Private Data in Public Hands

Fred H. Cate[1]

11th Annual Privacy & Security Conference
Victoria, British Columbia
February 9, 2010

1. Provincial Canadian Restrictions

In October 2004, the Information and Privacy Commissioner of British Columbia issued a report, *Privacy and the USA PATRIOT Act: Implications for British Columbia Public Sector Outsourcing,*[2] which concluded that there is a "reasonable possibility" that the U.S. government would use Section 215 of the USA PATRIOT Act[3] to obtain access to personal health data about British Columbia residents if those data were outsourced to "US-linked" companies in Canada.[4] The report therefore recommended that the provincial legislature:

- "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";

- "prohibit personal information in the custody or under the control of a public body from being . . . accessed outside Canada";

- "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" about British Columbians, even if doing so violates the national law to which the contractor is subject; and

- "make it an offense under FOIPPA [the British Columbia Freedom of Information and Protection of Privacy Act] 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"—even if in response to "a subpoena, warrant, order, demand, or request by a court or other authority," unless "it is a Canadian court, or other Canadian authority"—" punishable by a fine of up to $1 million or a significant term of imprisonment, or both."[5]

The British Columbia Legislative Assembly anticipated these recommendations by adopting Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004—which substantially

[1] Fred H. Cate is a Distinguished Professor, C. Ben Dutton Professor of Law, and director of the Center for Applied Cybersecurity Research at Indiana University, and a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP.

[2] Information and Privacy Commissioner of British Columbia, *Privacy and the USA PATRIOT Act: Implications for British Columbia Public Sector Outsourcing* (Oct. 2004).

[3] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections in numerous titles of U.S.C.).

[4] *Privacy and the USA PATRIOT Act*, supra at 18.

[5] Id. at 134-135.

enacted them into law even before the Commissioner's report was published.[6] Nova Scotia followed suit with its Personal Information International Disclosure Protection Act on July 13, 2006, which includes similar prohibitions.[7]

I and others have argued that these restrictions are ill-conceived, ill-focused, ineffective, and dangerous for Canadians.[8] Ironically, section 215 is almost never used—in fact, had never been used by the time these laws were adopted.

But while focused on the wrong cause and imposing what I believe is an unworkable solution, these laws do focus our attention on a critical issue—the extent to which governments obtain personal data about individuals from the private sector.

So I would like to briefly outline the government's expansive power to compel the private sector to disclose personal data and why it matters. While I intend to focus on the United States, in part because it was the United States that provoked the provincial Canadian laws, and in part because I know something about U.S. law, the issues I want to raise are by no means limited to the United States. In fact, data protection officials around the world are increasingly reporting that the greatest threat to individual privacy they encounter is not the private sector, but the government.

2. Government Access to Data

a. Routine Collection

Almost all of the statutes authorizing the government to engage in any activity include some authorization to collect data necessary to conduct that activity. So, for example, the government collects personal data to administer social service programs such as Social Security, Medicare, and workers' compensation insurance; administer tax programs and collect revenue; issue licenses for many personal, business, and professional activities; support hundreds of regulatory regimes ranging from voter registration and political campaign contributor disclosures to employee identity verification; maintain vital records about major lifecycle events, including birth, marriage, divorce, adoption, and death; operate facilities such as toll roads and national parks; conduct the census; as well as engage in law enforcement and protect national and homeland security. It is no exaggeration to say that "[i]nformation is the lifeblood of regulatory policy. . . . Regulators depend on information for nearly everything they do."[9]

Increasingly, that information is obtained not only from individuals directly, but from private-sector entities that either happen to hold the data or, more commonly, that are required by law to collect the data so that the government can access it.[10]

---

[6] Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004.

[7] Bill No. 19—the Nova Scotia Personal Information International Disclosure Protection Act, 2006.

[8] See Fred H. Cate, *Provincial Canadian Geographic Restrictions on Personal Data in the Public Sector*, submitted to the Trilateral Committee on Transborder Data Flows, Centre for Information Policy Leadership (2008); *Legal Restrictions on Transborder Data Flows to Prevent Government Access to Personal Data: Lessons from British Columbia,* Centre for Information Policy Leadership (2005).

[9] Cary Coglianese, Richard Zeckhauser & Edward Parson, "Seeking Truth for Power: Informational Strategy and Regulatory Policymaking," 89 *Minnesota Law Review* 277, 285 (2004).

