BNA, INC.

FEDERAL CONTRACTS

BNA Employee-Owned Since 1947

REPORT

Homeland Security

Almost a year ago, David Bodenheimer outlined for FCR some of the unique risks faced by Department of Homeland Security contractors as a result of privacy concerns that may limit information sharing.

The update below provides further information on how U.S. contractors may be ''caught in the crossfire'' when border and transportation security programs depend on international information sharing and foreign privacy requirements restrict such cross-border data flow.

WHEN HOMELAND SECURITY GOES ABROAD: *THE GLOBAL COLLISION OF PRIVACY & ANTI-TERRORISM LAWS*

BY DAVID Z. BODENHEIMER AND KRIS D. MEADE

In the war on terrorism, striking the right balance between privacy and homeland security remains as maddeningly elusive as leprechauns astride unicorns. Both privacy and homeland security deservedly bring powerful, determined champions ready to tip this balance in their favor and to pummel government policy-makers and contractors alike that fail to pay sufficient deference to either constituency. Domestically, a number of high-profile homeland security efforts – TIA, CAPPS II, MATRIX, and others – have paid a high price for underestimating the gravity of privacy interests as an integral element of security programs aimed at collecting, analyzing and sharing data to unmask terrorists.[1]

Bodenheimer and Meade are partners in the law firm of Crowell & Moring LLP in Washington, D.C. Mr. Bodenheimer specializes in government contracts, homeland security, and privacy and may be reached at (202) 624-2713 or dbodenheimer@crowell.com. Mr. Meade specializes in employment law and privacy and may be reached at (202) 624-2854 or kmeade@crowell.com.

[1] In 2003, Congress cut off funding for the Defense Department's Terrorist Information Awareness (TIA) program. In 2004, privacy problems and Congressional opposition forced the Transportation Security Administration (TSA) to end the Computer-Assisted Passenger Prescreening System (CAPPS) II program and restructure it as Secure Flight. By 2005, a num-

 ISSN 0014-9063

Internationally, the same dynamic is underway, except that privacy and security may collide with shattering force due to the great differences and many inconsistencies in privacy laws between the United States and other nations. Department of Homeland Security officials and contractors must heed these international privacy issues and concerns that can delay, disrupt, or even crush what initially appeared to be promising technologies and opportunities for hunting down terrorists.

This analysis addresses the interrelated roles of international cooperation, privacy, and information sharing in the homeland security mission and how privacy issues have shaped – and will continue to shape – United States and global initiatives in the ongoing fight against terrorism. Key issues include:

- the need for international cooperation and information sharing in fighting terrorism and the implications for global privacy;
- the differences in international privacy laws, particularly between the United States, Europe, and Canada; and
- the impact of international privacy issues on agencies and contractors supporting both domestic and international anti-terrorism programs.

INTERNATIONAL COOPERATION AND INFORMATION SHARING

Virtually everyone agrees on the need for international cooperation against terrorism, but progress on information sharing continues to face substantial challenges due, in part, to international differences on privacy.

International Cooperation

Terror is global. High-profile terror attacks have ripped through the international community – including London, Madrid, Amman, Bali, New York, and Washington, DC – underscoring the bitter fact that everyone everywhere is at risk. As a result, the need for international cooperation is almost universally acknowledged. For example, the President's National Strategy for Homeland Security states: ''In a world where the terrorist pays no respect to traditional boundaries, a successful strategy for homeland security requires international cooperation.''[2]

The critical importance of international cooperation and partnerships surfaces nearly everywhere, from the Southeast Asian Nations/Russian pact to the European Counter-Terrorism Strategy to the United States' 9/11 Commission Report.[3] To this end, the United States has made progress with other countries on a number of fronts, including the Container Security Initiative (CSI) agreements, biometric identifiers, and police and judicial cooperation.[4]

Information Sharing

Terrorism, by its nature, is sneaky and covert. Unlike our Cold War adversaries who were handily marked with a bright red star, the war on terror lacks readily identifiable foes statically entrenched behind jealously guarded borders. Instead, this new war hinges upon rapid information gathering, processing, and sharing to unmask the who, what, when, where, and how of terrorist plans before they hatch. To be effective, information sharing must be as global and instantaneous as the terrorist threat.

