WRITTEN STATEMENT

OF

HUGO TEUFEL III
CHIEF PRIVACY OFFICER
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS AND
NATIONAL ARCHIVES

FOR A HEARING ENTITLED:

PRIVACY: THE USE OF COMMERCIAL INFORMATION RESELLERS BY FEDERAL AGENCIES

MARCH 11, 2008

Introduction

Chairman Clay, Ranking Member Turner, and Members of the Subcommittee, I thank you for the opportunity to address the Subcommittee on Information Policy, Census and National Archives, on efforts of the Department of Homeland Security to promote privacy protections within Department programs, particularly those utilizing personally identifiable information (PII) obtained from commercial sources.

On April 4, 2006, the then Acting Chief Privacy Officer, Maureen Cooney, appeared before a Subcommittee of the House Judiciary Committee to address the uses of information acquired from commercial information resellers, following the issuance of a Government Accountability Office Report entitled "PERSONAL INFORMATION: Agency Reseller Adherence to Key Privacy Principles."[1] During her testimony, Ms. Cooney outlined the procedures then in place to understand the uses of commercially available information in the Department, and to identify and mitigate the privacy concerns raised by that use. She also outlined additional steps the Department planned in order to foster the effective use of commercial data in a manner that respects individual privacy interests.

Although the basic framework is the same today, the Privacy Office has made a number of improvements to the process to ensure that information obtained from information resellers will be used in accordance with the Fair Information Practice Principles (FIPPs), which overarch all DHS uses of information, however obtained. Therefore, my testimony will focus on the Privacy Office's robust privacy compliance program and update the Subcommittee on enhancements made since 2006 to understand and evaluate the use of commercial data in DHS programs.

Use of Commercially Available Data by DHS

As an initial matter, it is important to acknowledge that GAO accurately described the uses of commercial information in DHS programs in its 2006 report. Although the specific contract amounts and other particulars may be slightly out of date today, the report shows that a number of components use commercially available PII, including Immigration and Customs Enforcement, Customs and Border Protection, U.S. Citizenship and Immigration Services, the Transportation Security Administration, U.S. Secret Service, the Federal Emergency Management Agency, Office of Inspector General, U.S. Coast Guard, and the Federal Law Enforcement Training Center. As noted in the report, moreover, the three principal uses of this commercial data at the

[1] GAO-06-421, April 2006.

Department support (1) law enforcement, (2) counterterrorism, and (3) fraud detection and prevention missions.

Government use of commercial data aggregators may pose particular privacy concerns, because the information was initially compiled for commercial purposes and not for government purposes. Commercial purposes may have different acceptable levels of accuracy. The need for accuracy is lower, for example, for a company mailing a catalog than for the government relying on information to issue a government-issued credential. The impact to the individual for inaccuracy in a commercial setting can be lower than in a government setting, as well.

In recognition of this fact, the Privacy Office first held a Privacy and Technology Public Workshop on September 8 and 9, 2005, which Ms. Cooney highlighted in her testimony in April 2006. The workshop focused on the government's use of commercial data and its associated privacy concerns. We also committed the question to our panel of outside experts serving on the Data Privacy and Integrity Advisory Committee (DPIAC).

Efforts of the Data Privacy and Integrity Advisory Committee

The DPIAC was established under the Federal Advisory Committee Act (5 U.S.C. App.) to advise the Secretary and the Chief Privacy Officer on the privacy implications of DHS programs.

Given the importance of understanding the privacy issues surrounding the use of PII obtained from commercial information resellers, the Privacy Office twice tasked the DPIAC to provide recommendations on how to apply the FIPPs to this practice.

On September 28, 2005, the DPIAC issued a report entitled "The Use of Commercial Data to Reduce False Positives in Screening Programs."[2] The committee recommended that commercial data be used for screening programs only when:

- It is necessary to satisfy a defined purpose
- The minimization principle is used
- Data quality issues are analyzed and satisfactorily resolved
- Assess to the data is tightly controlled
- The potential harm to the individual from a false positive misidentification is substantial
- Use for the secondary purpose is tightly controlled
- Transfer to third parties is carefully managed
- Robust security measures are employed
- The data are retained only for the minimum necessary period of time
- Transparency and oversight are provided

[2] DPIAC Report No. 2005-01, available from http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_1streport.pdf; Internet; accessed 5 March 2008.