[10] See Fred H. Cate, "Government Data Mining: The Need for a Legal Framework," 43 *Harvard Civil Rights-Civil Liberties Law Review* 436 (2008).

Let me give just two examples from the U.S. experience.

i. Employee Data

The first is data about employees. Under the new E-Verify employment verification program, within three days of each new employee's hiring date U.S. employers must enter basic identification information—including SSN and name, date of birth, citizen status claimed by employee, and other data—into an automated government database.[11] The database attempts to match the data against the Social Security Administration's database or, for noncitizens, Department of Homeland Security databases.[12]

Employers are also required to report to their "State Directory of New Hires" the name, address, and SSN of all new hires within twenty days of their hiring date, and then to withhold from their paychecks any child support payments they may owe.[13] These state databases then feed the federal New Hires Directory. Congress also has mandated the creation of the Federal Parent Locator Service ("FPLS").[14]

ii. Financial Data

The second example I would highlight is data about financial transactions. The ironically named Bank Secrecy Act requires banks to maintain a copy of every customer check and deposit for six years or longer.[15]

The Bank Secrecy Act was amended in 2001 by the USA PATRIOT Act" to require financial institutions and a wide range of other businesses to report to the government on certain transactions that are "determined to have a high degree of usefulness in criminal, tax, regulatory, intelligence, and counter-terrorism matters."[16] The nation's 24,000 banks and credit unions, as well as broker-dealers and commodity traders, must file Suspicious Activity Reports ("SARs") concerning suspicious financial transactions. Currency Transaction Reports ("CTRs") for cash or coin transactions of $10,000 or more must be filed by financial institutions, the Post Office, casinos, travel agencies, pawnbrokers, real estate agents, automobile and boat retailers, jewelers, and anyone who accepts a check, travelers' check, or money order.[17] The reports are received by the IRS and by the Treasury's Financial Crimes Enforcement Network ("FinCEN").

---

[11] See U.S. Citizenship and Immigration Services, Dep't of Homeland Security, *I Am an Employer . . . How Do I . . . Use E-Verify?*, M-655 (2007), available at http://www.uscis. gov/files/nativedocuments/E4_english.pdf.

[12] See *Employment Eligibility Verification Systems*: Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways and Means, 110th Cong. (2007) 5 (testimony of Richard M. Stana, Director, Homeland Security and Justice Issues, Gen. Accountability Office), http://www.gao.gov/new.items/d07924t.pdf.

[13] Personal Responsibility and Work Opportunity Reconciliation Act of 1996, 42 U.S.C. § 653a (2000).

[14] 42 U.S.C.A. § 653 (West 2007).

[15] 12 U.S.C. §§ 1829b(d), 1829b(g) (2000); see United States v. Miller, 425 U.S. 435, 436 (1976); Cal. Bankers Ass'n v. Shulz, 416 U.S. 21 (1974).

[16] Dep't of the Treasury, *A Report to Congress in Accordance with § 357 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, at 4 (2002).

[17] See id. at 6; See also 31 U.S.C. § 5312(a)(2).

FinCEN has collected and stored more than 75 million reports over the past decade.[18] State and local law enforcement "in every state" as well as federal law enforcement officials have online access to this information.[19]

The USA PATRIOT Act also mandates new rules requiring all financial institutions to: (1) verify the identity of any person seeking to open an account; (2) maintain records of the information used to verify the person's identity (e.g., a driver's license or passport); and (3) provide the information to the government for matching with terrorist watch lists.[20]

There are obviously many other examples of the private-sector being required by law to be the hand-maiden of the government in procuring and sharing personal data. But because of time, I must move on to highlight a second point about the government's access to private-sector data—its extraordinary power to compel the disclosure of sensitive personal information even where there is no specific regulatory requirement.

b. Exceptional Authority

i. National Security Letters

As I have already mentioned, Section 215 of the USA PATRIOT Act, which motivated Canadian provincial action, has proved not to be a good example of the government's power to compel disclosure of specific records. National Security Letters are far more compelling. Four federal statutes authorize the FBI to issue "National Security Letters" (NSLs) to telephone companies, financial institutions, internet service providers, and consumer credit agencies, which require the recipients to produce the records that the government seeks.[21] The government need only state that the records sought are relevant to an authorized international terrorism or counterintelligence investigation and that the investigation is not being conducted "solely on the basis of activities protected by the first amendment" (e.g., not based solely on speech, protect, association, or religious practice). No court is involved, and the orders are issued and executed in secret.

