

Chapter 1

The Impact of Homeland Security Initiatives on the Confidentiality of the Energy Industry’s Sensitive Business Information and the Privacy of the Energy Industry’s Customer Information¹

Susan H. Pauley
Steptoe & Johnson PLLC
Charleston, West Virginia

Synopsis

§ 1.01.	Introduction	2
§ 1.02.	Department of Homeland Security and Other Federal Agency Information Privacy Initiatives in Connection with Homeland Security Efforts.....	4
	[1] — Department of Homeland Security Privacy Officer.....	4
	[a] — Biometrics.....	5
	[b] — Radio Frequency Identification Devices (RFID).....	6
	[c] — Multi-State Anti-Terrorist Information Exchange (MATRIX).....	7
	[d] — Computer Assisted Passenger Pre-Screening System (CAPPS II).....	7
	[2] — Privacy and Civil Liberties Oversight Board	9
§ 1.03.	Potential Private Sector Information Sources for Homeland Security Efforts and Status of Private Sector Information	10
	[1] — Compelled Disclosures—Section 215 Orders	12
	[2] — Voluntary Disclosures	14
	[a] — Critical Infrastructure Information	14
	[i] — Motivation for Enactment of CIIA	15
	[ii] — Key Defined Terms within the CIIA.....	16
	[iii] — Application of the CIIA.....	18
	[iv] — Reaction to the CIIA.....	21
	[v] — State Freedom of Information Acts, Public Records Acts, and Open Records Acts	23

¹ The author would like to thank Steven P. McGowan and Robert L. Bailey of Steptoe & Johnson PLLC, Charleston, West Virginia for their editorial comments.

[b] — Personally Identifiable Information 25

 [i] — Federal Privacy Statutes 26

 [ii] — Company Privacy Policies 28

 [iii] — Common Law Invasion of Privacy 35

§ 1.04. **Data Sharing and Mining**..... 37

 [1] — What Is Data Mining? 37

 [2] — Data Mining and Homeland Security 38

§ 1.05. **Information Security** 39

 [1] — How Great Is the Threat? What Is the
 Source of the Threat? 40

 [2] — Employee Background Checks 40

§ 1.06. **Conclusion**..... 41

§ 1.01. Introduction.

In his National Strategy for Homeland Security, President George W. Bush identified four foundations on which the framework for the nation’s homeland security efforts would be based.² Information sharing and information systems are among these four foundations.³ The importance of interconnected information systems to the nation’s homeland security efforts is clear. Homeland security officials will not be able to make timely decisions or take appropriate action without access to information and an effective means by which the information can be shared.⁴

Not only is the need to share information a key component of homeland security, but there has been a recognition that adequate information privacy protections also need to be implemented in connection with the increased sharing of information. Government data mining proposals and initiatives, for instance, have pushed the antiterrorism-versus-privacy debate to the forefront. The United States will be using information, for purposes that

² Office of Homeland Security, *The National Strategy for Homeland Security* x-xii (July 2002)(hereinafter *National Strategy for Homeland Security*). “The National Strategy for Homeland Security also describes four foundations—unique American strengths that cut across all of the mission areas, across all levels of government, and across all sectors of our society.” *Id.* at x.

³ The other three foundations on which our nation’s homeland security efforts will be based are “law, science and technology, . . . and international cooperation.” *Id.*

⁴ “Information systems contribute to every aspect of homeland security.” *Id.* at xi (emphasis added).

were not anticipated when the information was collected, in connection with identifying and locating individuals suspected of terrorism and in connection with efforts to predict terrorist activity.

Importantly, the debate regarding information privacy issues associated with increased information gathering and sharing in connection with the nation's antiterrorism efforts began with the inception of the Department of Homeland Security (DHS). DHS's Chief Privacy Officer described DHS's understanding of the importance of considering the potential privacy implications of homeland security initiatives and DHS's commitment to preserving individual privacy while, at the same time, protecting the nation's security as follows:

The responsible stewardship of personal information is fundamental to the Department's successful achievement of its mission. This mission is not only to protect our people and our homeland; it is to protect our way of life. Personal privacy is central to that way of life. Privacy is a core value, universally recognized, and a value long recognized in American law and jurisprudence. Because privacy is so essential to our way of life we recognize that the protection of privacy, of the very dignity and autonomy of the individual, is not a value that can be added on to this or any other organization as an afterthought. Thus, I am so pleased that the Privacy Office has been operational within the Department of Homeland Security from its earliest days. We will continue to work to ensure that privacy is woven into the very fabric of this organization as a guiding principle and value.⁵

While the government is the repository for certain data, the private sector is also a critical, and in some cases the primary source of information about individuals and critical infrastructures. The information held by the energy industry is a prime example of information held by private sector

⁵ Letter from Nuala O'Connor Kelly, Chief Privacy Officer, United States Department of Homeland Security, Privacy Office Report to Congress April 2003 – June 2004, available at http://www.dhs.gov/interweb/assetlibrary/privacy_annualrpt_2004.pdf (hereinafter DHS Privacy Office Report).

entities that might be important for the nation's homeland security efforts. The energy industry has the potential to be a key source of information about customers due to the large number of customers it serves. For example, the United States Energy Information Administration reports that there were 134,449,825 electricity customers in 2003 of which 117,092,348 were residential customers.⁶

The private sector, and in particular those members of the private sector that might be a source of information about individuals and critical infrastructures, might receive requests from the government for information that the private sector maintains. Recipients of such requests must be careful that, in their effort to assist in the nation's homeland security efforts, they do not violate the privacy of individuals about whom they maintain information. Businesses that maintain information about critical infrastructures should also be aware of the level of protection afforded to information about critical infrastructures that they submit to DHS.

The security of the information contained in the nation's information systems, including those maintained by the private sector, will also be vital to the information sharing and systems component of the nation's antiterrorism efforts. As the collection, use, and exchange of information increases, adequate security protections will become even more critical.

**§ 1.02. Department of Homeland Security (DHS)
and Other Federal Agency Information Privacy
Initiatives in Connection with Homeland
Security Efforts.**

**[1] — Department of Homeland Security (DHS) Privacy
Officer.**

Recognizing a need since the inception of the Department of Homeland Security to consider the impact of homeland security efforts on individual privacy, Congress included language in the Homeland Security Act requiring the establishment of a comprehensive privacy operation including the establishment of the DHS Privacy Officer and the appointment of an

⁶ United States Energy Information Administration, Electricity Quick Stats, www.eia.doe.gov/neic/quickfacts/quickelectric.htm (last visited June 28, 2005).

Officer for Civil Rights and Civil Liberties.⁷ Among the responsibilities of the DHS Privacy Officer are (1) evaluating technologies (*e.g.*, biometrics; Radio Frequency Identification Devices (RFID); and the Multi-State Anti-Terrorist Information Exchange (MATRIX)) to ensure that privacy protections regarding the collection, use, or disclosure of personal information are not compromised; (2) ensuring compliance with the Privacy Act of 1974; (3) evaluating legislative and regulatory proposals that involve the federal government's collection, use, and disclosure of personal information (*e.g.*, Transportation Security Administration's (TSA) once-proposed Computer Assisted Passenger Pre-Screening System (CAPPS II)); (4) conducting privacy impact assessments of proposed DHS rules; and (5) reporting to Congress annually regarding DHS's privacy-related activities.⁸ The DHS Privacy Officer has already begun evaluating the privacy protections associated with proposed technologies and legislative and regulatory proposals. Some of these proposals have already succumbed to concerns over privacy. Some of the technologies and legislative and regulatory proposals that have been considered by the DHS Privacy Officer are described in more detail below.

[a] — Biometrics.

According to the International Biometric Industry Association, biometrics are “technologies that automatically confirm the identity of people by comparing patterns of physical or behavioral characteristics in real time against enrolled computer records of those patterns.”⁹ Biometric technolo-

⁷ Homeland Security Act, Pub. L. No. 107-296, §§ 222, 705, 116 Stat. 2155, 2219, respectively (codified at 6 U.S.C.A. § 142 (West 2005) and 6 U.S.C.A. § 345 (West 2005)). *See also* H.R. Conf. Rep. No. 108-796, 108th Cong., 2nd Sess. (2004), § 8303, § 8305 (codified at 6 U.S.C.A. § 345 (West 2005))(Officer for Civil Rights and Civil Liberties) and 6 U.S.C.A. § 142 (West 2005)(Privacy Officer), respectively).

⁸ Homeland Security Act § 222; DHS Privacy Office Report, *supra* note 5, at 2, 15-28. Pursuant to the Homeland Security Act, the DHS Under Secretary of Information Analysis and Infrastructure Protection and the DHS Chief Information Officer are responsible for ensuring that DHS treats information in DHS databases and analytical tools in accordance with federal privacy law. Homeland Security Act § 201(d)(15)(B).

⁹ International Biometric Industry Association Home Page, <http://www.ibia.org/biometrics> (last visited April 23, 2005).

gies include, for example, technologies that scan faces, fingerprints, irises, and voices.¹⁰ In recognition of the importance of identification verification technologies to the nation's homeland security efforts, the DHS Privacy Office has stated that “[t]he Department is leading the way in exploring the use of these [biometric] technologies for identification purposes.”¹¹ For example, the US-VISIT (United States Visitor Immigrant Status Indicator Technology) Program relies on the collection and use of biometric identifiers.¹² As part of its information collection activities, the US-VISIT Program collects fingerprints and digital photographs from individuals who are “nonimmigrant visa holders traveling through air and sea ports.”¹³ This information, along with other information collected as part of the program, is used to verify the identity of those individuals covered by the program as they enter or leave the United States.¹⁴

[b] — Radio Frequency Identification Devices (RFID).

