E&MLF

CITE AS
26 *Energy & Min. L. Inst.* ch.1 (2005)

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 Information[1]

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).