The vital role of information sharing in fighting terrorism is well recognized.[5] Within the United States, the ''whole purpose'' of establishing the Department of Homeland Security (DHS) ''was to facilitate the notion of information sharing.''[6] Within Europe, the European Union (EU) identified its key role in coordinating anti-terrorism measures as promoting ''the exchange and sharing of information among member states.''[7] In 2001 and 2002, the EU and the United States concluded agreements allowing Europol and United States law enforcement authorities to ''share both 'strategic' information (threat tips, crime patterns, and risk assessments) as well as 'personal' information (such as names, addresses, and criminal records).''[8]

However, grave privacy concerns remain as a major counterweight that limits greater international information sharing and complicates trans-border flows of data for combating terrorism. Franco Frattini, European Commissioner for Justice, Freedom and Security, summed up the tension between privacy and global information sharing in the war on terrorism:

> It is obvious that organised crime and terrorism are internationally operating and that they can only be effec-

---

ber of states had pulled out of the law enforcement database known as the Multi-State, Anti-Terrorism Information Exchange (MATRIX) due, in part, to privacy concerns. *See* David Bodenheimer, ''Privacy vs. Information Sharing: The Gathering Storm Over Homeland Security and How Contractors Can Reduce Their Risks,'' 83 *BNA Federal Contracts Report* 540 (May 31, 2005).

[2] Office of Homeland Security, *National Strategy for Homeland Security* 59 (July 2002) (http://www.dhs.gov/dhspublic/interapp/publication/publication_0005.xml).

[3] Association of Southeast Asian Nations (ASEAN)-Russia Joint Declaration for Cooperation to Combat International Terrorism (July 2, 2004) (http://www.aseansec.org/16225.htm); Council of the European Union (CEU), *The European Union Counter-Terrorism Strategy* 4 (Dec. 1, 2005) (''Promoting International Partnerships''). (http://ue.eu.int/uedocs/cms_Data/docs/pressdata/en/jha/87257.pdf); *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* 367, 379 (W. W. Norton) (2004) (recommendations for international cooperation).

[4] Congressional Research Service (CRS) Report, *U.S.-EU Cooperation Against Terrorism* 3-4 (July 12, 2005) (RS22030); CEU, *Implementation of the Action Plan to Combat Terrorism* 9 (Dec. 1, 2005) (EU/US cooperation ''excellent'').

[5] *Out of Many, One: Assessing Barriers to Information Sharing in the Department of Homeland Security: Hearings Before the House Comm. on Gov. Reform*, 108th Cong., 1st Sess. 1 (2003) (''information-sharing'' is a ''vital mission''; statement of Rep. Davis) (''failure to share critical terrorist information'' was ''one of the single most significant problems'' leading to 9/11 attacks; statement of Rep. Waxman); GAO, ''Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues,'' p. 12 (Sept. 17, 2003) (GAO-03-1165T).

[6] *Can the Use of Factual Data Analysis Strengthen National Security? – Part I: Hearings Before the House Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census of the Comm. on Gov. Reform*, 108th Cong., 1st Sess. (May 6, 2003) (statement of Adm. Loy).

[7] EU Justice & Security, Anti-terrorism Policy (updated Feb. 16, 2006) (http://www.euractiv.com/Article?tcmuri=tcm:29-136674-16&type=LinksDossier).

[8] CRS Report, *U.S.-EU Cooperation Against Terrorism* 3 (July 12, 2005) (RS22030).

  FCR ISSN 0014-9063

> tively tackled by strong police and judicial cooperation between EU Member States, and, increasingly, between the EU and third countries. Such cooperation necessarily implies the exchange of personal data, indeed such exchange often proves vital in criminal investigations. However as this exchange of data has an impact on the personal data of many citizens it is necessary to ensure that these data are processed thoroughly and carefully. Fundamental principles regarding data quality and the legitimacy of data processing have to be respected.[9]

These tensions are driven, in part, by the considerable differences between U.S. privacy laws and those of other countries. These differences – and their impact on homeland security initiatives and government procurements – are discussed in greater detail below.

INTERNATIONAL VARIATIONS IN PRIVACY LAW

Since the EU adopted comprehensive requirements for privacy and data security, such privacy protections have become increasingly common around the world. A comparison of the law in the United States with that in the EU and Canada illustrates the very different approaches to protecting and regulating privacy.