Radio Frequency Identification Devices (RFID) are defined as “an analog-to-digital conversion technology that uses radio frequency waves to transfer data between a moveable item and a reader to identify, track or locate that item.”¹⁵ While RFID technology is not new, the recent focus on the issue is due to its expanded application in both the private and public sector for homeland security and other purposes. For example, RFID technology might be used in department stores to identify particular merchandise and on highways to more easily and quickly facilitate travel through tollbooths.¹⁶

The Department of Homeland Security is also using Radio Frequency Identification Devices technology.¹⁷ For example, airlines use RFID

¹⁰ *Id.*

¹¹ DHS Privacy Office Report, *supra* note 5, at 15-16.

¹² *Id.* at 16 and App. F, at 2.

¹³ *Id.* at App. F, at 2.

¹⁴ *Id.*

¹⁵ *Id.* at 17 (quoting http://www.cnet.com/video/webcast/wireless_glossary.html).

¹⁶ Federal Trade Commission, Radio Frequency Identification: Applications and Implications for Consumers 1 (March 2005), available at <http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf>.

¹⁷ *Id.* at 10.

technology to track at least some airline passenger luggage.¹⁸ Plans for expanded use of RFID technology have been met with certain concerns, including concerns over privacy. For example, the announcement of the State Department's plans to use RFID technology in passports has sparked concern over potential privacy issues.¹⁹

[c] — Multi-State Anti-Terrorist Information Exchange (MATRIX).

MATRIX was a pilot project designed to provide state and local law enforcement agencies with the ability to query existing criminal justice record systems and public and commercial databases in a timely manner.²⁰ The Multi-State Anti-Terrorist Information Exchange system included the following categories of records: pilot license information, property ownership information, Coast Guard records of registered watercraft, sexual offender lists, terrorist watch lists, corporate filings, Uniform Commercial Code filings, bankruptcy information, and professional licenses.²¹ Connecticut, Florida, Ohio, and Pennsylvania participated in the pilot project.²² The MATRIX Pilot Project ended on April 15, 2005.²³

[d] — Computer Assisted Passenger Pre-Screening System (CAPPS II).

In a further effort to improve the safety of air travel, the Transportation Security Administration attempted to develop the CAPPS II automated airline

¹⁸ *Id.*

¹⁹ See Sara Kehaulani Goo, "Privacy Advocates Criticize Plan to Embed ID Chips in Passports," *Wash. Post*, April 3, 2005, at A6.

²⁰ "MATRIX defined," http://www.matrix-at.org/matrix_defined.htm (activity of the Institute for Intergovernmental Research (last visited on April 23, 2005)(website discontinued after July 1, 2005)); see also "Frequently Asked Questions," http://www.matrix-at.org/matrix_defined.htm (last visited on April 23, 2005)(website discontinued after July 1, 2005).

²¹ "MATRIX Data Sources," http://www.matrix-at.org/data_sources.htm (last visited on April 23, 2005)(website discontinued after July 1, 2005).

²² "Participating States," <http://www.matrix-at.org/states.htm> (last visited on May 2, 2005)(website discontinued after July 1, 2005).

²³ "MATRIX," <http://www.matrix-at.org> (last visited on June 29, 2005)(website discontinued after July 1, 2005).

passenger screening system.²⁴ The original CAPPs system was limited due to its decentralized organization (*e.g.*, the Federal Aviation Administration regulated CAPPs while the airlines operated CAPPs) and its informational capacity (*e.g.*, CAPPs relied on information submitted by airline passengers to airline reservation systems but did not include access to publicly available commercial databases, international flight information from foreign carriers, or government watch list information).²⁵ The Transportation Security Administration intended to use CAPPs II to access commercial databases for the purpose of verifying individuals' identities and government databases for the purpose of determining an individual's threat score. This information would have alerted airport personnel of appropriate security procedures to follow based on the threat level.²⁶

TSA scrapped its plans to implement the CAPPs II system. One of the reasons for the demise of the CAPPs II system was the privacy firestorm that the announcement of the planned system set off.²⁷ Among the privacy concerns associated with the CAPPs II system were the system's access to personal data about individuals and the inability of travelers to challenge their risk designation.²⁸ The TSA has replaced CAPPs II with its Secure Flight program.²⁹ Under the Secure Flight program, the TSA will check airline passenger information against terrorist watch list information to determine whether additional security, including passenger screening, is needed.³⁰

²⁴ K.A. Taipale, "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data," 5 *Colum. Sci. & Tech. L. Rev.* 2, 37 (2003).

²⁵ DHS Office of Inspector General, Review of Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data (Redacted), 10 (March 2005)(hereinafter DHS OIG Report).

²⁶ Taipale, *supra* note 24, at 39.

²⁷ *See id.* at 38.

²⁸ "CAPPs II Crash-Lands. Homeland Security Cites Privacy Concerns in Canceling Airline Screening Project," *TechwebNews*, July 19, 2004, available at 2004 WLNR 4747997 (Westlaw).

²⁹ Transportation Security Administration, Secure Flight Program, www.tsa.gov/public/display?content=09000519800cf3a7 (last visited June 16, 2005)(hereinafter TSA Secure Flight Program Website Document); *see also* John M. Doyle, "TSA to Roll Out Replacement for CAPPs II Early in 2005," 3 *Aviation Week's Homeland Sec. & Defense*, Sept. 1, 2004, available at 2004 WLNR 14417241 (Westlaw).

³⁰ TSA Secure Flight Program Website Document, *supra* note 29. "The Transportation Security Administration (TSA) is developing a passenger pre-screening program called

Perhaps in part due to the privacy controversy that surrounded the CAPPs II proposal and in an effort to avoid similar criticisms, TSA has highlighted the privacy protections that are included within the Secure Flight Program in its documentation describing the Secure Flight Program.³¹

[2] — Privacy and Civil Liberties Oversight Board.

The Department of Homeland Security is not the only component of the federal government to dedicate resources to privacy issues related to its anti-terrorism activities. Other components of the executive branch have also decided to focus more attention on the issue. For example, the July 22, 2004 release of the 9/11 Commission Report generated significant national debate regarding the nation's intelligence operations. Included within the recommendations of the Commission is the recommendation that information should be subject to policy guidelines regarding the acquisition, sharing, and use of information in order to protect privacy and civil liberties.³² To ensure that privacy and civil liberty issues are adequately considered in connection with the nation's antiterrorism activities, Congress also established a Privacy and Civil Liberties Oversight Board within the Executive Office of the President.³³ Congress charged the Privacy and Civil Liberties

Secure Flight. Secure Flight involves the comparison of Passenger Name Records (PNRs) from domestic flights to names in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC). This database includes the expanded No-Fly and Selectee Lists and is used to identify individuals known or suspected to be engaged in terrorist activity." *Id.*

³¹ *Id.*

TSA is firmly committed to protecting the privacy and civil liberties of travelers. Testing of the system and eventual implementation will be governed by strict privacy protections including data security mechanisms and limitations on use, dissemination and storage of PNRs. Only TSA employees who have a "need to know" to perform their duties associated with Secure Flight will be able to see passenger information. In addition, the new program will include a redress mechanism through which people can resolve questions if they believe they are unfairly singled out for additional screening.

Id.

³² See *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States*, 418-19 (July 22, 2004).

³³ H.R. Rep. No. 108-796 (2004)(Conf. Rep.)(Conference Report for the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-485) § 1061.

Oversight Board with the responsibility of providing advice to the President and executive department and agency heads in order to ensure that privacy and civil liberties are considered in connection with the development and implementation of anti-terrorism regulations and policies.³⁴ As Part of the Intelligence Reform and Terrorism Prevention Act of 2004, Congress also recommended that every “executive department and agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer.”³⁵ As part of the 2005 Consolidated Appropriations Act, Congress has required the Departments of Transportation, Treasury, and Independent Agencies to appoint chief privacy officers and have privacy audits conducted at least every two years.³⁶

§ 1.03. Potential Private Sector Information Sources for Homeland Security Efforts and Status of Private Sector Information.

Pursuant to the Homeland Security Act, DHS has the authority to obtain information from governmental as well as private sector entities in connection with its homeland security activities. Specifically, the DHS Under Secretary for Information Analysis and Infrastructure Protection has the authority to

[A]ccess, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to –

(A) identify and assess the nature and scope of terrorist threats to the homeland;

(B) detect and identify threats of terrorism against the United States;
and

³⁴ *Id.* at § 1061(c).

³⁵ *Id.* at § 1062.

³⁶ Consolidated Appropriations Act, 2005, Pub. L. No. 108-447, 118 Stat. 2809, Division H, Title V, § 522 (2004).

(C) understand such threats in light of actual and potential vulnerabilities of the homeland.³⁷

A November/December 2002 online survey by CSO magazine of its subscribers regarding their data sharing habits with government agencies and law enforcement agencies provided an interesting insight into the frequency with which such data sharing has already occurred.³⁸ Seven hundred seventy-nine security professionals responded to the online survey.³⁹ Respondents represented federal, state, and local governments, the insurance/healthcare sector, computer companies, the financial/banking industry, the manufacturing industry, and the education sector.⁴⁰ Forty-five percent of executives responding to the survey reported that their organizations had supplied information about their customers, employees, or business partners to government agencies or law enforcement agencies.⁴¹ While nearly half of the surveyed companies reported such information sharing, 33 percent reported that they have not provided information to the government or law enforcement agencies.⁴²

While the recipients of these record requests might be attempting to assist in the nation's antiterrorism efforts, they might also be exposing themselves to privacy-related claims by voluntarily disclosing personally identifiable information. For that reason, private sector companies that maintain personally identifiable information need to be aware of the privacy protections that might apply to the disclosures of records that they maintain.

