the FISA court.

4. Perspective. It is important to note that the Patriot Act generally did not give the federal government any new subpoena powers; rather, it modified procedures to be followed by agencies such as the FBI in obtaining orders to produce things. Federal grand juries investigating crime always have had the authority to subpoena all types of records from all types of businesses and persons. With respect to the government's ability to obtain business records, in some respects the Patriot Act imposes more restrictions on subpoena powers than a federal grand jury subpoena for the same records.