BNA, INC.

FEDERAL CONTRACTS

BNA Employee-Owned Since 1947

REPORT

Homeland Security

Since the enactment of the Homeland Security Act of 2002, many federal contractors have focused on the Department of Homeland Security's SAFETY Act authority as a possible way to limit the risks of litigation arising from the deployment of antiterrorism technologies.

However, the department's unique mission also can pose—rather than limit—risks for its contractors. Companies interested in contracting with DHS need to be aware of these risks and some steps they can take to mitigate them.

Privacy vs. Information Sharing: The Gathering Storm Over Homeland Security and How Contractors Can Reduce Their Risks

BY DAVID Z. BODENHEIMER

A paradoxical mission bedevils the Department of Homeland Security (DHS) – share information broadly and quickly, but without jeopardizing privacy through too much information sharing. If terrorist data remains bottled up in DHS or other agencies, we lose real opportunities for preempting another 9/11 terrorist attack. Conversely, huge caches of personal data – aggregated, sifted, and networked at the national level – stoke privacy concerns of an Orwellian Big Brother capable of overseeing an individual's every move.

Mr. Bodenheimer is a partner in the law firm of Crowell & Moring LLP in Washington, D.C., where he specializes in government contracts and homeland security. He handles litigation, advises clients, and writes and lectures on a variety of high-technology and biodefense matters, including SAFETY Act coverage, privacy and information security, chemical and biological protection, and homeland security technology. Mr. Bodenheimer may be reached at (202) 624-2713 or dbodenheimer@crowell.com.

Even as DHS attempts to balance these statutory mandates of sharing information and protecting privacy, the balance point is tilting in favor of greater privacy protection. Increasingly, opposition to homeland security technologies and programs centers upon privacy concerns. At the same time, recent headlines and congressional hearings have spotlighted multiple instances in which personal information may have been compromised by private data aggregators such as ChoicePoint due to apparent lapses in information security.

In combination, these events are generating a powerful tailwind of privacy concerns that DHS and homeland security contractors alike must heed. If such con-

 ISSN 0014-9063

cerns are not addressed up front by DHS and its contractors, the risks to homeland security programs – delays, political opposition, or even termination of funding and support – escalate rapidly, thus postponing ready access to critical anti-terrorism technology. In addition, certain breaches of privacy may expose DHS and private contractors to administrative, civil, or even criminal sanctions.

This analysis addresses the interrelated roles of privacy and information sharing in homeland security and how privacy issues have shaped – and will continue to shape – DHS initiatives in the fight against terrorism. Key issues include:

- the privacy framework for DHS specifically and federal programs generally;
- the impact of privacy concerns on homeland security programs; and
- the growing pressures for tougher privacy protections.

THE PRIVACY FRAMEWORK

By law, DHS has responsibility for considering privacy as a factor in achieving its homeland security mission. While the existence of this duty is clear, its nature and scope are not, for at least three reasons. First, the privacy mandate is *relative*, not absolute – privacy can never completely trump DHS's core mission of sharing information to deter terrorism. Second, domestic privacy rules are *fragmented* – the United States generally governs privacy with a patchwork of industry-specific laws and policies, rather than a single, comprehensive federal privacy statute. Third, privacy risks and rules are *dynamic* – technology breakthroughs create new and unanticipated privacy risks, while international trends towards greater privacy protection clash with global initiatives to unmask the terrorists.

The Divided Mission: Sharing Information and Protecting Privacy

In the Homeland Security Act of 2002 (Pub. L. No. 107-296), Congress gave DHS a multi-pronged mission, with sharing information and protecting privacy being high on the priority list.

Information Sharing

A broad consensus exists that information sharing – ''connecting the dots'' – represents a core purpose of, and ''vital mission'' for, DHS.[1] As the Transportation Security Administration (TSA) Director testified in 2003, ''the whole purpose of DHS . . . was to facilitate the notion of information sharing.''[2] To this end, the Homeland Security Act requires DHS not only to access, analyze, and integrate information necessary for combating terrorism, but also to:

> disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

Pub. L. No. 107-296, §§ 201(d)(1), (3), (9). Congress expressly recognized that this treasure trove of information might come, in part, from ''data-mining and other advanced analytical tools.'' *Id.,* § 201(d)(14).