37 Homeland Security Act, Pub. L. No. 107-296, § 201(d)(1), 83 Stat. 2145 (2002)(codified at 6 U.S.C.A. § 121(d)(1)(West 2005))(emphasis added).

38 Lorraine Cosgrove Ware, "Confidence in IT Security Growing," *CSO Research Reports* (Dec. 18, 2002), available at <http://www.csoonline.com/csoresearch/report49.html> (hereinafter CSO Dec. 18, 2002 Survey Results); see also Privacy & American Business, Guide to Homeland Security Information Requirements, 35-36 (March 5, 2003)(hereinafter Guide to Homeland Security Information Requirements).

39 CSO Dec. 18, 2002 Survey Results, *supra* note 38.

40 *Id.*

41 *Id.* See also John Schwartz, "Some Companies Will Release Customer Records on Request," *N.Y. Times*, Dec. 18, 2002, at A16.

42 Guide to Homeland Security Information Requirements, *supra* note 38, at 36 (citing CSO Dec. 18, 2002 Survey Results).

Disclosures generally fall into two categories: (1) compelled disclosures; and (2) voluntary disclosures.

[1] — Compelled Disclosures—The “Section 215” Order.⁴³

In an effort to make information more readily available to the government for antiterrorism purposes, Congress included Section 215 in the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (“USA PATRIOT Act”).⁴⁴ This provision provides the Federal Bureau of Investigation (FBI) with broad authority to obtain business records.⁴⁵ Under Section 215, when the FBI is participating in terrorism and intelligence investigations, the FBI may obtain a court order to obtain privately held business records. Furthermore, the FBI is not required to specify the target of the investigation.⁴⁶

The language of Section 215 has the potential to allow the FBI to obtain a much greater amount of information than the information that could be obtained through a particularized search about an individual suspect.⁴⁷ In addition, the court to which the FBI seeks an order under Section 215, the Foreign Intelligence Surveillance Court, must grant any such FBI request as long as the request is for an authorized intelligence investigation.⁴⁸ Further-

43 Because the focus of this chapter is on voluntary disclosures of information to the federal government for homeland security purposes, the discussion of Section 215 Orders is included for illustrative purposes only. This subsection is not intended to provide a comprehensive description of all methods by which the government may compel disclosures of information from private sources.

44 USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 287 § 215 (2001)(codified at 50 U.S.C.A. § 1861 (West 2005)).

45 James X. Dempsey and Lara M. Flint, “Commercial Data and National Security,” 72 *Geo. Wash. L. Rev.* 1459, 1482 (August 2004).

46 *Id.* at 1482. “The Director of the Federal Bureau of Investigation or a designee of the Director . . . may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.” USA PATRIOT Act § 215.

47 “Broadly read, the provision allows the FBI to access an entire database of privately held information, rather than just the records of a particular suspect.” Dempsey and Flint, *supra* note 45, at 1482.

48 *Id.*

more, under the existing language of Section 215, recipients of a Section 215 request are prohibited from revealing that the FBI has sought or received information from them.⁴⁹ Persons who act in good faith to produce information are protected from liability for any such production.⁵⁰ This provision of the USA PATRIOT Act would appear to protect from liability those companies that produce information in response to a Section 215 order. Of course, this protection would not apply to voluntary disclosures. Accordingly, in order to protect themselves, some companies at a minimum get a written request while some insist on receiving a valid court order.⁵¹

According to recent testimony by Attorney General Alberto Gonzales, as of March 30, 2005, 35 requests for Section 215 orders submitted to the Foreign Intelligence Surveillance Court have been granted.⁵² Interestingly, while there has been much concern about the federal government's use of this provision to obtain information from libraries and bookstores, the Department of Justice reports that it has not used Section 215 to obtain these kinds of records.⁵³ Instead, Attorney General Gonzales has testified before the Senate Judiciary Committee that Section 215 has been used to obtain the following categories of information: "driver's license records, public accommodation records, apartment leasing records, credit card records and subscriber information, such as names and addresses for telephone numbers captured through court-authorized pen register devices."⁵⁴

Congress is currently considering the reauthorization of the USA PATRIOT Act. As part of this reauthorization process, Congress is reviewing the language of Section 215. During reauthorization hearings, Attorney General Gonzales has testified that the Department of Justice has already taken the

⁴⁹ USA PATRIOT Act § 215.

⁵⁰ "A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production." USA PATRIOT Act, § 215.

⁵¹ See Ben Worthen, "What to Do When Uncle Sam Wants Your Data? How to Serve Your Company and Your Country," *CIO Magazine*, April 15, 2003, at 56, 64.

⁵² Transcript: Senate Judiciary Hearing on the Patriot Act, April 5, 2005 (Stmt. of Attorney General Gonzales), available at <http://www.washingtonpost.com/wp-dyn/articles/A28081-2005April5.html> (last visited April 24, 2005).

⁵³ *Id.*

⁵⁴ *Id.*

position that recipients of Section 215 orders may consult with legal counsel and may pursue a legal challenge to such an order.⁵⁵ In addition, the Department of Justice has also taken the position that government requests for records under Section 215 are limited to only those records that are relevant to national security investigations.⁵⁶ Accordingly, Attorney General Gonzales has testified that the Department of Justice would support amendments to Section 215 that would clarify these provisions of Section 215.⁵⁷

[2] — Voluntary Disclosures.

[a] — Critical Infrastructure Information.

The collection of information and sharing of information, especially about critical infrastructures and resources, are indispensable elements of the nation's homeland security efforts.⁵⁸ The private sector owns and operates over 85 percent of the nation's infrastructure.⁵⁹ Because many of the nation's critical infrastructures are owned and operated by the private sector, the government must work in partnership with the private sector to obtain information about these critical infrastructures. By obtaining this information, the federal government can consolidate the information from submitters and analyze the data to identify potential threats and vulnerabilities to the nation's critical infrastructure.⁶⁰

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ Among the responsibilities of the DHS Under Secretary for Information Analysis and Infrastructure Protection is the:

develop[ment of] a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.

Homeland Security Act, Pub. L. No. 107-296, § 201(d)(5), 116 Stat. 2145 (2002)(codified at 6 U.S.C.A. § 121(d)(5)(West 2005)).

⁵⁹ United States Department of Homeland Security, Protected Critical Infrastructure Information (PCII) Program Frequently Asked Questions—for Submitters, <http://www.dhs.gov/dhspublic/display?theme=92&content=3756&print=true> (last visited April 17, 2005).

⁶⁰ *Id.*

**[i] — Motivation for Enactment of the
Critical Infrastructure Information
Act (CIIA).**

Prior to the enactment of the Critical Infrastructure Information Act (CIIA), some private sector entities had concerns about disclosing sensitive information to the federal government due to the potential use of that information against the submitter and the potential for redisclosure to the public under the Freedom of Information Act (FOIA), 5 U.S.C.A. Section 552.⁶¹ Interestingly, the Critical Infrastructure Information Act appears to have its roots in the confidential collaboration between government agencies and the computer industry during Y2K preparations.⁶² Following the Y2K collaboration, the computer industry was concerned about the potential impact of a terrorist attack on the nation's computer systems and approached members of Congress regarding legislation to authorize further confidential communications.⁶³ The scope of the term "critical infrastructure" then grew from computer systems to other areas. In an effort to encourage the sharing of such information, Congress included the Critical Infrastructure Information Act of 2002 (CIIA) within the Homeland Security Act.⁶⁴ The CIIA provides certain protections to information defined as "critical infrastructure information" that is voluntarily submitted to a covered federal agency and used by that agency for specified purposes.⁶⁵

It is also worth noting that the Critical Infrastructure Information Act operates against the backdrop of a memorandum regarding disclosures under FOIA issued by Attorney General John Ashcroft on October 12, 2001

⁶¹ See Christina E. Wells, "National Security' Information and the Freedom of Information Act," 56 *Admin. L. Rev.* 1195, 1213 (2004)("[The Commission on Critical Infrastructure Protection] further noted that, because private industry was reluctant to share information due to liability concerns and fear of losing competitive advantage, Congress should consider enacting a FOIA exemption protecting the shared material as an incentive for information exchange.").

⁶² Rena Steinzor, "Democracies Die Behind Closed Doors?: The Homeland Security Act and Corporate Accountability," 12 *Kan. J. L. & Pub. Pol'y* 641, 642-643 (2003).

⁶³ *Id.* at 643.

⁶⁴ See Homeland Security Act, §§ 211 – 215, 83, and 6 C.F.R. Part 29 (2005).

⁶⁵ See 6 U.S.C.A. § 133(a)(1)(West 2005).

(“Ashcroft Memorandum”) establishing what is referred to as the “sound legal basis” standard.⁶⁶ The memorandum, issued shortly after the events of September 11, 2001, reflected a significant change in federal FOIA policy.⁶⁷ In his memorandum, Attorney General Ashcroft stated that

“[w]hen you carefully consider FOIA requests and decide to withhold records, in whole or in part, you can be assured that the Department of Justice will defend your [FOIA] decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records.”⁶⁸

The Bush Administration’s FOIA policy articulated in the Ashcroft Memorandum also encourages federal agency personnel to consider homeland security values when making FOIA disclosure decisions.⁶⁹

[iii] — Key Defined Terms Within the Critical Infrastructure Information Act (CIIA).

Understanding the scope of the Critical Infrastructure Information Act requires addressing three defined terms: (1) “critical infrastructure information”; (2) “voluntary”; and (3) “covered Federal agency” and one term that is not defined in the CIIA, “critical infrastructure.”

“Critical Infrastructure”: At least one commentator has suggested that DHS and the courts will look to the USA PATRIOT Act for guidance regarding the definition of “critical infrastructure.”⁷⁰ Under the Critical Infrastructure Protection Act of 2001, which is included as Section 1016 of the USA PATRIOT Act, “critical infrastructure” is defined (for purposes of that section) as follows: “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic

⁶⁶ Keith Anderson, “Is There Still a ‘Sound Legal Basis?’: The Freedom of Information Act in the Post-9/11 World,” 64 *Ohio St. L.J.* 1605, 1621-1622 (2003).