The use of NSLs is growing dramatically, and they appear to be the instrument of choice for the FBI to use to obtain information in any way connected to counterterrorism or counterintelligence investigations. The FBI is required to inform Congress twice a year about its use of NSLs. In 2007, the Department of Justice Inspector General found that the FBI had substantially under-reported to Congress the number of NSLs it issued between 2003 and 2005. Instead of the 52,199 NSLs reported by the FBI, the actual figure is 143,074.[22] In 2006, the FBI issued 49,425 NSLs.[23] Each request may seek

[18] Id. at 9.

[19] See id. at 10.

[20] See, e.g., Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090 (June 9, 2003) (codified at 31 C.F.R. pts. 21, 103, 208, 211, 326, 563, and 748).

[21] Right to Financial Privacy Act (1978) (codified as amended at 12 U.S.C. § 3401(a)(5)); the Electronic Communications Privacy Act (1986) (codified as amended at 18 U.S.C. § 2709(b)(2)); the Fair Credit Reporting Act (1970) (codified as amended at 15 U.S.C. § 1681u(a)); the 1994 amendments to the National Security Act (1947) (codified as amended at 50 U.S.C. § 436(A)(1)).

[22] U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* 37-38 (2007), http://www.usdoj.gov/oig/special/s0703b/final.pdf.

records concerning many people. In fact, nine NSLs in one investigation sought data on 11,100 separate telephone numbers.[24]

ii. Exigent Letters

The Inspector General has also disclosed that the FBI has sought personal information through "exigent letters." The Inspector General found that "from 2003 through 2005 the FBI improperly obtained telephone toll billing records and subscriber information from 3 telephone companies pursuant to over 700 so-called 'exigent letters.'"[25] These letters typically provide:

> Due to exigent circumstances, it is requested that records for the attached list of telephone numbers be provided. Subpoenas requesting this information have been submitted to the U.S. Attorney's Office who will process and serve them formally to [information redacted] as expeditiously as possible.[26]

The Inspector General found that the FBI used these letters in "non-emergency circumstances," without in fact submitting the promised subpoenas, and even without having open the "duly authorized investigation" necessary under FBI policies to seek data about specific individuals.[27] The Inspector General concluded that "the FBI's use of these letters inappropriately circumvented the requirements of the NSL statute, and violated Attorney General Guidelines and FBI policies."[28] In August 2008, the FBI announced that targets of the exigent letter requests included reporters at the *New York Times* and the *Washington Post*.[29] Some letters called for the production of thousands of telephone numbers and customer transaction data.

In January 2010, the Department of Justice Office of the Inspector General found that FBI agents lied about their use of exigent letters and the data they obtained using them.[30]

iii. Administrative Subpoenas

Hundreds of agencies are authorized to issue administrative subpoenas. Many agencies have exceptionally broad authority in this area. The power and scope of administrative subpoenas was clearly demonstrated when shortly after the terrorist attacks of September 11, 2001, the U.S. Treasury Office of Foreign Assets Control began issuing administrative subpoenas for the data held in the U.S. operations center of the Society for Worldwide International Financial Telecommunication (SWIFT). By the end of 2006, SWIFT had received 65 subpoenas, each of which required it to provide the government with potentially millions of records "relevant to terrorism investigations."[31] Under an agreement reached in

---

[23] U.S. Department of Justice, Office of the Inspector General, *A Review of the FBI's Use of National Security Letters* 9 (2008), available at http://www.usdoj.gov/oig/special/s0803b/final.pdf.

[24] Eric Lichtblau, "F.B.I. Data Mining Reached Beyond Initial Targets," *New York Times*, Sept. 9, 2007, at A1.

[25] 2007 Report, supra at 8.

[26] Id.

[27] Id. at 8-9.

[28] Id. at 9

[29] "F.B.I. Obtained Reporters' Phone Records," *New York Times*, Aug. 9, 2008, at A15.

[30] U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* (2010).

[31] Office of the Privacy Commissioner of Canada, *Commissioner's Findings* ¶ 30 (Apr. 2, 2007), http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_e.asp.

June 2007 between U.S. and European officials, personal data obtained from SWIFT will not be retained for longer than five years, although that agreement is now in jeopardy.[32]

c. The Fourth Amendment

The government's extraordinary access to personal data held by the private sector is exacerbated by the U.S. Supreme Court's remarkable interpretation of the Fourth Amendment—our primary constitutional protection against government intrusion into personal privacy.