- The restrictions of the Privacy Act are applied, regardless of whether an exemption may apply
- Simple and effective redress is provided
- Less invasive alternatives are exhausted

When these recommendations proved valuable, the Privacy Office asked the DPIAC to expand the scope of its examination to include the full range of DHS programs using commercial data, in addition to screening programs. On December 6, 2006, the committee issued a report entitled "Use of Commercial Data."[3] After advocating universal application of the recommendation from its screening report, the committee offered the following additional recommendations:

- The definition of Commercial Data should not exclude the following: (a) Publicly Available Data, data in the public domain that can be obtained or accessed from publicly accessible sources, both public and private; and (b) Public Record Data, data collected and maintained by a government entity for a public purpose and used outside of that public purpose.
- DHS should publish System of Records Notices (SORNs) for new or revised systems of records that use Commercial Data in a systematic manner or where there is substantial risk of harm.
- Apply Privacy Impact Assessments (PIAs) to programs that use Commercial Data, where the Privacy Threshold Analysis (PTAs) shows Commercial Data is used systematically or where there is substantial risk of harm.
- Revise the PIA template and guidance documents to include a Commercial Data module and amend the analysis of completed PIAs where necessary.
- Have the DHS Privacy Office analyze the template contract language for Commercial Data vendor relationships, propose any necessary modifications, and review each relationship and contract.
- Make certain the DHS Privacy Office can effectively require the accurate and timely processing of PIAs, and mitigation of privacy risks noted therein.
- Make certain DHS commits sufficient resources to the DHS Privacy Office to (a) review the PIAs, (b) follow up to make certain privacy risks are mitigated, and (c) ensure the PIA continues to be accurate as programs change.

As we have come to expect from the DPIAC, these recommendations were valuable as well. The Privacy Office spent the early months of 2007 evaluating how to incorporate them into the Department's PIA process.

[3] DPIAC Report No. 2006-03, available from http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_commdata.pdf; Internet; accessed 5 March 2008.

Privacy Impact Assessments under E-Government Act and PIA Guidance

The Privacy Office agrees with GAO's assessment in its'06 report that PIAs are an important tool for agencies to publicly address privacy issues early in the process of developing new information technology (IT) systems. Indeed, the *E-Government Act of 2002* requires agencies to conduct a PIA when developing or procuring IT systems or projects that collect, maintain, or disseminate information in an identifiable form or about members of the public.

As the Chief Privacy Officer, I was pleased to note that GAO found DHS had increased both the number and quality of our PIAs during its last review of our office.[4] This impressive improvement is due to the regular review and revision of the PIA Guidance and accompanying training presentations, developed by the Privacy Office's Director of Privacy Compliance. The last revision issued in May 2007 incorporates the recommendations of two DPIAC reports on the use of commercial data.

The connection between the need for a PIA and the use of commercial data is made plain in the PIA Guidance. Under the heading *When to Conduct a PIA*, for instance, program or system officials are instructed to complete a PIA "if a program or system adds additional sharing of information either with another agency or incorporates commercial data from an outside data aggregator…"[5]

The PIA Guidance then calls for information and analysis about the proposed use of commercial data in no fewer than nine places, giving expression to the DPIAC's recommendations. These include a required discussion of why the commercial data is "relevant and necessary" to the system's purpose, and how it is used to fulfill these purposes. Additionally, PIAs now call for a discussion of the "levels of accuracy" of the commercial data required by the contract between DHS and the commercial aggregator. This is consistent with the DPIAC recommendation that the Privacy Office review certain provisions of vendor contracts.