Privacy Protection

In its report, the 9/11 Commission acknowledged the tension between sharing information and protecting privacy, as reflected in the following recommendation: ''As the President determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared.''[3] Recognizing the risks associated with gathering and sharing information at each and every level of government, Congress placed certain constraints upon DHS, including the mandate to protect privacy. In particular, DHS must ''treat information in such databases in a manner that complies with applicable Federal law on privacy.'' Pub. L. No. 107-296, § 201(d)(15). Similarly, the Homeland Security Act requires the department to ''establish procedures'' to ''protect the constitutional and statutory rights of any individuals who are the subjects of such information'' and to appoint a privacy officer responsible for ''privacy policy'' and protecting privacy rights.'' *Id.,* §§ 221(3), 222.

Federal Privacy Standards

To date, the federal government has not established comprehensive privacy standards covering both the private and public sectors. For the private sector, the federal approach has been to legislate to address specific privacy problems in specific industries. *See, e.g.*, Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-08 (financial institutions); Health Insurance Portability and Accountability Act (HIPAA) (health care industry), 42 U.S.C. § 1320d; 45 CFR § 164.512. The scope, protections, and exemptions (such as disclosure for law enforcement purposes) vary considerably due to the patchwork nature of the federal privacy rules applicable to the private sector.

In the public sector, the Privacy Act generally restricts federal agencies from disclosing private information from government records unless appropriate notice is given and individual consent is received. 5 U.S.C. § 552a. The Privacy Act may also extend to government contractors responsible for operating a federal agency's ''system of records.'' 5 U.S.C. § 552a(m)(1). Indeed, the Federal Acquisition Regulation (FAR § 24.102(b))

---

[1] *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).

[2] *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).

[3] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* 395 (W. W. Norton) (2004); also available at www.9-11commission.gov.

  FCR ISSN 0014-9063

warns of the possibility of criminal penalties for Privacy Act violations:

> An agency officer or employee may be criminally liable for violations of the Act. When the contract provides for operation of a system of records on individuals, contractors and their employees are considered employees of the agency for purposes of the criminal penalties of the Act.

International Privacy Standards

Given the global reach of terrorism, the United States must often cooperate with countries imposing considerably more stringent privacy requirements. Within the European Economic Area (EEA), the European Data Protection Directive (Directive 95/46/EC) requires member states to implement national laws to establish minimum standards regulating not only how personal information is collected and used within the EEA, but also what protections must exist for data transfers outside of the EEA. To satisfy the directive's minimum standards, the personal information must, *inter alia*, be relevant, accurate, securely stored, fairly and lawfully processed, obtained for a proper purpose, and not transferred outside the EEA without ''an adequate level of protection.''

Some United States anti-terrorism initiatives have already collided with the European data protection requirements as Europeans say the use of extensive information on passengers violates privacy laws.[4] The European Commission and the United States temporarily resolved the impasse over sharing air passenger data by entering into an agreement covering such exchanges for a three-and-a-half-year period. *See* European Commission Decision (May 14, 2004). However, the prospect for future collisions between international information sharing and privacy is increasing as European countries continue to toughen their own data protection laws and other countries (such as Japan, Hong Kong, Australia, New Zealand, and Taiwan) adopt comprehensive data protection laws patterned upon the European model. Accordingly, both DHS and industry must be prepared to navigate foreign privacy laws that may be at odds with certain data collection and sharing practices needed in the fight against terrorism.

THE IMPACT OF PRIVACY ON HOMELAND SECURITY INITIATIVES

Privacy issues have swirled around many homeland security initiatives, such as certain provisions in the PATRIOT Act (Pub. L. No. 107-56) for law enforcement and intelligence gathering.[5] When personal information is at stake, privacy concerns can delay, reshape, or even effectively end homeland security programs.