⁶⁷ *Id.* at 1620-21.

⁶⁸ *Id.* at 1621 n.76 (quoting October 12, 2001 Ashcroft Memorandum).

⁶⁹ Anderson, *supra* note 66, at 1622.

⁷⁰ Steinzor, *supra* note 62, at 645-46.

security, national public health or safety, or any combination of those matters.”⁷¹ An earlier provision of the Critical Infrastructures Protection Act of 2001 identifies certain infrastructures as “critical” including “telecommunications, energy, financial services, water, and transportation sectors.”⁷²

“Critical Infrastructure Information”: Generally, “critical infrastructure information” includes information of the type that is not publicly available and is associated with critical infrastructure or protected system security.⁷³ Specifically, “critical infrastructure information” is defined as follows:

The term “critical infrastructure information” means information not customarily in the public domain and related to the security of critical infrastructure or protected systems:

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vul-

⁷¹ USA PATRIOT Act, Pub. L. No. 107-56, § 1016(e), 115 Stat. 272, 401 (2001)(codified at 42 U.S.C.A. § 5195c(e)(2005)).

⁷² USA PATRIOT Act § 1016(b)(2); *see also* Congressional Research Service, “Critical Infrastructures: What Makes an Infrastructure Critical?” 7-8 (Jan. 29, 2003), available at <http://www.fas.org/irp/crs/RL31556.pdf> (hereinafter CRS Report). The CRS Report authors cited the language in § 1016(b)(2) of the USA PATRIOT Act. The CRS Report also cites language in documentation related to the Administration’s draft legislation for establishing DHS that describes “critical infrastructures” as ““those assets, systems, and functions vital to our national security, governance, public health and safety, economy, and national morale.”” In addition, in its “National Strategy for Homeland Security,” the Administration also referred to the definition of “critical infrastructure” included in the USA PATRIOT Act. CRS Report, *supra* note 72, at 7-8.

⁷³ Homeland Security Act, Pub. L. No. 107-296, § 212(3), 83 Stat. 2145, 2151 (2002)(codified at 6 U.S.C.A. § 131(3)(West 2005)).

nerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.⁷⁴

“Voluntary” and “Covered Federal Agency”: Under the CIAA, “voluntary” means “the submittal thereof in the absence of such agency’s exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.”⁷⁵ Under the CIA, the term, “covered Federal agency,” is defined as DHS.⁷⁶

[iii] — Application of the Critical Infrastructure Information Act (CIA).

Under FOIA, the federal government must make records available to the public unless the requested information falls within one of the nine categories of exemptions.⁷⁷ Under the CIAA, critical infrastructure information that is voluntarily submitted to DHS for its use in connection with the security of the critical infrastructure is exempt from disclosure under FOIA when the information is accompanied by an “express statement” identifying information or records in the following, or substantially similar, manner: “This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of

⁷⁴ Homeland Security Act § 212(3).

⁷⁵ Homeland Security Act § 212(7)(A).

⁷⁶ Homeland Security Act § 212(2).

⁷⁷ 5 U.S.C.A. § 552(a)(West 2005); Karen E. Jones, “The Effect of the Homeland Security Act on Online Privacy and the Freedom of Information Act,” 72 *U. Cin. L. Rev.* 787, 802 (2003).

the Critical Infrastructure Information Act of 2002.”⁷⁸ An individual entity or an Information Sharing and Analysis Organization may submit CII.⁷⁹

The United States Department of Justice Office of Information and Privacy has stated that CII is exempt from FOIA disclosure under the third exemption to the FOIA, 5 U.S.C.A. Section 552(b)(3), which exempts matters that are specifically exempted from disclosure by another statute.⁸⁰ Unlike the “confidential business information” FOIA exemption, 5 U.S.C.A. Section 552(b)(4), there is no requirement that companies designating information as “critical infrastructure information” demonstrate that their submitted information qualifies for critical infrastructure information status.⁸¹

In addition, the special status afforded to critical infrastructure information provides the following further protections: (1) CII is exempt from certain restrictions regarding *ex parte* communications with decision-making officials; (2) CII may not be used by the agency or other governmental authority or third party in a civil action under federal or state law without

⁷⁸ Homeland Security Act § 214(a)(2)(A).

⁷⁹ Homeland Security Act § 212(7). An “Information Sharing and Analysis Organization” is defined as:

any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of –

(A) gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a [sic] interference, compromise, or a [sic] incapacitation problem related to critical infrastructure or protected systems; and

(C) voluntarily disseminating critical infrastructure information as to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

Homeland Security Act § 212(5).

⁸⁰ United States Department of Justice, Office of Information and Privacy FOIA Post, Critical Infrastructure Information Regulations Issued by DHS, available at www.usdoj.gov/oip/foiapost/2004foiapost6.htm (last visited June 18, 2005).

⁸¹ Steinzor, *supra* note 62, at 645.

the submitter's consent as long as the information is submitted in good faith; (3) CII may not be used or disclosed without the submitter's consent for other purposes except in connection with the investigation or prosecution of a criminal act or when the disclosure is to Congress or the Comptroller General; and (4) if CII is provided to a state or local government agency, the critical infrastructure information may not be disclosed pursuant to a law requiring such disclosure (e.g., state FOIA), otherwise be disclosed without the submitter's consent, or used for purposes other than critical infrastructure protection or investigation of criminal activity.⁸²

Furthermore, voluntary submission of such information does not constitute a waiver of any privilege or other protection otherwise provided by law (e.g., trade secret protection).⁸³ Also of importance to submitters (and others seeking information) is the CIIA exemption of critical infrastructure information from the requirements of the Federal Advisory Committee Act (FACA).⁸⁴ This Critical Infrastructure Information Act provision would protect communications between Department of Homeland Security and industry representatives from the requirements of the Federal Advisory Committee Act, including, for example, open meeting requirements.⁸⁵

Under the Critical Infrastructure Information Act, employees who knowingly make improper disclosures of critical infrastructure information are subject to criminal penalties that include fines and/or imprisonment for up to one year and removal from his/her office or employment.⁸⁶ This provision could result in unnecessary withholding of information from disclosure in order to avoid CIIA criminal penalties.⁸⁷ The Critical Infrastructure Information Act does not prohibit government entities from independently obtaining

⁸² Homeland Security Act § 214(a)(1).

⁸³ Homeland Security Act § 214(a)(1)(F).

⁸⁴ Homeland Security Act § 214(b).

⁸⁵ See James W. Conrad, Jr., American Chemistry Council, *Protection of Information from Terrorism vs. Openness of Regulatory & Safety Information: The Homeland Security Dilemma* 1, 11 (American Bar Association)(Feb. 6, 2004).

⁸⁶ Homeland Security Act § 214(f).

⁸⁷ Wells, *supra* note 61, at 1197.

critical infrastructure information.⁸⁸ Such independently obtained critical infrastructure information is not subject to the restrictions of the CIIA.⁸⁹

The application and parameters of the Critical Infrastructure Information Act do not appear to have been interpreted in any great detail in a reported court decision yet.⁹⁰ However, information is available regarding the number of submissions to the Department of Homeland Security under the Critical Infrastructure Information Act. On April 21, 2004, Robert Liscouski, Assistant Secretary for Infrastructure Protection, United States Department of Homeland Security, testified before the House Homeland Select Subcommittee on Infrastructure and Border Security and Subcommittee on Cybersecurity, Science, and Research & Development. During his testimony, Assistant Secretary Liscouski stated that two companies and two associations had submitted critical infrastructure information to DHS.⁹¹ In February 2005, DHS made additional information regarding the number of Critical Infrastructure Information Act submissions available following the initiation of legal proceedings in the D.C. Circuit Court by OMB Watch.⁹² As of February 2005, the DHS Critical Infrastructure Program reported that it has received 29 submissions, seven of which were rejected.⁹³

[iv] — Reaction to the Critical Infrastructure Information Act.

Enactment of the Critical Infrastructure Information Act has been met with certain criticism. Congressional Democrats criticized the CIIA as being overly broad and duplicative of existing Freedom of Information Act (FOIA)

⁸⁸ Homeland Security Act § 214(c).

⁸⁹ *Id.*

⁹⁰ See *In re* Utility Service Area and Infrastructure Maps, 2003 WL 21757727 (Me. P.U.C. May 7, 2003)(AT&T attempted to apply the CIIA to its submission of service area maps and key infrastructures to the Maine Public Utilities Commission (Maine PUC). However, the Maine PUC declined to apply the CIIA, reasoning that the CIIA only applies to critical infrastructure information that is voluntarily submitted to DHS rather than a state agency).

⁹¹ OMB Watch, “DHS Receives Few CII Submissions” (May 3, 2004), <http://www.ombwatch.org/article/articleprint/2150/-1/83> (last visited June 29, 2005).

⁹² OMB Watch, “DHS Finally Speaks on CII,” www.ombwatch.org/article/articleprint/2683/-1/83 (last visited on April 18, 2005)(hereinafter OMB Watch).

