

**DEPARTMENT OF HOMELAND SECURITY****Office of the Secretary****Public Workshop: Privacy and Technology: Government Use of Commercial Data for Homeland Security**

**AGENCY:** Privacy Office, Department of Homeland Security.

**ACTION:** Notice announcing public workshop.

**SUMMARY:** The Department of Homeland Security Privacy Office will host a public workshop, "Privacy and Technology: Government Use of Commercial Data for Homeland Security," to explore the policy, legal, and technology issues associated with the government's use of personally identifiable commercial data in protecting the homeland.

**DATES:** The workshop will be held on September 8, 2005, from 8 a.m. to 4:30 p.m. and on September 9, 2005, from 8:30 a.m. to 12:30 p.m.

**ADDRESSES:** The Privacy and Technology Workshop will be held in the auditorium at the DHS Offices at the GSA Regional Headquarters Building located at 7th and D Streets, SW., Washington, DC 20024.

**FOR FURTHER INFORMATION CONTACT:** Toby Milgrom Levin, Robyn Kaplan, Kenneth Mortensen, or Peter Sand at Privacy Workshop, Privacy Office, Department of Homeland Security, Arlington, VA 22202, by telephone 571-227-3813, by facsimile 571-227-4171, or by e-mail at [privacyworkshop@dhs.gov](mailto:privacyworkshop@dhs.gov).

**SUPPLEMENTARY INFORMATION:****Workshop Goals**

The Department of Homeland Security (DHS) Privacy Office is holding

a public workshop to explore the policy, legal, and technology issues surrounding the government's use of personally identifiable commercial data for homeland security. The program will include a broad range of experts and perspectives, including representatives from academia, business leaders, privacy advocates, legal experts, technologists, and policy leaders. In addition to the panel discussions, time will be allotted during the workshop for questions and comments from the audience that may be directed to each panel.

### Reason for the Workshop

The government's use of technology to access and analyze vast amounts of personally identifiable data collected by companies and data aggregators raises important privacy concerns. The DHS Privacy Office is holding this workshop to inform the Privacy Office, DHS, and the public about the policy, legal, and technology issues surrounding the government's access and use of such information for counterterrorism and how to protect privacy given the government's need for better data analysis.

Commercially available personal information ranges from directory information, such as individual names, addresses, and telephone numbers, to records of retail purchases, including travel, insurance, and financial data, to public record information obtained from Federal, state, and local offices, including court documents, professional licenses, and property records.

A number of reports have been issued urging that the government adopt standards for using such information for intelligence analysis, including the Department of Defense, Technology and Privacy Advisory Committee (TAPAC) Report and the two reports of the Markle Foundation's Task Force on National Security in the Information Age.<sup>1</sup> This workshop is intended to provide a forum for considering such standards as well as for examining whether and how information technology and commercial data can help improve national security. Finally, the workshop will look at technologies to aid in data analysis and

information management that are more privacy protective.

### The Workshop

The program will begin with a discussion of how government agencies are using personally identifiable commercial data in homeland security. Among the questions that we may examine are: What types of personally identifiable commercial data are being used; what are the benefits of using such data; what commercial data is needed to help identify terrorists; can commercial data be used to reduce the incidence of false positives, and if so, what data is needed to do so; and how accurate is commercial data for such purposes.

The second topic will address the privacy and legal issues raised by government use of commercial data. This panel will explore the adequacy of current laws, particularly the Privacy Act of 1974, to protect against government abuses when using commercial data. The panel will also examine the privacy implications of government's use of commercial data and whether there should be any limitations or protections. The panel may also discuss whether there are international laws and standards that can provide models for protecting privacy in this context.

The third panel will focus on current and developing technologies to aid the government in analyzing data for homeland security. This panel will examine the technologies government agencies are using to access and process data and whether such uses raise privacy concerns. The panel may also discuss how to evaluate the quality of such technologies, the accuracy of the underlying data, and whether further research is needed before agencies invest in such technologies.

The fourth panel will examine how technology can help protect individual privacy while enabling government agencies to analyze data. This panel will review privacy-enhancing technologies (PETs) that enable data analysis without disclosing the identity of individuals by using de-identified or anonymized data. In addition, the technologists will discuss how matching, linking, and knowledge discovery can be done in a more privacy-sensitive manner.

The final panel will build on the discussion of the previous panels to develop a recommended roadmap for DHS on building privacy protections into information programs that use commercial data. This closing panel will discuss options concerning privacy protective rules and standards DHS can adopt without waiting for changes in law. The panel may also consider how

technology can be used as a governance tool to ensure that the agency's privacy policies are implemented.

### Registration Information

The workshop is open to the public and there is no fee for attendance. For general security purposes, all attendees will be required to show a valid form of photo identification, such as a driver's license, to enter the building.

The Privacy Office will accept registration for this workshop. Registration is not necessary to attend, but is encouraged so that we may better plan this event. To register, please send an e-mail to the e-mail box for the workshop, [privacyworkshop@dhs.gov](mailto:privacyworkshop@dhs.gov), indicating your intent to attend. The Privacy Office will not retain your e-mail or e-mail address. For additional information, including routine uses permitted by the Privacy Act, see the DHS Privacy Policy on the DHS Web site at <http://www.dhs.gov/dhspublic/privacy.jsp>.

The Privacy Office will post additional information about the workshop, including a detailed agenda, on the DHS Privacy Office Web site at <http://www.dhs.gov/privacy> prior to the event. A transcript of the workshop will be posted shortly after the workshop.

Dated: July 25, 2005.

**Nuala O'Connor Kelly,**  
*Chief Privacy Officer Department of  
Homeland Security.*

[FR Doc. 05-15488 Filed 8-4-05; 8:45 am]

BILLING CODE 4410-10-P

<sup>1</sup> Technology and Privacy Advisory Commission, *Safeguarding Privacy in the Fight Against Terrorism* (2004) available at <http://www.sainc.com/tapac/finalreport.htm>; Markle Foundation, Task Force on National Security in the Information Age, *Creating a Trusted Information Network for Homeland Security* (2003); Markle Foundation, Task Force on National Security in the Information Age, *Protecting American's Freedom in the Information Age* (2002). The Markle reports are available at <http://www.markle.org>.