Program Cancellation

During 2002, both Congress and privacy advocates began close scrutiny of the Defense Advanced Research Projects Agency (DARPA) data analysis program originally known as Total Information Awareness (TIA):

> A key component of the TIA program is the deployment of data mining technologies to sift through data and transactions to find patterns and associations to discover and track terrorists. The idea is that ''if terrorist organizations are going to plan and execute attacks against the United States, their people must engage in transactions and they will leave signatures in this information space. . . .''[6]

By 2003, the TIA program galvanized privacy advocates who warned of an ''all-encompassing surveillance tool'' that would ''pose an enormous threat to Americans' privacy.''[7] During congressional hearings in May 2003, the DARPA director admitted the agency had been so ''stunned'' by the comments that ''we didn't do anything about it for some time'' and ''[w]e watched it, and finally we woke up.''[8] Without a full and prompt response to these privacy concerns by the agency, Congress effectively killed the TIA program by barring further funding. *See* 2004 Department of Defense Appropriations Act, Pub. L. No. 108-87, § 8131.

Program Delay and Restructuring

To upgrade security for airline passengers, Congress authorized TSA to proceed with the Computer-Assisted Passenger Prescreening System (CAPPS II) program to assist with authentication of passenger identities and to compare passenger lists against terrorist watch lists.[9] The CAPPS II program encountered initial turbulence due to European privacy concerns about transfer of European passenger data, but the European Commission and the United States reached a temporary accommodation in an agreement covering such exchanges for a three-and-a-half-year period. *See* European Commission Decision (May 14, 2004). Congress subsequently slowed down CAPPS II development pending a GAO review of privacy safeguards.[10] Further delays resulted when air carriers balked at disclosing passenger data needed for conducting system testing.[11] Faced with these delays, TSA has since restructured the CAPPS II program.

Erosion of Funding Support

Originally conceived by the Florida Department of Law Enforcement and a private contractor, the Multi-State, Anti-Terrorism Information Exchange (MATRIX) database furnished law enforcement officials with ready access to personal data from public records and commercial sources, such as property records, Internet domains, address histories, utility connections, bankrupt-

---

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

[5] *See, e.g.,* Perine, ''Focusing on Patriot Act vs. Privacy,'' *Congressional Quarterly Today* (Apr. 4, 2005); *Oversight Hearing on Implementation of the USA PATRIOT Act: Sections of the Act that Address—Crime, Terrorism, and the Age of Technology, Sections 209, 217, and 220: Hearings Before House Subcomm. on Crime, Terrorism and Homeland Security of the Comm. of the Judiciary*, 109th Cong., 1st Sess. (2005) (statement of Mr. Dempsey).

[6] Congressional Research Service, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws* 1 (Feb. 14, 2003) (RL31730) (quoting from DARPA technical presentation).

[7] American Civil Liberties Union (ACLU), ''Total Information Compliance: The TIA's Burden Under the Wyden Amendment,'' (May 19, 2003) (www.aclu.org).

[8] *See* 2003 House hearings in note 3 above (statement of Dr. Tether).

[9] Aviation and Transportation Security Act, Pub. L. No. 107-71, § 136, 115 Stat. 597, 637 (2001).

[10] 2004 Department of Homeland Security Appropriations Act, Pub. L. No. 108-90, § 519, 117 Stat. 1137, 1155-56 (2003).

[11] GAO, ''Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges,'' p. 4 (Feb. 2004) (GAO-04-385).

cies, and liens.[12] Backed by federal grant funds, the MATRIX program originally attracted participation from 13 states, but most withdrew due to a combination of privacy and budget concerns.[13] In April 2005, the MATRIX program shut down after federal funds ran out, although individual states could still continue to fund pieces of the program. The program ended amid controversy, with MATRIX program officials pointing to expiration of federal funds as the reason for shutting down operations, while privacy advocates claimed privacy concerns led to the program's demise.[14]

Public Opposition and Boycott

A number of other homeland security initiatives have met with public opposition – or even boycott – due to privacy concerns. Examples include:

- *RFID Passports*. The plan to embed radio frequency identification (RFID) chips in passports has raised privacy concerns about ''skimming,'' in which nearby information thieves could steal personal data with hand-held chip readers.[15]

- ''*Intelligent Mail*.'' In the wake of the anthrax attacks, the President's Commission on the United States Postal Service recommended ''Intelligent Mail'' that would provide ''sender identification for every piece of mail,'' but privacy advocates warned that such disclosures were contrary to privacy rights long respected by the Postal Service.[16]

- *Passenger Information*. Public opposition can have economic consequences, as one group organized a boycott in 2003 against Delta Airlines for its planned cooperation in sharing passenger data for developing a passenger screening system. (www.boycottdelta.org).