⁹³ *Id.*; 151 Cong. Rec. S2737 (daily ed. March 15, 2005)(statement of Sen. Leahy).

exemptions and limiting the government's right to use such information for legitimate public health and safety purposes.⁹⁴

Some commentators have questioned the application of the Critical Infrastructure Information Act protections to "information" rather than "records," which is typical under the federal FOIA.⁹⁵ A submitter could take the position that if documents contain the same information and the information is protected from Freedom of Information Act disclosure under the Critical Infrastructure Information Act, then all documents containing that information would be covered.⁹⁶ Another key area of contention is the suggestion that companies will use the Critical Infrastructure Information Act to shield themselves from liability by submitting information voluntarily and invoking the protections of the Critical Infrastructure Information Act.⁹⁷ In response to questions regarding the misuse of the CIIA, proponents argue that the CIIA does not dismiss regulated entities' obligations to report required information, that information access rights under other laws continue to exist, and that private litigants have other avenues to obtain critical infrastructure information.⁹⁸

Opponents to the Critical Infrastructure Information Act continue to try to revisit the issue. For example, Senators Patrick Leahy (D-VT) and John Cornyn (R-TX) have introduced S. 394, the "Openness Promotes Effectiveness in our National Government Act of 2005" ("OPEN Government Act of 2005") which, among other things, would require the United States Comptroller General to submit a report to Congress regarding CIIA activity. On March 15, 2005, Senators Patrick Leahy (D-VT), Carl Levin (D-MI),

⁹⁴ See Statement of Senator Patrick Leahy, The Homeland Security Department Act (Nov. 19, 2002) available at <http://leahy.senate.gov/press/200211/111902c.html> (last visited June 29, 2005); Darren W. Stanhouse, "Ambition and Abdication: Congress, the Presidency, and the Evolution of the Department of Homeland Security," 29 *N.C. J. Int'l L. & Com. Reg.* 691, 703-06 (2004).

⁹⁵ Steinzor, *supra* note 62, at 642.

⁹⁶ "This assertion will almost certainly spawn widespread litigation because the submission of a single piece of information could invalidate the use of the same information memorialized in countless other formats." Steinzor, *supra* note 62, at 642.

⁹⁷ See Conrad, *supra* note 85, at 13.

⁹⁸ *Id.*

Russ Feingold (D-WI), and Joe Lieberman (D-CT) reintroduced S. 622, the “Restoration of Freedom of Information Act of 2005” (“Restore FOIA”).⁹⁹ S. 622 would amend the Homeland Security Act of 2002 in six ways: (1) the exemption from disclosure under FOIA would only be applied to critical infrastructure “records” submitted to DHS rather than critical infrastructure “information”; (2) government agencies would be permitted to share CII records; (3) government whistleblowers would be protected instead of subject to criminal penalties; (4) civil immunity for companies voluntarily submitting critical infrastructure information would be eliminated; (5) state or local law regarding disclosures of information that state or local government agencies independently receive would not be preempted; and (6) Congress would not be restricted in its use or disclosure of critical infrastructure information that is voluntarily submitted.¹⁰⁰

**[v] — State Freedom of Information Acts,
Public Records Acts, and Open
Records Acts.**

State FOIAs may be amended to include additional exemptions from state agency disclosure for certain specific categories of information that are important for national security or antiterrorism efforts. For example, the West Virginia Freedom of Information Act, W. Va. Code Section 29B-1-1 through Section 29B-1-7, was amended in 2003 to include eight additional categories of information that are exempt from disclosure.¹⁰¹ Specifically, these eight new categories protect information with potential homeland security implications:

- (a) The following categories of information are specifically exempt from disclosure under the provisions of this article . . .

⁹⁹ Senator Leahy (D-VT) introduced the Restore FOIA during the 108th Congress. That bill, S. 609, was referred to the Senate Committee on the Judiciary. Its companion bill, H.R. 2526, was referred to the House Government Reform Committee, Subcommittee on Technology, Information Policy, Intergovernmental Relations the Census, and the following three subcommittees of the House Homeland Security Committee (Select): (1) and the Subcommittee on Infrastructure and Border Security; (2) the Subcommittee on Intelligence and Counterterrorism; and (3) the Subcommittee on Cybersecurity, Science, and Research and Development but did not receive any further attention.

¹⁰⁰ 151 Cong. Rec. S2737 (daily ed. March 15, 2005)(statement of Sen. Leahy).

¹⁰¹ See W. Va. Code § 29B-1-4 (2005).

- (9) Records assembled, prepared or maintained to prevent, mitigate, or respond to terrorist acts or the threat of terrorist acts, the public disclosure of which threaten the public safety or the public health;
- (10) Those portions of records containing specific or unique vulnerability assessments or specific or unique response plans, data, databases, and inventories of goods or materials collected or assembled to respond to terrorist acts; and communication codes or deployment plans of law enforcement or emergency response personnel;
- (11) Specific intelligence information and specific investigative records dealing with terrorist acts or the threat of a terrorist act shared by and between federal and international law-enforcement agencies, state and local law enforcement and other agencies within the department of military affairs and public safety;
- (12) National security records classified under federal executive order and not subject to public disclosure under federal law that are shared by federal agencies, and other records related to national security briefings to assist state and local government with domestic preparedness for acts of terrorism;
- (13) Computing, telecommunications and network security records, passwords, security codes or programs used to respond to or plan against acts of terrorism which may be the subject of a terrorist act;
- (14) Security or disaster recovery plans, risk assessments, tests, or the results of those tests;
- (15) Architectural or infrastructure designs, maps or other records that show the location or layout of the facilities where computing, telecommunications or network infrastructure used to plan against or respond to terrorism are located or planned to be located; and
- (16) Codes for facility security systems; or codes for secure applications for such facilities referred to in subdivision (15), subsection (a) of this section.¹⁰²

¹⁰² *Id.*

[b] — Personally Identifiable Information.

Since the tragic events of September 11, 2001, various private companies have responded to informal government requests or voluntarily disclosed customer records to law enforcement agencies. The types of organizations that have voluntarily turned over customer records have been varied.¹⁰³ The disclosure of personally identifiable information raises a number of information privacy issues.

Privacy protections in the United States are generally derived from three sources: (1) constitutional law; (2) statutory law; and (3) common law.¹⁰⁴ While the privacy protections derived from the United States Constitution may be applied to governmental activities, they do not appear to restrict the government from requesting or accessing customer databases maintained by the private sector, nor do they generally apply to the activities of the private sector.¹⁰⁵ In order to determine whether a voluntary disclosure of customer information to the government by a private entity would expose the private entity to potential liability, the private entity should first consider whether there are any statutory restrictions on such a disclosure. Second, as described in further detail below, it will be important to consider whether the entity's own privacy policy may prohibit such a disclosure. Finally, because consumers might also try to pursue a common law invasion of privacy claim in this arena, it is important to consider such claims.¹⁰⁶

¹⁰³ Worthen, *supra* note 51, at 56-66 (organizations turning over information include the Professional Association of Diving Instructors, supermarket chains, and home improvement stores).

¹⁰⁴ See Robert R. Belair and Kevin Coy, "United States Privacy Law and Policy," *The Future of Financial Privacy* 18, 30 (2000) ("When record keepers in confidential and fiduciary relationships disclose personal information without authorization, some courts have provided victims of the disclosure with a cause of action for breach of an implied promise of confidentiality.").

¹⁰⁵ See Dempsey and Flint, *supra* note 45, at 1472 ("The federal Privacy Act does not apply to governmental use of commercial databases that were collected for business purposes. The Supreme Court's reading of the Constitution does not offer guidelines for government access to data generated in the course of commercial transactions and held by private companies.").

¹⁰⁶ In addition to having personally identifiable information about customers, companies might have information about employees, vendors, and/or independent contractors. While a detailed discussion of restrictions on the disclosure employment and other records is beyond the scope of this chapter, the analysis regarding potential privacy issues associated with the

[i] — Federal Privacy Statutes.

The United States has adopted a sector-by-sector statutory approach to protecting information privacy as opposed to adopting a comprehensive legislative structure.¹⁰⁷ For example, Congress has enacted information privacy statutes with respect to the following categories of personally identifiable information that may be maintained by the private sector:

- (1) consumer reports (*i.e.*, Fair Credit Reporting Act, 15 U.S.C.A. Section 1681 *et seq.*, as amended by the Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159);
- (2) education records (*i.e.*, Family Educational Rights and Privacy Act, 20 U.S.C.A. Section 1232g);
- (3) financial information (*i.e.*, Gramm-Leach-Bliley Act, 15 U.S.C.A. Section 6801 *et seq.*);
- (4) medical records (*i.e.*, Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C.A. Section 1320d *et seq.* and the HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164);
- (5) personal information obtained online from children (*i.e.*, Children’s Online Privacy Protection Act, 15 U.S.C.A. Section 6501 *et seq.*); and
- (6) video rental/purchase records (*i.e.*, Video Privacy Protection Act of 1988, 18 U.S.C.A. Section 2710).¹⁰⁸

If the records at issue are subject to one or more privacy statutes, then disclosure in violation of the statute(s) would result in liability. However, it is not uncommon for federal privacy statutes to contain language that carves out an exception for at least certain disclosures to governmental entities.¹⁰⁹

disclosure of such information parallels, to a certain degree, the discussion herein involving disclosures of customer information. Of course, personnel files might contain a variety of types of information that might be subject to additional disclosure restrictions.

¹⁰⁷ See Belair and Coy, *supra* note 104, at 31-35.

¹⁰⁸ See *id.*

¹⁰⁹ See Dempsey and Flint, *supra* note 45, at 1476 – 1481 (citing the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Gramm-Leach-Bliley Act, HIPAA, the Family

If the use or disclosure of the records at issue is not subject to any statutory restriction, then a voluntary disclosure to the federal government for homeland security purposes would not appear to expose the entity making the disclosure to liability unless, as described below, the disclosure violates the company's privacy policy or a customer has a common law invasion of privacy claim.¹¹⁰ Utility records, for example, are not subject to federal statutory privacy law, however, they may be subject to state statutory or regulatory restrictions.¹¹¹

It is important to note that while current federal information privacy statutes might not address all or any customer records maintained by a particular company or industry, Congress continues to consider privacy legislation that could not only impose additional restrictions on categories of information already subject to restrictions but could also expand the universe of information subject to use and disclosure restrictions.¹¹²

Educational Rights and Privacy Act, and the Electronic Communications Privacy Act (some of these exceptions involve compelled disclosures (*e.g.*, disclosures compelled under the FBI's National Security Letter authority)).