Privacy Laws in the United States

The United States does not have a ''comprehensive federal statute that protects the privacy of personal information held by the public sector and the private sector.''[10] Instead, a patchwork of laws govern privacy with wide variations in protection depending upon the type of data, the industry, and the public/private control of such data.[11]

For federal agencies with ''systems of records'' containing personal information, the Privacy Act (5 U.S.C. § 552a) establishes a variety of safeguards restricting disclosure without the individual's consent, granting the individual a right of access and the opportunity to seek correction of errors, and establishing ''fair information practices'' for collection, maintenance, and dissemination of records. These requirements also may apply to government contractors that operate these systems of records on the federal agency's behalf.[12]

Beyond the federal government, a welter of federal statutes target specific data in specific industries and areas. These laws range from videotape rental information and educational records[13] to financial institutions and health care entities.[14] At the state level, the continuing parade of front-page news articles on privacy breaches have propelled state legislatures to enact a host of statutes requiring notice of security breaches and other privacy safeguards; some mandate pre-breach security measures, but many do not.[15] As a result of such piecemeal legislation, the risk and complexity of privacy compliance continues to grow in the United States.

European Privacy Law

For the European Economic Area (EEA), the member nations adopted a more rigorous and comprehensive set of requirements for privacy and data security. In 1995, the European Data Protection Directive (Directive 95/46/EC) established minimum standards governing personal information for individuals within the EEA region. Some EAA nations, such as Spain, have supplemented these standards with even more stringent requirements for protecting and securing privacy. To enforce these safeguards, the Data Protection Authorities come armed with ample sanctions including criminal penalties and fines, as well as compensation to injured parties and injunctive power to halt the processing of personal information.

The Directive covers all types of organizations that collect (data controllers) or process (data processors) personal information, regardless of whether such entities are public or private. Furthermore, the Directive requires that personal information be:

- processed fairly and lawfully, with adequate notice to the data subject of the intended uses of personal information;
- collected for a specific and legitimate purpose;
- relevant and not excessive in relation to its purpose;
- kept no longer than necessary for such purpose;
- accurate and (where necessary) current;
- stored in a secure fashion; and
- not transferred outside of the EEA without ''an adequate level of protection.''

Of these ''data protection principles,'' the last one – restrictions on data flows outside of the EAA – weighs most heavily upon international information exchanges to combat terrorism. In particular, the EU does not consider privacy laws in the United States to provide ''an adequate level of protection,'' with the result that the EU has often resisted sharing anti-terrorism information in the absence of specific bilateral agreements limiting the type, use, and availability of the exchanged data.[16]

Canadian Privacy Law

In 2000, Canada's Parliament enacted the Personal Information and Protection and Electronic Documents Act (PIPEDA) to protect how personal information is

---

[9] ''EU steps up personal data safeguards as part of fight against terrorism,'' PublicTechnology.net (Oct. 10, 2005). (http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=3772).

[10] CRS Report, *Privacy: Total Information Awareness Programs and Related Information Access, Collection and Protection Laws* 5 (Feb. 14, 2003) (RL31730).

[11] Robert Ellis Smith, *Compilation of State and Federal Privacy Laws* (2002); Eric Dash, ''Strong privacy laws may explain data security in Europe,'' *The New York Times* (Aug. 8, 2005).

[12] 5 U.S.C. § 552a(m)(1); Federal Acquisition Regulation (FAR) § 24.102.

[13] The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (educational records); Video Privacy Protection Act, 18 U.S.C. § 2710 (videotape records).

[14] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-08 (financial institutions); Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d (health care entities).

[15] Alpin, ''In 2006, More States Seek to Add to Body of 23 Data Breach Notice Laws,'' *BNA Privacy Law Watch* (Feb. 17, 2006); Krim, ''States Scramble to Protect Data,'' *Washington Post*, p. E1 (Apr. 9, 2005).

[16] CRS Report, *U.S.-EU Cooperation Against Terrorism* 3 (July 12, 2005) (RS22030).

collected, used or disclosed. This statute requires that ''every organization'' that ''collects, uses or discloses'' personal information ''in the course of commercial activities'' must take steps to safeguard individual privacy.[17] Unlike privacy laws in the United States, the EU recognizes Canadian privacy law embodied in PIPEDA as assuring an ''adequate level of protection,'' thus facilitating the exchange of information for anti-terrorism and other purposes.

Companies doing business in Canada can expect much more rigorous PIPEDA enforcement in the near future. Canada's Federal Privacy Commissioner Jennifer Stoddart recently warned that ''she will make greater use of her statutory powers to crack down on privacy violations in Canada because organizations are not taking their privacy responsibilities seriously enough.''[18]

GOVERNMENT CONTRACTORS CAUGHT IN THE CROSSFIRE

United States contractors doing business abroad face a Hydra-headed list of legal risks, ranging from Foreign Corrupt Practice Act marketing restrictions (15 U.S.C. §§ 78dd-1-3) to export controls and regulations. To this list must be added international privacy and security laws and sanctions. While the risks are many, three types of information sharing should raise red flags, causing both agencies and contractors to pay close attention to privacy and data security risks: (1) border and transportation security programs dependent upon international information sharing; (2) domestic contractors sharing information with foreign vendors; and (3) United States contractors and their foreign subsidiaries caught between domestic anti-terrorism laws and foreign privacy requirements.