ESCALATING PRESSURES FOR GREATER PRIVACY PROTECTION

While another terrorist attack could quickly alter the current balance between sharing information and protecting privacy in the homeland security arena, recent developments suggest that pressure will steadily grow to impose greater privacy protections in the near future.

The Domestic Spotlight on Privacy

Propelled by a series of well-publicized incidents involving the compromise of personal data by private companies and universities, privacy concerns have gained traction as a compelling domestic issue. Recent headlines capture both the risks to individual companies, as well as the growing pressure to assure protection of personal data:

> ''ID Thieves Breach Lexis/Nexis, Obtain Information on 32,000,'' *Washington Post,* p. E1 (Mar. 10, 2005)
>
> ''Burned by ChoicePoint Breach, Potential ID Theft Victims Face a Lifetime of Vigilance,'' *Information Week* (Feb. 24, 2005)
>
> ''Break-In at SAIC Risks ID Theft,'' *Washington Post,* p. E1 (Feb. 12, 2005)

Igniting more than just negative publicity, such incidents have sparked a conflagration of legislative hearings and bills at both the federal and state level. For example, senior officials at ChoicePoint and Lexis/Nexis have had the opportunity to testify before multiple Senate and House subcommittees that have dissected apparent corporate breaches of information security and heard privacy advocates press for new legislation imposing stricter privacy controls on personal data.[17] In addition to proposed privacy legislation at the federal level, the state legislatures have seized upon privacy and information security issues as platforms for new legislation: ''Bills are on the table in 28 states responding to a series of high-profile security breaches at information brokers, banks and universities that so far this year have resulted in more than 1 million Social Security numbers, driver's license numbers, names and addresses falling into the hands of potential identity thieves.''[18] In combination, these security breaches, the extensive publicity focusing upon these incidents, and federal and state legislative activity targeting privacy issues all point to stricter, more comprehensive domestic privacy requirements in the near future.

The International Expansion of Privacy Protection

The United States can hardly decouple homeland security from the international community as millions of foreign visitors and cargo tonnage routinely cross the borders. As a result, international privacy concerns and requirements inevitably become intertwined with domestic homeland security initiatives.

In addition to strict European data protection laws within the EAA, other countries (*e.g.,* Canada, Argentina, and Switzerland) have adopted comparable levels of privacy protection. Many other countries have turned to the guidelines for data protection and transfer developed by the Organisation for Economic Co-Operation and Development (OECD) in 1980 and embraced by the European Union (EU) in the Data Protection Directive. Other countries imposing substantial privacy and data control requirements include Australia, Chile, Hong Kong, Israel, Japan, New Zealand, Romania, Russia, and Taiwan. Based upon recent trends, international privacy laws will likely shift towards the OECD guidelines and/or the EAA model, thus pressuring global

---

[12] ''Controversial Terror Database Matrix Shuts Down,'' *Security Pipeline* (Apr. 19, 2005) (www.securitypipeline.com).

[13] Brief of Amici Curiae Electronic Privacy Information Center (EPIC), *Hiibel v. Sixth Judicial District Court of Nevada,* No. 03-5554 (Sup. Ct., Dec. 13, 2003).

[14] Barton, ''Controversial Terror Database Matrix Shuts Down,'' *Miami Herald* (Apr. 15, 2005) (www.miami.com/mld/miamiherald); ACLU, ''ACLU Applauds End of 'Matrix' Program'' (Apr. 15, 2005) (www.aclu.org).

[15] Goo, ''Privacy Advocates Criticize Plan to Embed ID Chips in Passports,'' *Washington Post,* p. A6 (Apr. 3, 2005).