¹¹⁰ Companies may also include language in their privacy policies to notify customers that disclosures may be made as permitted or as required by law in order to try to reduce the possibility of privacy-related issues or complaints associated with such disclosures.

¹¹¹ "Categories of information for which there is no applicable [federal] privacy law include, inter alia: travel records, retail purchases—online and offline—of anything ranging from books to groceries, 'Easy Pass' [sic] toll records, real estate and mortgage information, magazine subscriptions, club memberships, and utility bills." Dempsey and Flint, *supra* note 45, at 1476 (emphasis added). *See also*, New Jersey Division of the Ratepayer Advocate, Preliminary Position Paper on Consumer Protection Proposals for Electric Restructuring in New Jersey (Feb. 1998), available at <http://www.rpa.state.nj.us/consupro.htm> (last visited April 23, 2005) ("Consumers may expect that their utility billing and payment records are confidential because utilities have typically protected this information from disclosure and do not routinely sell or make available their customer-oriented research and survey results. There is no federal law, however, that compels this and, in many states, there is no statute that specifically protects such records." (emphasis added)). The author did not conduct a survey of all 50 states to determine whether customer records typically maintained by energy companies are subject to state statutory or regulatory restrictions.

¹¹² *See, e.g.*, Privacy Act of 2005, S. 116, 109th Cong. (2005) (introduced by Sen. Dianne Feinstein (D-CA)). For example, Title I of the Privacy Act of 2005 would require consumers to receive notice and an opportunity to opt-out before a commercial entity may sell (or disclose for marketing) personally identifiable information. With the exception of nonprofit organizations and entities that are subject to the Gramm-Leach-Bliley Act or HIPAA, this

On a similar note, state privacy-related statutes and regulations might impose restrictions on the private sector's use and disclosure of certain categories of personally identifiable information. Disclosures in violation of state privacy statutes might also expose companies to potential liability.¹¹³

[ii] — Company Privacy Policies.

Even if the information contained in customer databases is not subject to statutory or regulatory restrictions, companies should also make sure that they abide by any promises that they might have made to their customers regarding the collection, maintenance, use, or disclosure of customer information as posted in their privacy policies.¹¹⁴ Many organizations that collect personal information about customers have adopted privacy policies regarding their collection, maintenance, use, and disclosure of this information. The adoption of privacy policies/notices might be mandated by statute (*e.g.*, HIPAA, 42 U.S.C.A. Section 1320d *et seq.*, and the HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164); Title V of the Gramm-Leach-Bliley Act, 15 U.S.C.A. Section 6801 *et seq.*; or the Children's Online Privacy Protection Act, 15 U.S.C.A. Section 6501 *et seq.*) or organizations might adopt them voluntarily. While privacy policies might vary from organization to organization, they typically address the following issues known as "fair information practice principles": (1) notice of the entity's information practices; (2) choice/consent regarding how information collected about an individual may be used; (3) individual access to information and the right to challenge the information's accuracy and completeness; (4) integrity and security of information; and (5) enforcement of privacy policies.¹¹⁵

Federal Trade Commission Activity: Companies that adopt privacy policies might create an expectation in their customers regarding the protec-

legislation would apply across-the-board rather than to a single category of information collectors or records. *Id.* at § 104.

¹¹³ *See, e.g.*, American Public Power Association, Consumer Privacy and Public Information Issues, <http://www.appanet.org/aboutpublic/index.cfm?ItemNumber=9566&sn.ItemNumber=2102> (last visited April 28, 2005).

¹¹⁴ Companies that are subject to certain statutory restrictions regarding the use or disclosure of customer information should ensure that their privacy policies take those requirements into account.

¹¹⁵ Federal Trade Commission, Privacy Online: A Report to Congress 7-11 (June 1998) available at www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited June 29, 2005).

tions afforded to information that the companies collect. The Federal Trade Commission has pursued legal action under Section 5 of the Federal Trade Commission Act, 15 U.S.C.A. Section 45(a)(1), against companies that violate their own stated privacy policies by, for example, disclosing personal information in violation of the company's privacy policy.¹¹⁶ Individuals have also filed suit alleging violation of company privacy policies, as evidenced by the JetBlue and other litigation described below.

JetBlue: One of the most widely publicized examples of challenges to company disclosure of customer information in connection with national security/antiterrorism efforts is JetBlue's September 2002 transfer of five million records regarding over 1.5 million passengers to a government contractor.¹¹⁷ In this case, the Transportation Security Administration was involved in helping the Department of Defense and its contractor for a base security enhancement project find an airline willing to share its passenger data for this purpose.¹¹⁸ Under the Aviation and Transportation Security Act, the Transportation Security Administration is authorized to obtain airline passenger data for transportation security purposes.¹¹⁹ The Department of Homeland Security Office of Inspector General found that although the Transportation Security Administration could have done more to protect privacy, the DHS OIG did not find any "evidence of harm to individual privacy."¹²⁰ The Army Office of Inspector General conducted its own inquiry into the JetBlue data transfer.¹²¹ After being contacted by the Transportation

¹¹⁶ See, e.g., Federal Trade Commission, "Gateway Learning Settles FTC Privacy Charges – Company Rented Customer Information It Pledged to Keep Private," www.ftc.gov/opa/2004/07/gateway.htm (last visited June 29, 2005).

¹¹⁷ United States Department of Homeland Security, Privacy Office, Report to the Public on Events Surrounding jetBlue Data Transfer 5 (Feb. 20, 2004)(hereinafter DHS Report to the Public on Events Surrounding JetBlue Data Transfer). According to the DHS Office of Inspector General, JetBlue provided information about over 2.2 million passengers. DHS OIG Report, *supra* note 25, at 22.

¹¹⁸ DHS OIG Report, *supra* note 25, at 20-22.

¹¹⁹ *Id.* at 5.

¹²⁰ *Id.* at 40.

¹²¹ *Id.* at 15, n.21 (citing United States Department of Defense, Department of the Army, Office of the Inspector General, Report of Investigation 04-007, JetBlue (June 21, 2004)("The Army OIG report found that its subcontractor, Torch Concepts, did not violate the Privacy Act in its receipt and analysis of the JetBlue data.") *Id.* at 15.

Security Administration, JetBlue provided the contractor with passenger information.¹²² The contractor later purchased additional demographic information from a data aggregator.¹²³ Information from JetBlue and the data aggregator was used not only to test the base security system but was also used in connection with a process for analyzing passenger demographic information for risk assessment purposes.¹²⁴ JetBlue's data transfer was in violation of its privacy policy which stated in part that "[t]he financial and personal information collected on this site is not shared with any third parties[.]"¹²⁵

Nine class actions brought by passengers against JetBlue were consolidated in the United States District Court for the Eastern District of New York for pretrial proceedings.¹²⁶

Privacy advocacy groups have also expressed concern about the JetBlue incident. On September 22, 2003, EPIC, the Electronic Privacy Information Center, submitted a privacy complaint to the Federal Trade Commission alleging that the exchange of JetBlue's passenger data constituted a violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C.A. Section 45(a)(1).¹²⁷

¹²² DHS Report to the Public on Events Surrounding jetBlue Data Transfer, *supra* note 117, at 5.

¹²³ *Id.*

¹²⁴ *Id.* at 6.

¹²⁵ Electronic Privacy Information Center, "In the Matter of JetBlue Airways Corporation and Acxiom Corporation, Complaint and Request for Injunction, Investigation and for Other Relief," www.epic.org/privacy/airtravel/jetblue/ftccomplaint.html (last visited June 18, 2005).

¹²⁶ See *In re JetBlue Airways Corp. Privacy Litig.*, 305 F. Supp. 2d 1362 (J.P.M.L. 2004). The cases that have been consolidated for pretrial proceedings include the following: *Turrett v. JetBlue Airways Corp.* (C.D. C.A. No. 2:03-6785); *Florence v. JetBlue Airways Corp.* (E.D.N.Y. C.A. No. 1:03-4847); *Richman v. JetBlue Airways Corp.* (E.D.N.Y. C.A. No. 1:03-4859); *Hakim v. JetBlue Airways Corp.* (E.D.N.Y. C.A. No. 1:03-4895); *Seidband v. JetBlue Airways Corp.* (E.D.N.Y. C.A. No. 1:03-4933); *Block v. JetBlue Airways Corp.* (E.D.N.Y. C.A. No. 1:03-4963); *Singleton v. JetBlue Airways Corp.* (E.D.N.Y. C.A. No. 1:03-5011); *Fleet v. JetBlue Airways Corp.* (E.D.N.Y. C.A. No. 1:03-5017); and *Mortenson v. JetBlue Airways Corp.*, (E.D.N.Y. C.A. No. 1:03-5209). (These cases are cited in *In re JetBlue Airways Corp. Privacy Litig.*, 305 F. Supp. 2d 1362 at Schedule A).

¹²⁷ "EPIC Submits Privacy Complaint to FTC Regarding JetBlue" (September 22, 2003), available at www.techlawjournal.com (last visited June 29, 2005); see also "EPIC's Complaint and Request for Injunction, Investigation and for Other Relief," available at www.epic.org/privacy/airtravel/jetblue.ftccomplaint.html. (last visited June 18, 2005).