Border and Transportation Security Information Sharing

The 9/11 terrorists came from abroad. This simple fact illustrates the critical importance of international information sharing to border and transportation security both here and abroad. Nonetheless, European privacy laws have had a direct effect on border and transportation security programs in the United States.

After complaints that the United States' demands for passenger data violated European privacy laws,[19] the European Commission (EC) and the United States struck a temporary agreement for exchanging air passenger data.[20] However, this agreement remains highly controversial and the top official for the EU's highest court – the European Court of Justice – has sought its annulment.[21] Privacy concerns have also hampered U.S. efforts to require biometric passports for EU visitors.[22]

For homeland security contractors, these international uncertainties over information sharing can have concrete effects in disrupting programs and causing delays. For example, the CAPPS II passenger prescreening program depended upon obtaining ''critical'' information regarding foreign nationals on domestic and international flights. According to the Government Accountability Office:

> [O]btaining international cooperation for access to this data remains a substantial challenge. The European Union, in particular, has objected to its citizens' data being used by CAPPS II, whether a citizen of a European Union country flies on a U.S. carrier or an air carrier under another country's flag. The European Union has asserted that using such data is not in compliance with its privacy directive and violates the civil liberties and privacy rights of its citizens.[23]

Lack of such data not only had short-term implications for testing ''the system's initial operating capabilities,'' but also longer term effects of ''compromising the full capabilities and effectiveness of CAPPS II.''[24] Ultimately, a combination of domestic and international privacy concerns delayed the program and caused the Transportation Security Administration to replace it with Secure Flight – a program that also was canceled.

Domestic Information Sharing with Foreign Vendors

While the global economy becomes increasingly interwoven, a variety of information security rules place restrictions and/or reporting requirements upon domestic government contractors that seek to share information with foreign vendors. For example, the information security requirements imposed by the Federal Information Security Management Act (FISMA) continue to flow down hill, requiring not only federal agencies but government contractors as well to establish and enforce appropriate safeguards to protect the vast treasure troves of government information to which they have access.[25] As a senior State Department official explained at an India-United States Information Security Summit recently, such security requirements must be flowed down to foreign vendors: ''More and more, the U.S. will insist on the implementation of a management chain of trust, to ensure that the security safeguards in

---

[17] R.S.C., ch. 5, § 4(1) (http://www.privcom.gc.ca/legislation/02_06_01_e.asp). The statute is based on the Canadian Standards Association's *Model Code for the Protection of Personal Information* that recognized ten core privacy principles: (1) accountability; (2) identified purpose; (3) consent; (4) limited collection; (5) limited use, disclosure, and retention; (6) accuracy; (7) security safeguards; (8) openness; (9) individual right of access; and (10) compliance and individual redress. (http://canada.justice.gc.ca/en/news/nr/1998/attback2.html).

[18] ''Canada's Federal Privacy Commissioner Vows to Crack Down on PIPEDA Non-Compliance,'' *BNA Privacy Law Watch* (Mar. 15, 2006).

[19] Knight, ''Some Air Carriers in Europe Skirt Antiterror Steps,'' *The Wall Street Journal*, p. D10 (Sept. 24, 2003).

[20] EC Decision (May 14, 2004).

[21] Lipowicz, ''EU official urges halt of European passenger data transfer to DHS,'' *Government Computer News* (Nov. 23, 2005); Opinion of Advocate General Leger, Case C-317/04, *European Parliament v. Council of the European Union* (Nov. 22, 2005).

[22] Rohde, ''Possible U.S.-EU Fight Looms Over Biometric Passports,'' *ComputerWorld* (Apr. 4, 2005) (www.computerworld.com).

[23] GAO, ''Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges'' 27 (Feb. 2004) (GAO-04-385).

[24] *Id.* at 28; *see also* GAO, ''Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed'' 59-60 (Mar. 2005) (GAO-05-356).

[25] Pub. L. No. 107-347, Title III, now codified at 44 U.S.C. §§ 3541-45; FAR § 39.101(d).