[16] Krebs, ''Mail Tracking System Raises Privacy Fears,'' *Washingtonpost.com* (Aug. 7, 2003) (www.washingtonpost.com); 70 Fed. Reg. 22516 (2005) (''For over two centuries, the USPS has valued privacy and built a brand that customers trust'').

[17] *See, e.g., Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use: Hearings Before the Senate Judiciary Comm.,* 109th Cong., 1st Sess. (2005); *Protecting Consumers' Data: Policy Issues Raised by ChoicePoint: Hearings Before House Subcomm. on Commerce, Trade, and Consumer Protection of the Comm. on Energy and Commerce,* 109th Cong., 1st Sess. (2005).

[18] Krim, ''States Scramble to Protect Data,'' *Washington Post,* p. E1 (Apr. 9, 2005).

  FCR ISSN 0014-9063

companies and multinational organizations to adapt to more stringent standards for protecting privacy.

Increasingly, the United States will find that its Homeland security objective for information sharing will clash with international standards for privacy and data protection. For example, the EU's top justice official warned that ''We need to make sure that the right to security and the fight against terrorism . . . can be reconciled with the full protection of fundamental rights.''[19] Similarly, the German Data Protection Commissioner recently complained that ''sweeping anti-terror laws'' in Germany had ''undermined basic protection from state snooping into private lives.''[20] One of the near-term international issues pitting security against privacy will likely erupt over United States requirements for biometric passports for EU visitors.[21] Thus, both DHS and homeland security contractors will increasingly find that the price for international cooperation will include United States concessions to stricter privacy and data protection.

CONCLUSION

By law and practice, sharing information and protecting privacy are inextricably bound together in the DHS mission. To assure that overlooked privacy issues do not derail critical homeland security initiatives, both DHS and its contractors must build privacy protection into these initiatives from the beginning. At a minimum, the public and private sectors should be ready to address the types of questions posed during congressional hearings that focused upon privacy and homeland security issues:

> As government and law enforcement begin to implement new strategies using advanced technologies such as data mining, there are a number of questions and concerns that need to be addressed. These agencies will need to address how existing privacy laws would apply to their programs; what data sources do they intend to draw from; how the reliability of the data will be insured; what procedures would be in place to secure the data collected from intrusion; and what recourse would be available to an individual who believes that his or her information is inaccurate or incomplete.[22]

To reduce the risks of embarrassing publicity, program delays or cancellation, or even potential civil or criminal sanctions associated with private information being compromised, a sound privacy plan should typically address such factors as:

- *Purpose*: state the purpose for which data is collected;
- *Physical Security*: identify measures to maintain physical security of the facility housing private data;
- *Electronic Security*: establish means for maintaining cybersecurity;
- *Accuracy*: assess the accuracy of the data collected and analyzed;
- *Due Process*: provide mechanisms for correcting erroneous data;
- *Monitoring*: conduct periodic audits or reviews to enforce procedures;
- *Oversight*: consider internal and/or external oversight, such as a designated privacy officer;
- *Remedial Measures*: establish procedures for notice and safeguards in the event of a privacy breach.

In developing a privacy plan, both contracting officials and contractors should consider not only existing privacy laws, but also how to allow flexibility to adapt to new standards, as recent events and international trends foretell stricter and more comprehensive privacy requirements in the near future. While tension will always exist between the dual objectives of sharing information and protecting privacy, the success of the homeland security mission must inevitably be measured against both.

---

[19] ''EU Pledges to Protect Rights in Anti-Terrorism Fight,'' *Daily Times* (Apr. 27, 2005) (www.dailytimes.com.pk/default.asp?page=story_27-4-2005_pg4_13).

[20] ''Germany's Data Protection Head Worried,'' *Deutsche Welle* (Apr. 19, 2005) (www.dw-world.de).

[21] Rohde, ''Possible U.S.-EU Fight Looms Over Biometric Passports,'' *ComputerWorld* (Apr. 29, 2005) (www.computerworld.com).

[22] *Can the Use of Factual Data Analysis Strengthen National Security?—Part II: Hearings Before the House Subcomm. on Technology, Information Policy, Intergovernmental Relations, and Census of the Comm. on Government Reform*, 108th Cong., 1st Sess. 5 (May 20, 2003) (statement of Rep. Putnam).