The JetBlue incident also resulted in a Department of Homeland Security review regarding the propriety of the Transportation Security Administration's actions.¹²⁸ The Department of Homeland Security made the following five conclusions regarding the incident, focusing to a large extent on the Transportation Security Administration's involvement: (1) because data was not provided directly to TSA or its parent agency, the United States Department of Transportation, TSA employees did not violate the Privacy Act; (2) while other data analysis programs might have benefited from the data exchange, the principal purpose for the data exchange was the "Base Security Enhancement Project"; (3) Transportation Security Administration employees were clearly involved in the data exchange by facilitating the contact between JetBlue and the Department of Defense and failing to identify privacy implications of the data exchange; (4) the Transportation Security Administration's involvement in the data exchange was essential because it appears that JetBlue would not have participated in the data exchange without TSA involvement; and (5) the data exchange exceeded the Privacy Act principle restricting agency data collection to that information necessary to carry out TSA's mission.¹²⁹

The focus on government access to and use of private-sector databases has also resulted in the introduction of federal legislation that would impose a reporting requirement on federal agencies with law enforcement or intelligence responsibilities regarding their use of private sector and public databases. S. 1484, the "Citizens' Protection in Federal Database Act," which was introduced by Senator Ron Wyden (D-OR) during the 108th Congress also would have required these agencies to report as to what privacy protections, if any, are provided to the record subjects and would have prohibited database searches based only on hypothetical situations.¹³⁰

Other Airlines: JetBlue is not the only airline to face litigation as a result of disclosures of its passenger information in connection with homeland security activities. For example, Northwest Airline passengers filed suit

¹²⁸ DHS Report to the Public on Events Surrounding JetBlue Data Transfer, *supra* note 117, at 8-9.

¹²⁹ *Id.*

¹³⁰ 149 Cong. Rec. S10149-10151 (daily ed. July 29, 2003)(statement of Senator Wyden and text of S. 1484).

against the airline alleging that the airline disclosed passenger name records (PNRs) to the National Aeronautical and Space Administration (NASA) for a NASA study about airline security.¹³¹ “PNRs” consist of “electronic records of passenger information . . . contain[ing] information such as a passenger’s name, flight number, credit card data, hotel reservation, car rental, and any traveling companions.”¹³² Plaintiffs filed suit under the following eight legal theories: (1) the Electronic Communications Privacy Act, 18 U.S.C.A. Section 2701 *et seq.*; (2) the Fair Credit Reporting Act, 15 U.S.C.A. Section 1681 *et seq.*; (3) the Minnesota Deceptive Trade Practices Act, Minn. Stat. Section 325D.44; (4) common law invasion of privacy; (5) trespass to property; (6) negligent misrepresentation; (7) breach of contract; and (8) breach of express warranties.¹³³ The United States District Court for the District of Minnesota granted Northwest’s motion to dismiss with respect to all of plaintiffs’ counts.¹³⁴ Those portions of the court’s decision addressing the invasion of privacy and breach of contract claims are instructive for purposes of this chapter.

Plaintiffs’ invasion of privacy claim alleged that Northwest’s disclosure of PNRs to NASA constituted an intrusion upon their seclusion.¹³⁵ The court granted Northwest’s motion to dismiss plaintiffs’ invasion of privacy claim after determining that Northwest’s disclosure of this information to NASA would not be highly offensive to a reasonable person.¹³⁶ The court considered the following three factors in reaching that conclusion:

- (1) The plaintiffs voluntarily provided information about themselves to Northwest.¹³⁷

¹³¹ *In re Northwest Airlines Privacy Litig.*, 2004 WL 1278459 (D. Minn. June 6, 2004)(mem. & order)(consolidation of seven putative class actions).

¹³² *Id.* at *1.

¹³³ *Id.*

¹³⁴ *Id.*

¹³⁵ *Id.* at *5. “Intrusion upon seclusion exists where someone ‘intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person.’” *Id.* (quoting *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 233 (Minn. 1998)(quoting Restatement (Second) of Torts § 652B)).

¹³⁶ *In re Northwest Privacy Litig.*, 2004 WL 1278459 (D. Minn. June 6, 2004)(Mem. & Order) at *5.

¹³⁷ *Id.*

(2) While Northwest had a privacy policy posted on its website, plaintiffs apparently did not read the privacy policy before providing information to Northwest. As a result, the court determined that their expectations of privacy regarding the information were low.¹³⁸

(3) The court also took into account the fact that the disclosure was not made to the general public.¹³⁹ Furthermore, the court seemed to look favorably on Northwest's motives for disclosing the information to NASA. (*i.e.*, disclosure to a government agency for airline security purposes).¹⁴⁰

Plaintiffs' breach of contract claim was equally unsuccessful. Plaintiffs contended that Northwest's privacy policy constituted a contract between Northwest and its customers and that Northwest's disclosure of PNRs constituted a breach of the provision in the privacy policy that stated: "When you reserve or purchase travel services through Northwest Airlines nwa.com Reservations, we provide only the relevant information required by the car rental agency, hotel, or other involved third party to ensure the successful fulfillment of your travel arrangements."¹⁴¹

The court based its dismissal of the plaintiffs' breach of contract claim on the following three findings: (1) the privacy policy did not constitute a contract between Northwest and its customers, but was a general statement of company policy; (2) Northwest retained discretion regarding disclosures of the information to third parties; and (3) because plaintiffs never read the privacy policy, plaintiffs' breach of contract claim is missing a critical component—the acceptance of the contract by plaintiffs.¹⁴² The court added that even if the privacy policy constituted a contract and plaintiffs read the privacy policy before supplying their information to Northwest, plaintiffs' breach of contract claim would likely fail as a matter of law because plaintiffs

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.* (citing Complaint).

¹⁴² *In re Northwest Privacy Litig.*, 2004 WL 1278459 (D. Minn. June 6, 2004)(Mem. & Order) at *6.

did not allege any contractual damages.¹⁴³ This decision would not appear to eliminate the possibility that under a different set of facts, a breach of contract claim might be successful.¹⁴⁴

In *In re American Airlines Inc., Privacy Litigation*, the United States District Court for the Northern District of Texas dismissed the plaintiffs' putative nationwide class actions for damages allegedly resulting from American's disclosure of passenger information to TSA without passenger consent.¹⁴⁵ On its website privacy policy, American stated that it did not sell customer information or disclose customers' email addresses unless required by law and it did not disclose customer information to its affiliates or unaffiliated third parties except to fulfill customer product or service requests or for tax, security, or regulatory purposes, as required by law.¹⁴⁶ In June 2002, American provided 1.2 million passenger name records (PNRs) to TSA.¹⁴⁷ While denying the disclosures at first, American finally admitted that it had authorized the disclosure to TSA.¹⁴⁸ The defendants filed a motion to dismiss the plaintiffs' claims. The plaintiffs' claims included allegations that the disclosure of the passenger information constituted a violation of the Electronic Communications Privacy Act (ECPA) and various state-based causes of action including trespass to property, invasion of privacy, and deceptive trade practices, and resulted in unjust enrichment.¹⁴⁹ The court granted the motions to dismiss, rejecting the plaintiffs' ECPA-based arguments and finding that the state-based claims were expressly preempted by the Airline Deregulation Act (ADA) because they were related to American's

¹⁴³ *Id.*

¹⁴⁴ See also *Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196 (D. N.D. 2004) (Plaintiffs' Electronic Communications Privacy Act and breach of contract causes of action against Northwest were dismissed without prejudice).

¹⁴⁵ *In re Am. Airlines Inc., Privacy Litig.*, 370 F. Supp. 2d 552, 555 (N.D. Tex. 2005) (includes the following cases consolidated for pretrial proceeding purposes: *Rosenberg v. AMR Corp.* (N.D. Tex. C.A. No. 3:05-CV-1040-D); *Kimmell v. AMR Corp.* (N.D. Tex. C.A. No. 3:04-CV-0750-D); and *Baldwin v. AMR Corp.* (N.D. Tex. C.A. No. 3:04-CV-1148-D)).

¹⁴⁶ *In re Am. Airlines Inc., Privacy Litig.*, 370 F. Supp. 2d at 556.

¹⁴⁷ *Id.*

¹⁴⁸ *Id.*

¹⁴⁹ *Id.* at 554, 563.

ticketing services and its reservation services.¹⁵⁰ With respect to the plaintiffs' breach of contract claims, the court determined that those claims were neither expressly nor implicitly preempted by the ADA.¹⁵¹ However, the court rejected the plaintiffs' breach of contract claims due to plaintiffs' failure to sufficiently plead contract damages in their complaint.¹⁵² The court did grant plaintiffs' request for leave to amend their complaint.¹⁵³ The court noted that "plaintiffs may have little difficulty remedying the pleading deficiency in their breach of contract claim."¹⁵⁴

[iii] — Common Law Invasion of Privacy.

Plaintiffs might also pursue a common law invasion of privacy claim following a company's allegedly improper disclosure of personal information. Common law invasion of privacy claims fall into one of four categories: (1) intrusion upon seclusion; (2)(mis)appropriation of name or likeness; (3) unreasonable publicity of an individual's private life; and (4) publicity that unreasonably places an individual in a false light.¹⁵⁵

¹⁵⁰ *Id.* at 554, 561, 563-565.

¹⁵¹ *Id.* at 566.

¹⁵² *Id.* at 567.

¹⁵³ *Id.*

¹⁵⁴ *Id.* at 568.

¹⁵⁵ Restatement (Second) of Torts § 652A (2005). One might be liable under an "intrusion upon seclusion" theory if "[o]ne intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offense to a reasonable person." Restatement (Second) of Torts § 652B (2005). An "appropriation of name or likeness occurs when "one appropriates to his own use or benefit the name or likeness of another." Restatement (Second) of Torts § 652C (2005). The "publicity given to private life" invasion of privacy cause of action involves "[o]ne who gives publicity to a matter concerning the private life of another . . . if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." Restatement (Second) of Torts § 652D (2005). Finally, liability might be imposed under a "false light" common law invasion of privacy claim when one "gives publicity to a matter concerning another that places the other before the public in a false light . . . if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed." Restatement (Second) of Torts § 652E (2005).