In 1976, the Supreme Court held *United States v. Miller* that there can be no reasonable expectation of privacy in information held by a third party.[33] The case involved copies of cancelled checks, to which, the Court noted, "respondent can assert neither ownership nor possession." Such documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," and therefore the Court found that the Fourth Amendment is not implicated when the government sought access to them:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[34]

The Court's decision in *Miller* is remarkably sweeping. The bank didn't just happen to be holding the records the government sought. The government compelled the bank under the Bank Secrecy Act to store the information, and then sought the information from the bank on the basis that since it held the data about its customer's checks, there couldn't be any reasonable expectation of privacy and the Fourth Amendment therefore did not apply. A majority of the Supreme Court was not troubled by this end-run around the Fourth Amendment: "even if the banks could be said to have been acting solely as Government agents in transcribing the necessary information and complying without protest with the requirements of the subpoenas, there would be no intrusion upon the depositors' Fourth Amendment rights."[35]

The Court reinforced its holding in *Miller* in *Smith v. Maryland*, involving information about telephone calls.[36] The Supreme Court found that the Fourth Amendment is inapplicable to telecommunications "attributes" (e.g., the number dialed, the time the call was placed, the duration of the call, etc.) because that information is necessarily conveyed to, or observable by, third parties involved in connecting the call. "[T]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this

[32] See James Risen, U.S. Reaches Tentative Deal with Europe on Bank Data, *N.Y. Times*, June 29, 2007, at A6.

[33] 425 U.S. 435 (1976).

[34] Id. at 443 (citation omitted).

[35] Id. at 444.

[36] 442 U.S. 735 (1979).

information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[37]

As a result, under the Fourth Amendment, the use of "pen registers" (to record out-going call information) and "trap and trace" devices (to record in-coming call information) does not require a warrant because they only collect information about the call that is necessarily disclosed to others.

The third party exemption from the Fourth Amendment made little sense in the cases in which it was created. Individuals who write checks and dial telephone calls do not "voluntarily" convey information to third parties. But irrespective of whether *Miller* and *Smith* were correct when decided, however, excluding records held by third parties from the protection of the Fourth Amendment raises far more significant issues today. Dramatic advances in digital technologies and society's increased reliance on them mean that more and more of individuals' daily activities, transactions, and communications are routinely captured and stored as digital data. This is especially true online, where merchants record data not only on what individuals buy and how we pay for our purchases, but also on every detail of what we look at, what we search for, how we navigate through web sites, and with whom we communicate.

All indications are that this is just the beginning. Broadband Internet access into homes has not only increased the personal activities we now engage in online, but also created new and successful markets for remote computer back-up and online photo, e-mail, and music storage services. With Voice Over IP telephone service, digital phone calls are becoming indistinguishable from digital documents: both can be stored and accessed remotely. Global positioning technologies are appearing in more and more products, and Radio Frequency Identification Tags are beginning to be used to identify high-end consumer goods, pets, and even people.

Advances in technologies, and the development of new products and services in response to those changes, have significantly expanded the scope of the *Miller* exclusion of records held by third parties from the protection of the Fourth Amendment. Today there are vastly more personal data in the hands of third parties, they are far more revealing, and much more readily accessible than was the case in the 1970s. As a result, the scope of the *Miller* decision has been greatly expanded and the balance between the government's power to obtain personal data and the privacy rights of individuals fundamentally altered.[38]

3. Conclusions

I would like to offer three conclusions.

First, unrestrained government access to vast swaths of sensitive personal information poses a significant threat to privacy.

Second, the rapid expansion of the government's access to data held by the private sector should concern the private sector. It threatens to turn industry into the government's data center. While

[37] Id. at 743.

[38] See Fred H. Cate, "The Vanishing Fourth Amendment," *BNA Privacy & Security Law Report*, Dec. 10, 2007, at 1875.

some U.S. telephone companies appear to regard this as a new revenue source, many other businesses have found government demands for data time-consuming, distracting, and a source of legal liability and customer distrust. Remember that most of the laws the government uses to access personal data from the private sector ignore privacy policies or contractual commitments, and do not require compensation.

Moreover, the fact that the government has unrestricted access to commercial records has already contributed to calls for greater privacy regulation applicable to the privacy sector on the basis that if industry cannot collect the data then they will not be available for the government to seize.

Third, the government's voracious appetite for private-sector data suggests that Canadian provincial governments are right to worry about allowing their citizens' data to come within the purview of U.S. law. The problem is that geographic responses simply don't work, for many reasons.

