Statement of James X. Dempsey
Executive Director
Center for Democracy & Technology

before the
House Committee on the Judiciary
Subcommittee on Commercial and Administrative Law

"Privacy in the Hands of the Government:
The Privacy Officer for the Department of Homeland Security"

February 10, 2004

Chairman Cannon, Ranking Member Watt, Members of the Subcommittee, thank you for the opportunity to testify today about the Privacy Officer for the Department of Homeland Security. Based upon the short but significant record of that office to date, it is clear that a statutory Privacy Officer, participating in senior level policy deliberations and using the tools of Privacy Act notices and Privacy Impact Assessments, can be an important mechanism for raising and mitigating privacy concerns surrounding the government's use of personal information. Certainly, the DHS Privacy Officer legislation is a model for other agencies, including the Department of Justice. With some further reforms we support, including enactment of the Defense of Privacy Act and improvements to the Privacy Act of 1974, statutory Privacy Officers should be an important element of the overall approach to meeting the public's deeply-held and constitutionally-based interest in privacy protection even in the pursuit of urgent governmental missions like counterterrorism.

The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the Internet. Our core goals include enhancing privacy protections both in consumer transactions and

between citizens and their government. We are also strong supporters of electronic government, having worked closely with key Members of the House and Senate for enactment of the E-Government Act of 2002. We commend you for your sustained attention to the important privacy issues associated with the government's collection and use of personal information. We look forward to ongoing work with you on these matters.

I. SUMMARY

The federal government has many legitimate needs for collection and use of personal information, ranging from administration of benefits programs to tax collection to winning the war on terrorism. Especially in light of the digital revolution, this government demand for information brings with it heightened risk to privacy and the associated values of Fair Information Practices – including notice; limits on collection, use, disclosure and retention; data quality; security; and the citizen's right to review and correct information held about himself.

One of the best ways to protect privacy, while facilitating the effective collection and use of information where necessary to carry out a governmental function, is to raise privacy concerns early in the development of a new program, so that those concerns can be addressed and mitigated in advance. We call this "privacy by design" – building in privacy protections from the ground up. Watchdog groups like CDT and even Members of Congress often find out about a privacy problem only after a system has been implemented. Then, it is often difficult to correct the problem. To ensure that privacy issues are addressed early on, many private companies and some government agencies

have created a Chief Privacy Officer position -- someone inside the organization, who can be consulted during the conceptualization phase of a new project involving collection of personal information.

In the Federal government, the Department of Homeland Security (DHS) has a statutorily created Privacy Officer – the only such statutory position in the U.S. government today. While this is a new position, CDT has been impressed with the role that Nuala O'Connor Kelly has assumed within the Department. We believe that the DHS experience should serve a model for agencies across the government.

We would also like to take this time to again voice our support for the Defense of Privacy Act (DOPA), which will require agencies to publish Privacy Impact Assessments (PIAs) for all regulations. DOPA will serve as a sound complement to Section 208 of the E-Government Act of 2002, which requires that federal agencies conduct PIAs whenever they purchase a new information technology or initiate a new collection of personally identifiable information. One of the first published PIAs was the one written by the DHS Privacy Officer on the US-VISIT (United States Visitor and Immigrant Status Indicator Technology) program. It is an important document and has served to bring greater transparency to that program. PIAs can be especially effective if they are published before the system design or regulatory process is completed.

II. CHIEF PRIVACY OFFICERS

A. History of Chief Privacy Officers in the Federal Government

For years, many federal agencies have had "Privacy Act Officers." In some agencies, this has actually been a part-time job. Privacy Act Officers often spend much

of their time not on privacy issues per se, but in dealing with requests from individuals who want to see their government records under the access provisions of the Privacy Act. In addition, these officers usually are also responsible for the other major records disclosure law, the Freedom of Information Act. Privacy Act Officers, despite their title, have no statutory basis in the Privacy Act. There is no mechanism for including them in internal deliberations on matters affecting privacy. They are often mid-level career officials and do not have the ability to intervene at a policy level even when a major privacy issue comes to their attention. They are often brought into discussions about a program only at the last minute to draft a notice required under the Privacy Act when the government creates or changes a "system of records," but that notice generally serves no role in shaping policy.

Realizing that this system was not effective, the Clinton Administration in 1998 required all agencies to "designate a senior official within the agency to assume primary responsibility for privacy policy."[1] The Clinton Administration used these "privacy leaders" to review Privacy Act compliance within each agency. The next year, Peter Swire was named Chief Privacy Counselor for the Administration within the Office of Management and Budget. Mr. Swire worked on both commercial and government privacy issues and had a voice in deliberations concerning agencies across the government. Among his accomplishments was requiring all government Web sites to include privacy notices.

---

[1] William J. Clinton, "Memorandum for the Heads of Executive Departments and Agencies," May 14, 1998, <http://www.cdt.org/privacy/survey/presmemo.html>.