Some commentators have taken the position that common law invasion of privacy claims are unlikely to apply to disclosures by companies of information about their customers derived from customer transactions.¹⁵⁶ Under this theory, there is no privacy invasion because consumers implicitly consent to the collection of data about them by participating in the transaction.¹⁵⁷

Surprisingly, most of the collection of personal information occurs in an area that is usually beyond legal debate—within the collectors' property, and when gathering information regarding the collector's clients, employees and customers. Those individuals subject to collection, such as shoppers identifying themselves through the use of a supermarket club membership card, may be irritated and frustrated by the surveillance to which they are subject but have a very weak claim of breach of their perceived privacy. This is because their entrance into the collector's domain (both on and off line) could be construed as implied consent to any form of surveillance or information collection.¹⁵⁸

Of course, there might be an exception to that general rule in those situations in which the company has created an expectation of privacy in such information (*i.e.*, through its privacy policy). While some commentators dismiss the possibility of a successful common law invasion of privacy cause of action, it is possible that with the right set of facts, such a claim might be successful. If nothing else, companies against which such lawsuits might be filed will have to spend valuable time and resources defending such lawsuits. As described above, the plaintiffs who sued Northwest Airlines, although unsuccessful, included a common law invasion of privacy claim (*i.e.*, intrusion upon seclusion) against Northwest.¹⁵⁹

¹⁵⁶ See Tal Z. Zarsky, "Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society," 56 *Me. L. Rev.* 13, 20 (2004).

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*

¹⁵⁹ *In re Northwest Airlines Privacy Litig.*, 2004 WL 12778459, at *5.

§ 1.04. Data Mining.**[1] — What Is Data Mining?**

While collecting and aggregating data is important to homeland security efforts, the ability to analyze and use the data as a predictor of terrorist activity is also critical. Accordingly, various government agencies are participating in and/or considering “data mining” projects. “Data mining” has been defined as “the application of database technology and techniques — such as statistical analysis and modeling — to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results.”¹⁶⁰ “Data mining” has also been described as:

the process of looking for new knowledge in existing data. The basic problem addressed by data mining is turning low-level data, usually too voluminous to understand, into higher forms (information or knowledge) that might be more compact (for example, a summary), more abstract (for example, a descriptive model), or more useful (for example, a predictive model). At the core of the data mining process is the application of data analysis and discovery algorithms to enumerate and extract patterns from data in a database.¹⁶¹

Federal government agencies use data mining for a number of different purposes, including antiterrorism activities.¹⁶² In a recent survey of federal government agencies by the United States General Accounting Office (GAO), the GAO reported that of 128 federal departments and agencies participating in the survey, 52 of those agencies already use or are planning to use data mining.¹⁶³ These agencies participating in data mining reported 131 operational data mining projects and 68 planned data mining projects.¹⁶⁴ Of the combined 199 planned or operational data mining activities, 122 reportedly used personal information.¹⁶⁵ While most of the federal government data

¹⁶⁰ United States General Accounting Office, *Data Mining: Federal Efforts Cover a Wide Range of Uses*, 1 (May 2004)(hereinafter *GAO Data Mining Report*).

¹⁶¹ Taipale, *supra* note 24, at 22.

¹⁶² *GAO Data Mining Report*, *supra* note 160, at 2-3.

¹⁶³ *Id.* at 2.

¹⁶⁴ *Id.*

¹⁶⁵ *Id.* at 3.

mining projects are designed to improve service or to detect fraud and abuse, since the events of September 11, 2001, there has been an increased focus on the use of data mining for antiterrorism activities.¹⁶⁶ Additionally, agencies from all levels of government have indicated that they are interested in incorporating commercial databases in their data mining efforts.¹⁶⁷

[2] — Data Mining and Homeland Security

Pursuant to the Homeland Security Act, the DHS Under Secretary for Information Analysis and Infrastructure Protection (“Under Secretary”) is required to establish and utilize data mining technology for purposes of analyzing data in furtherance of DHS’s responsibilities.¹⁶⁸ Specifically, the Under Secretary’s responsibility with respect to data mining is described as follows:

To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including datamining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.¹⁶⁹

The use of data mining technology is controversial because it involves the aggregation of data and the use of data from multiple sources for purposes other than that for which the information was originally collected. In fact, the use of data mining technology to predict terrorist activity without any specific suspicion is particularly troubling to privacy advocates.¹⁷⁰ Additional privacy concerns related to data mining have been identified as including the following: the quality and accuracy of the underlying data; collection of data for one purpose and use for another purpose; activities resulting in

¹⁶⁶ *Id.* at 5, 8.

¹⁶⁷ *Id.* at 5.

¹⁶⁸ See Homeland Security Act, Pub. L. No. 107-296, § 201(d)(14), 116 Stat. 2145 (codified at 6 U.S.C.A. § 121(d)(14)(West 2005)).

¹⁶⁹ *Id.*

¹⁷⁰ Taipale, *supra* note 24, at 50.

the unauthorized access, modification or disclosure of the information; and customary individual rights afforded to individuals about whom personal information has been collected including notice of data collection activities, access rights, and the right to request that inaccurate information be amended.¹⁷¹ In response to concerns over the use of data mining by DHS, Congress included language in the DHS Appropriations FY05 legislation requiring DHS to report on its use and/or development of data mining technology including an “assessment of the likely impact of the implementation of the technology on privacy and civil liberties” within 90 days of the end of fiscal year 2005.¹⁷²

Concerns over privacy have already proved to be a stumbling block for at least one government data mining program: the Defense Advanced Research Project’s Terrorism Information Awareness (TIA) project.¹⁷³ The TIA project would have allowed certain government agencies to access government and commercial databases in an attempt to identify patterns and relationships characteristic of terrorists.¹⁷⁴ Critics of TIA considered the program to be a veiled attempt to build dossiers on 300 million Americans or as an attempt to build a “supercomputer” of information about individuals.¹⁷⁵

§ 1.05. Information Security.¹⁷⁶

Protecting critical energy infrastructures, including databases and computer systems associated with such critical infrastructures, from information system security breaches is an important component of the nation’s homeland security efforts. While information privacy and security are not synonymous, they are both critical components of a strategy to protect the accuracy and integrity of information contained in private sector databases that might be of interest for homeland security purposes. One of the greatest threats to

¹⁷¹ GAO, *supra* note 160, at 6.

¹⁷² H.R. Rep. No. 108-774, at 30 (Conf. Rep. for DHS Appropriations Act, 2005, Pub. L. No. 108-334).

¹⁷³ Taipale, *supra* note 24, at 39.

¹⁷⁴ *Id.* at 40.

¹⁷⁵ *Id.*

¹⁷⁶ While an entire chapter could be written on information security, an in-depth discussion of information security is beyond the scope of this chapter. However, a few general observations are included to enhance the discussion of the information privacy issues discussed herein.

information system security might not be from outside sources, but might be from company personnel.

[1] — How Great Is the Threat? What Is the Source of the Threat?

According to a recent survey, 75 percent of companies have reported a serious data leak in the past year.¹⁷⁷ Sixty-nine percent of companies attribute their serious data leaks to employee actions.¹⁷⁸ Nearly 40 percent of companies participating in the survey reported that their leading security breach was attributable to employee error.¹⁷⁹ By contrast, external causes were responsible for only 16 percent of serious data leaks (*e.g.*, hackers).¹⁸⁰

[2] — Employee Background Checks.

Recognizing the potential threat to the security of critical infrastructures from those within the facilities (*e.g.*, critical infrastructure employees), the Department of Homeland Security has been tasked with reviewing the current status of background checking for critical infrastructure personnel and to propose national background check standards for individuals in these industries.¹⁸¹ As part of this effort, private sector representatives will work with representatives from federal, state, and local governments to consider whether there are any legal or policy impediments to establishing these national background check standards.¹⁸² This effort is likely to set off a significant debate about a variety of privacy-related issues, including, for example, what information sources might be used to conduct background checks; what background checking methods will be used; what criteria will be used to determine qualified applicants; who will be responsible for determining whether an individual's background check meets established criteria; and subsequent uses for such information.

¹⁷⁷ "Leading Cause of Data Security Breaches are Due to Insiders, Not Outsiders," *DMReview* (citing (2005) Ponemon Institute's Survey on Data Security Breaches) available at www.dmreview.com/article_sub.cfm?articleID=101928 (last visited June 29, 2005).

¹⁷⁸ *Id.*

¹⁷⁹ *Id.*

¹⁸⁰ *Id.*

¹⁸¹ National Strategy for Homeland Security, *supra* note 2, at 34.

¹⁸² *Id.*

§ 1.06. Conclusion.

Information systems and information sharing are key components of the nation's homeland security efforts. The federal government has made a commitment to integrate privacy protections into its homeland security efforts. The federal government (particularly, DHS) has dedicated resources to protecting the nation from future terrorist attacks while at the same time preserving individual privacy. Remarkably, information privacy, which was once considered a back-burner issue, has become a formidable force in the homeland security arena. Proposed programs that could have had significant homeland security implications have faltered due to the negative impact they might have had on individual privacy.

Undoubtedly, the private sector is a key component to the nation's homeland security efforts. Among other things, the private sector might be a source for personally identifiable information about individuals (*e.g.*, customers, employees) and a source (if not the only source) for critical infrastructure information. While critical infrastructure organizations might want to assist in the nation's homeland security efforts by, among other things, providing the government with access to their information, critical infrastructure companies should consider any potential liability that might arise as a result of their disclosure of information to the government before disclosing any information.