Additional Authority for PIAs

It is well understood that the E-Government Act requires PIAs for many government IT systems, including most making use of commercial data. As the GAO report points out, however, DHS cites OMB guidance in an Appendix to its PIA Guidance, which includes a parenthetical exception to this requirement: "Merely querying [a commercial source] on an ad hoc basis using existing technology does not trigger the PIA requirement."[6] Thus, the undefined difference between "systematic" and "ad hoc" uses, prompted GAO to

[4] GAO-07-522, DHS PRIVACY OFFICE: Progress Made but Challenges Remain in Notifying and Reporting to the Public, April 2007.
[5] Privacy Impact Assessment: Guidance, DHS Privacy Office, May 2007,
[6] Id. Appendix I: PIA Triggers (citing OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003).

recommend that OMB revise its guidance to clarify the applicability of the Privacy Act and the E-Government act to the use of PII from resellers.

When the DPIAC examined this question for the Department, it recommended that a PIA be conducted where commercial data is used systematically as required by E-Government Act or where there "is substantial risk of harm" from the use, even if that use is ad hoc and exempt from the requirement under OMB guidance. This recommendation recognizes that the DHS Chief Privacy Officer has additional authority to conduct PIAs beyond the authority under the E-Government Act.

Section 222 of the Homeland Security Act of 2002, the Privacy Office's organic legislation, gives the Chief Privacy Officer separate and distinct authority to conduct PIAs on his own initiative in order to "assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information." We have found that PIAs are an invaluable tool for programs to understand how their use of information impacts privacy. In addition, PIAs enhance the confidence the public has in the steps DHS takes to protect privacy. Under this additional authority, the Privacy Office has pioneered the use of PIAs beyond what the E-Government Act requires in two ways.

First, the Privacy Office recognizes that privacy can be impacted by programs, policies, certain uses of information, and rules, in addition to information technology. Therefore, as a matter of policy the Privacy Office conducts PIAs to examine these offices, policies, uses, and rules, as well, even though it is not required to under the E-Government Act.

These PIAs examine the application of the Fair Information Practice Principles (FIPPs) to the policy or, in this case, a particular use. The eight FIPPs are rooted in the tenets of the Privacy Act and govern the appropriate use of personally identifiable information (PII) at the Department.[7] They are:

1. Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system whose existence and purpose is a secret.
2. Individual Participation: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should

[7] The Department's PIA Guidance defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department." Section 208 of the E-Gov Act requires agencies to conduct a PIA for systems which collect, maintain, or disseminate information in an identifiable form, which is defined as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." (P.L. 107-347)

provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

3. Purpose Specification: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used and shared.

4. Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

5. Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department is limited to purposes compatible with the purpose for which the PII was collected.

6. Data Quality and Integrity: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

7. Security: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

8. Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Second, although it is less relevant in this context, as a matter of policy the Privacy Office conducts PIAs on national security systems, which are exempted from the requirement under Title II of the E-Government Act (Section 202(i)); although, consistent with the need to protect the processes associated with national security, the Privacy Office refrains from publishing these PIAs on our public facing website, www.dhs.gov/privacy.

Armed with the authority of Section 222 of the Homeland Security Act, and mindful of the issues associated with commercial data, the Privacy Office implements the DPIAC recommendation that the Department conduct a PIA whenever there is a substantial risk of harm flowing from the use of commercial data, even if the use is exempt from the requirement under the E-Government.

Conclusion

The Privacy Office is committed to ensuring DHS programs are a success, both in terms of forwarding the critical law enforcement, counterterrorism, and fraud detection missions of the Department and the United States Government to ensure the safety and

well-being of our citizens, and equally in preserving the privacy protections the American public has a right to expect.

This will require close scrutiny of the use of PII, particularly when it is obtained from commercial information resellers. The Privacy Office will continue to use the Privacy Impact Assessment to examine the use of commercial data whenever it is required by the E-Government Act or under the authority of Section 222 of the Homeland Security Act, when even ad hoc use presents a substantial risk of harm.

In sum, the Privacy Office has taken a leadership role on the use of PII from commercial sources data benefiting what we have learned from our Advisory Committee, a public workshop, and robust implementation of Privacy Impact Assessments.

I thank the Subcommittee for this opportunity to testify about the use of commercial data at the Department and the steps we take to make sure it is used consistent with the Fair Information Practice Principles. I look forward to answering your questions.