At the same time, many companies in the private sector began to hire or promote employees to be "Chief Privacy Officers." The CPO position is now very common in the e-commerce, banking and health care industries. Several membership organizations of CPOs have formed. The largest of these, the International Association of Privacy Professionals (IAPP), now meets twice yearly and includes a wide range of industry and government representatives from around the world.

In 2001, many of the privacy leaders within federal agencies — mostly political appointees — left government service with the change in administrations. Despite urging from privacy advocates,[2] the Bush Administration did not hire a new Chief Privacy Counselor and only a few agencies kept their privacy leaders. Some of these privacy leaders thrived in new full time roles as Chief Privacy Officers. In fact, a few of the federal government Chief Privacy Officers have been among the most innovative in the world, in either the public or private sectors.

B. Two Examples of Chief Privacy Officers in the US Federal Government

-- *Internal Revenue Service*

After a series of hearings in the late 1990s, which exposed extraordinary privacy abuses by IRS agents, the IRS began to take privacy more seriously and appointed Peggy Irving to the position of "Privacy Advocate." Ms. Irving drew upon the Canadian model of Privacy Impact Assessments to ensure that program managers understood the privacy implications of their projects, took proper steps to protect personal information, and

---

[2] Several privacy groups and academics including CDT wrote to OMB Director Mitch Daniels urging him to continue the position <http://www.cdt.org/privacy/010416omb.shtml>.

trained employees on the privacy aspects of new programs or systems. The Federal Chief Information Officer (CIO) Council soon recognized this model as a best practice and it became the basis for the E-Government Act's requirements for Privacy Impact Assessments as well as a model for private sector PIAs. In 2003, Ms. Irving left for a job with the federal courts and Maya Bernstein filled the Privacy Advocate position. Ms. Bernstein has already begun to take a leadership role in the privacy community and has been active in government-wide discussions on privacy policy.

-- ***US Postal Service***

The Postal Service collects a wide range of personal information from individuals in order to deliver the mail properly, yet it maintains one of the most trusted brand names among Americans.[3] In 2001, Zoë Strickland became the agency's first Chief Privacy Officer. Ms. Strickland worked with the Postal Service's CIO to reexamine the organization's Privacy Act Systems of Records and data flows within the agency, improving both efficiency and privacy simultaneously. After this process was complete, Ms. Strickland helped put together for project managers a full "business impact assessment" process that examines a wide range of potential issues, including privacy and security impact assessments. Ms. Strickland has also been a strong advocate for simplifying the often complex and legalistic privacy notices published both on Web sites and in the Federal Register. Ms. Strickland is frequently mentioned in the media as one of the top privacy officers in the world.

---

[3] According to a "privacy trust" survey of government agencies, industries and others conducted by Carnegie Mellon University and the Ponemon Institute, the Postal Service placed 5th of 26 categories, just above law enforcement and charitable organizations. DHS finished 25th of 26. Dr. Larry Ponemon, "In Whom Do You Trust," Darwin Magazine, November 2003. <http://www.darwinmag.com/read/110103/trust.html>.

C. The DHS Privacy Officer

Based on these positive experiences, Congress created the first statutory privacy officer in Section 222 of the Homeland Security Act of 2002. The DHS Privacy Officer's statutory responsibilities include "evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government" and "conducting a privacy impact assessment of proposed rules of the Department . . . including the type of personal information collected and the number of people affected." The Privacy Officer reports directly to the Secretary.

In April, 2004, Nuala O'Connor Kelly was named to the post. In CDT's opinion, Ms. Kelly was the right person for a difficult job. She had privacy sector experience dealing with a startup company that was trying to rapidly improve privacy protection while expanding its business, and she had experience within the Bush Administration as Chief Privacy Officer at the Commerce Department. She was well known to privacy advocates and industry.

In only ten months on the job, Ms. Kelly has been able to show why the Privacy Officer position is so vital to the success of the new department. She has become a trusted participant in internal agency deliberations while at the same time reaching out to privacy advocates and increasing public transparency of some of the most controversial programs in government today.

For example, despite the tight time pressures created in the implementation of the US-VISIT program in January, DHS released a forthright and clear analysis of the privacy issues involved with the program. After the PIA was released, the Privacy Officer hosted a meeting for a wide range of privacy advocates and immigration groups

with the US-VISIT team. Advocates expressed their concerns about issues such as the lack of information on redress issues for visitors who believe that information held about them may be incorrect or incorrectly interpreted and the unclear nature of the data quality and data retention rules. Ms. Kelly and the US-VISIT team promised that these issues will be actively addressed as the program moves forward.

We do have specific criticisms of the way DHS has handled privacy issues. The PIA on US-VISIT would have been far more meaningful if it had been issued before the program was actually being implemented. After all, the PIA is intended to surface privacy issues so they can be resolved with public input before a program is implemented. Ms. Kelly has stated that the agency will release future PIAs in advance of the program launch. In addition, as noted above, the US VISIT PIA was deficient on the question of redress and should have been more specific on data quality and data retention.