  FCR ISSN 0014-9063

place in the company providing the outsourcing services meet the requirements of FISMA.''[26]

Beyond FISMA information security requirements, domestic government contractors must also beware of a number of other obligations and risks associated with sharing information for foreign partners and vendors:

- *Data Export Controls*. Providing foreign companies with access to certain technology data may trigger export control requirements.[27]
- *Sensitive Security Information*. TSA security restrictions may limit the disclosure of information relating to transportation security systems.[28]
- *Critical Infrastructure Information (CII)*. Protected CII generally must not be disclosed even to subcontractors without written agency approval.

Foreign Subsidiaries and Data Flows to Domestic Parents

Canadian subsidiaries of United States corporations currently find themselves in the middle of a free-fire zone, as the United States anti-terrorism laws and Canadian privacy requirements unload conflicting, high-risk obligations upon such companies. On one hand, the USA PATRIOT Act extends global reach to anti-terrorism intelligence gathering as it ''gave the FBI an expanded national security role and armed it with extraordinary legal processes to acquire personal information (about Americans and about foreign nationals) held by American companies and by foreign companies affiliated with American companies, no matter where those companies were located or whom they were working for.''[29]

This spectre of the United States compelling extra-territorial disclosure of personal information of Canadian citizens has produced a privacy backlash with, in a number of cases, the impact being felt by Canadian subsidiaries of United States companies. For example, Statistics Canada (a federal statistics agency) outsourced its census data management to a Canadian subsidiary to a major United States defense contractor. When risk of information access under the USA PATRIOT Act became apparent, the Canadian Federal Privacy Commissioner outlined the actions taken, including revising the contract to beef up privacy requirements and promising ''on-site review'' to enforce compliance.[30] For another United States-linked contractor picked by the British Columbia government to run the province's public health insurance program, the government union opposed the outsourcing because ''contractors who possess personal information could be secretly compelled under the [USA PATRIOT Act] to turn it over to US authorities.''[31] The British Columbia government did eventually award the contract, but required the company ''to set up a BC-based subsidiary overseen by Canadian directors and committed to maintaining the medical records inside British Columbia.''[32]

Meanwhile, the Alberta government has proposed dramatically increased fines for privacy breaches: ''The proposed changes would seek to protect Albertans' personal information from improper access by foreign governments (such as the United States under its USA Patriot Act),'' according to the Alberta Government Services.[33] Thus, the potential for conflicting legal requirements and sanctions for privacy breaches make the risk of doing business in Canada much greater, especially for United States companies and their Canadian subsidiaries.

CONCLUSION

Around the world, both government officials and contractors are struggling to serve two masters – the twin mandates to combat terrorism through international information sharing and to protect privacy and civil liberties with additional safeguards. Both mandates require leadership commitment, technological advances, and public trust that neither objective will be sacrificed in the single-minded pursuit of the other. The Canadian Privacy Commissioner summed it up rather starkly:

> I want to remind you of the lay of the privacy landscape – or perhaps it is better called a battlefield. On that battlefield, the world has become a more dangerous place.[34]

Government officials or contractors that fail to heed this warning may well find themselves the next casualty on the international privacy ''battlefield.''

---

[26] ''In India, U.S. Official Outlines Measures For Outsource Services, U.S. Security Standards,'' *BNA Privacy Law Watch* (Jan. 19, 2006) (quoting Michele Markoff, State Department senior coordinator for International Critical Infrastructure Protection).

[27] 15 C.F.R. Parts 730-74; 22 C.F.R. Parts 120-130.

[28] 69 Fed. Reg. 28070 (May 18, 2004).

[29] Alberta Office of the Information and Privacy Commissioner, *Public-sector Outsourcing and Risks to Privacy* 11 (Feb. 2006) (*http://www.gov.ab.ca/acn/200602/19490.pdf*).

[30] ''Canadian Privacy Commissioners Address Impact of USA PATRIOT Act,'' *BNA Privacy Law Watch* (Mar. 1, 2006).

[31] Alberta Office of the Information and Privacy Commissioner, *Public-sector Outsourcing and Risks to Privacy* 8 (Feb. 2006) (*http://www.gov.ab.ca/acn/200602/19490.pdf*).

[32] *Id.* at 14.

[33] ''Alberta Proposes Privacy Amendments to Respond to USA PATRIOT Act Fears,'' *BNA Privacy Law Watch* (Mar. 15, 2006).

[34] Jennifer Stoddart (Privacy Commissioner of Canada), ''Taking on the Privacy Challenges Ahead,'' 7th Annual Privacy and Security Conference: Privacy and Security is Everyone's Responsibility (Feb. 9, 2006), quoted in ''Canada's Federal Privacy Commissioner Vows to Crack Down on PIPEDA Non-Compliance,'' *BNA Privacy Law Watch* (Mar. 15, 2006).