- The U.S. government may have direct access to the data it needs to investigate international terrorism and other serious criminal activity through its existing surveillance programs, often operated in collaboration with Canadian authorities. Look at SWIFT.

- The U.S. government is unlikely to access personal information held by Canadian provincial governmental bodies through service providers because it is more likely—in fact, legally required—to simply request the data from Canadian officials. Canada and the United States have for years sought personal information from each other's territories, shared information across their borders, and negotiated when efforts to obtain that information conflicted with the values of either nation.

  Canada and the United States are parties to a Mutual Legal Assistance Treaty, which governs the transborder collection of information between the two countries.[39] In addition, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has a memorandum of understanding with the U.S. Financial Crimes Enforcement Network (FinCEN), as well as authorities in 44 other countries, that facilitates the sharing of financial transaction information. The U.S.-Canada Treaty on Mutual Assistance in Criminal Matters governs the sharing of data between the U.S. Department of Justice and the Canadian Department of Justice.[40] Under the Shared Border Accord and Smart Border Declaration, Canada and the United States operate the NEXUS program, which allows the Canadian Border Services Agency and U.S. Customs and Border Protection to jointly gather and share information and to conduct bi-national security screening on Canadian and U.S. travelers.[41]

  Canadian law provides Canadian law enforcement and antiterrorism officials with power to access personal data similar to those in U.S. law, as the Privacy Commissioner of Canada, Jennifer Stoddart, has noted repeatedly: "The risk of personal information being disclosed to government authorities is not a risk unique to U.S. organizations. In the national security and

[39] Mutual Legal Assistance Treaty Between United States and Canada, reprinted in S. Treaty Doc. 100-14, 100th Cong., 2d Sess. (1988).

[40] See Office of the Privacy Commissioner of Canada, *Commissioner's Findings* ¶ 30 (Apr. 2, 2007), http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_e.asp.

[41] Documents Required for Travelers Departing From or Arriving in the United States at Sea and Land Ports-of-Entry From Within the Western Hemisphere, supra at 35093.

anti-terrorism context, Canadian organizations are subject to similar types of orders to disclose personal information held in Canada to Canadian authorities."[42]

With such a long and enduring relationship between Canada and the United States, U.S. government officials would likely just ask their Canadian counterparts for what they need for their counterterrorism and law enforcement efforts, as they are required to do under the Mutual Legal Assistance Treaty. In short, the tension over privacy is not between Canada and the United States, but rather within each government.

- The geographic approach to data protection also poses significant burdens on Canadians and Canadian industry. As written, the Canadian provincial laws are not limited to outsourcing large data sets outside Canada. The scope of the restrictions in at least two provinces includes using networks and services that involve "access from" another country, processing through a central data center located in another country transactional data involving public employees or services, servicing equipment containing personal data remotely from outside of Canada, sending and routing through another nation emails containing personal data from the public sector, and even placing telephone calls from or to a location outside Canada in which any personal data from the public sector is communicated.

  Outlawing all of these activities will lead to fewer services being available to Canadian public bodies and residents, increased bureaucracy and significantly reduced efficiency, higher financial costs, the real threat of tangible harms to health and safety, and the undermining of competition for public bodies' business and of Canada's burgeoning services industry, which accounts for 80 percent of new Canadian jobs between 1992 and 2005.[43]

- Finally, the geographic approach to data protection is clearly contrary to the continuing globalization of data flows, online commerce, and international trade and travel. It will be ironic if just as the world is truly becoming smaller and more integrated, we use national and even provincial laws to try to drive people farther apart.

We are going to have to find a better way forward based on respect for national sovereignty, international data flows and trade in data products and services, and individual privacy. The private sector plays a critical role and, in the long run, has the most to lose if we fail.

---

[42] Office of the Privacy Commissioner of Canada, *Bank's Notification to Customers Triggers PATRIOT Act Concerns* (PIPEDA Case Summary #313), Oct. 19, 2005, http://www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp; see also Office of the Privacy Commissioner of Canada, *Report of Findings in Files 6100-02681, 6100-02682, 6100-02683,* ¶ 37 (Aug. 7, 2008).

[43] Canadian Services Coalition & Canadian Chamber of Commerce, *Canadian Services Sector: A New Success Story* 3 (2006), http://www.canadianservicescoalition.com/CanadianServicesSectorANewSuccessStory.pdf.