These criticisms should not detract from the basic point: the DHS Privacy Officer is an important institution and one that deserves support. CDT looks forward to continued work with the Privacy Officers as she actively builds an internal team and hones the tools she will need to ensure that privacy is adequately respected in all homeland security projects.

D. Statutory Authority for Privacy Officers

Based upon the DHS experience, as well as the experience at other agencies and in the private sector, CDT believes that every federal agency should have a statutory Privacy Officer with authorities similar to those provided under the Homeland Security Act. This officer would have the stature and authority to gain attention to this important

issue and effectively conduct privacy impact assessments and train agency staff in their privacy responsibilities.

The essential elements of an effective Privacy Officer function, as we see it are three-fold: (1) statutory basis; (2) adequate staff; (3) inclusion in senior-level policy deliberations.

Even with these elements, the Privacy Officer is not a panacea. Congress cannot create Privacy Officers and claim to have solved the privacy problems associated with government in the digital age. Continued oversight will be needed. And the underlying statutory authorities must be strengthened. Privacy Officers alone cannot mitigate, for example, the problems associated with data mining and the blurring of the lines between government and private sector databases. That will require Congressional and Executive Branch action to detail the standards and guidelines for information access and sharing.

III. FURTHER PRIVACY REFORMS NEEDED

Privacy Officers are part of the answer to the privacy challenge, but they cannot be effective if the privacy laws remain outmoded for changing technology. The best, most effective Privacy Officer will achieve nothing if she does not have good laws to work with.

PIAs have become a key tool for Privacy Officers, Congress and the public to monitor federal programs. Under the Section 208 of the E-Government Act, signed into law by President Bush at the end of 2002, federal agencies were supposed to begin posting PIAs in April 2003. Those that have been made available have been high quality documents, yet, unfortunately, most agencies have not been making their PIAs publicly

available. This is partly due to the fact that OMB only published guidance for Section 208 in November 2003. But more importantly now, OMB has encouraged agencies not to make PIAs available until after their budgets are finalized. This is inconsistent with the purpose and value of PIAs. PIAs should be released as soon as they are completed, to promote public participation in the debate over pressing privacy concerns.

There is also a need for greater awareness within government of the new privacy provisions of the E-Government Act. CDT has been working with key partners to organize a series of workshops to educate government officials on what they need to do to comply with the Act's core requirements. In April 2003, CDT co-hosted a workshop on the new privacy rules that were being drafted under the Act. Speakers included the DHS Chief Privacy Officer and representatives from OMB. In November, CDT co-hosted a public workshop to help agencies craft and review the reports on privacy activities required under Act. In 2004, we will be hosting further workshops on implementation of the E-Government Act. The first of these already took place on January 22, when CDT co-hosted a forum to help agencies comply with the Act's provisions on machine readable privacy notices. And on March 31, CDT will be hosting, along with the Council for Excellence in Government and the American Council for Technology, a workshop on PIAs.

CDT previously testified that the Privacy Impact Assessments required under the Defense of Privacy Act will complement the PIA requirements of the E-Gov Act. We are very pleased that the Subcommittee is planning to report the bill. As DOPA moves forward, we recommend that you ensure that the PIA provisions of DOPA and the E-Government Act are congruent. Our initial thoughts are that this should be done by

making the list of factors to be considered in a PIA the same in both laws, and by making it clear that when a new collection of information is initiated by rule, the notice and comment provisions of the Defense of Privacy Act apply to the privacy impact assessment process. Indeed, the publication requirement of DOPA is an improvement over the E-Government Act; it may be desirable to amend the latter to make it clear that PIAs must generally be published for comment before a system is procured or a program is implemented.

Other privacy issues that need to be addressed include the need to update the Privacy Act. One of the Act's key definitions -- "system of records" – is ill-suited to the current data environment, in which much information useful to the government is held by the private sector. Under current law, the government may be able to bypass the Privacy Act by accessing existing private sector databases rather than collecting the information itself. When citizens and policymakers alike are concerned about the potential abuses of "data-mining" techniques, Congress obtain a full reporting from all agencies as to their uses of commercial databases and should insist that there be clear guidelines as to the access to and use of commercial data.

IV. CONCLUSION

CDT commends the Subcommittee for holding this important hearing. The excellent work of the DHS Chief Privacy Officer provides a vision of what could be. Privacy Officers cannot alone solve every privacy problem that will face the federal government. However, if the Privacy Officer position is statutorily chartered for each agency and if Privacy Impact Assessments are required to be published for both

regulations and information collections, the public will be insured greater accountability and responsibility on this important issue.

For more information, contact:

Jim Dempsey
(202) 637-9800 x112
jdempsey@cdt.org
http://www.cdt.org