October 23, 2009

Representative Bennie G. Thompson
Chair,
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

Representative Peter T. King
Ranking Member
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

Dear Chairman Thompson and Ranking Member King,

We are writing to you regarding the Chief Privacy Officer of the Department of Homeland Security and the recently released Privacy Report to Congress.[1] As you know, the operation of this office is particularly important with respect to the privacy rights of Americans, and accordingly, the Officer is required to assure that technologies, deployed by the DHS, "do not erode" the privacy of American citizens.[2] No federal agency has greater budget authority to develop systems of surveillance directed toward the American public here in the United States than the Department of Homeland Security. It is for this reason that we call your attention to the adequacy of the work of the office, as reflected in the most recent Privacy Report.

As set out in the DHS Act and amended by the 9/11 Commission Act of 2007, the statutory responsibilities of the Chief Privacy Officer include the following:

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;
(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;

[1] DHS Privacy Office, Annual Report to Congress, July 2008 – June 2009, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf [hereinafter "Annual Report"].
[2] 6 U.S.C. § 142(1).

(5) coordinating with the Officer for Civil Rights and Civil Liberties to ensure that—
    (A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and
    (B) Congress receives appropriate reports on such programs, policies, and procedures; and
(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.[3]

To help the Officer achieve these goals, Congress granted considerable investigative authority, including access to nearly all documentation relating to Department programs, the power to conduct investigations into any program or operation, the power to take sworn affidavits, and the power to issue subpoenas with the approval of the Secretary.

Having now reviewed the most recent annual report, it is our view that the Chief Privacy Officer for DHS has failed to fulfill her statutory obligations and that the Congress must consider the establishment of alternative oversight mechanisms, including the creation of an office that is independent of the agency it purports to oversee. Without such an independent office,[4] it will be impossible to ensure the proper protection of privacy rights, because the decisions of the Chief Privacy Officer will continue to be subject to the oversight of the Secretary and the rest of the Executive branch.

Discussion

The primary statutory duty of the Chief Privacy Officer is to assure "that the use of technologies sustain, and do not erode, privacy protections."[5] The CPO has not done so, focusing instead almost exclusively on the fourth statutory duty, conducting a "privacy impact assessment"[6] on each Department action. The structure of the annual report reveals the Office's confusion of these two duties, to the detriment of the former. The report notes that the Office "is divided into two major functional units: Privacy Compliance; and Departmental Disclosure and FOIA."[7] The report claims that the Compliance Group "manages statutory and policy-based responsibilities by working with each component and program throughout the Department to ensure that privacy considerations are addressed when implementing a program, technology, or

[3] Homeland Security Act, Section 222, codified as amended at 6 U.S.C. § 142 (2008).
[4] *See*, *e.g.,* European Commission, Data Protection – National Commissioners, *available at* http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm (last visited Oct. 13, 2009); Office of the Privacy Commissioner of Canada, *available at* http://www.priv.gc.ca/index_e.cfm; Office of the Privacy Commissioner for Personal Data, Hong Kong, *available at* http://www.pcpd.org.hk/.
[5] *Id.* at § 142(1).
[6] *Id.* at § 142(4).
[7] Annual Report at i.

policy."[8] This description should encompass the fulfillment of the statutory responsibility to prevent erosion of privacy. Yet the section of the annual report entitled "Compliance" barely discusses ways in which the Office has done so; it focuses almost entirely on the conducting of assessments.[9] In fact, the "Privacy Compliance Process" graphic describes the process as containing Review, Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), and if necessary, a System of Records Notice (SORN), followed by a repetition of the cycle after three years for programs still in force.[10]

It is true that the assessment process is a possible avenue for the Office to protect privacy. The report gives at least one example of this taking place: the PIA for the USCIS Fraud Detection and National Security System Data System (FDNS-DS). According to the report, the PIA identified a risk and set forth a solution: procedures that USCIS must follow in certain circumstances to mitigate the risk. The report only describes a handful of other PIAs, leaving the full list to an appendix, but in none of the other examples cited does the Office report that the PIA actually had a meaningful effect on the Department's activities.[11]

The following is a brief list of examples, programs undertaken by the Department of Homeland Security during or since the reporting period which have substantially eroded privacy protections:

- Fusion Centers and the Information Sharing Environment
- Whole Body Imaging
- Closed-Circuit Television (CCTV) Surveillance
- Suspicionless Electronic Border Searches

In each of the above cases, the Privacy Office has failed in its statutory duty to assure that the use of technologies does not erode privacy protections relating to use, collection, and disclosure of personal information.[12] It has written Privacy Impact Assessments, but these Assessments have no force, no meaningful effect on the Department's activities.

Fusion Centers and the Information Sharing Environment

In May 2004, the Department of Justice announced its progress in implementing the National Criminal Intelligence Sharing Plan. The announcement made public the decision to create a Criminal Intelligence Coordinating Council (CICC) that would be managed by Global. By December 2004, the push for a national Fusion Center initiative received a boost when the Department of Justice sponsored Global Infrastructure/Standards Working Group published A Framework for Justice Information Sharing: Service Oriented Architecture (SOA). States using local, state, and federal funds created information Fusion Centers. In August 2005, the Institute for Intergovernmental Research published the Fusion Center Guidelines:

---

[8] *Id.*
[9] *Id.* at 33–44.
[10] *Id.* at 35.
[11] *Id.* at 38–39.
[12] 5 U.S.C. § 142(1).

> The principal role of the fusion center is to compile, analyze, and disseminate criminal/terrorist information and intelligence and other information (including, but not limited to, threat, public safety, law enforcement, public health, social services, and public works) to support efforts to anticipate, identify, prevent, and/or monitor criminal/terrorist activity. This criminal information and intelligence should be both strategic (i.e., designed to provide general guidance of patterns and trends) and tactical (i.e., focused on a specific criminal event).[13]

A Congressional Research Service Report on Fusion Centers outlined several fundamental problems with the Guidance on Fusion Center development: first, adherence is voluntary, second, the philosophy outlined is generic and does not translate theory into practice, and third, they are oriented toward the mechanics of Fusion Center establishment.[14] The majority of regional Fusion Centers are concentrated in large urban areas. The jurisdictions of these centers are also covered by state Fusion Centers, but there is a question regarding how overlapping jurisdictions are managed.

The CRS Report on Fusion Centers also point out that there is no single legal authority that govern the operation of Fusion Centers.[15]

The Department of Homeland Security set out an objective to create by 2008 a network of fusion centers as a unique law enforcement and threat information resource that could facilitate across jurisdictions and functions supported by multidisciplinary teams dispersed throughout a national network of information hives.

In December, 2008, the Privacy Office finally released its PIA for the Fusion Center project.[16] The PIA identifies seven "risks to privacy" presented by the program, then "examines these issues and explains the mitigation strategies for those risks . . . . Where necessary, the Privacy Office offers recommendations on how DHS (and individual fusion centers) can take additional action to further enhance the privacy interests of the citizens they are charged with protecting."[17] These mitigation strategies are not solutions, however, and they do not prevent the fusion center program from eroding citizens' privacy.

For instance, the PIA emphasizes that "fusion centers are encouraged to publish their privacy compliance documentation, including an individualized PIA; establish a privacy

---

[13] Institute for Intergovernmental Research, Fusion Center Guidelines: Law Enforcement Intelligence, Public Safety, and the Private Sector 13, *available at* http://www.iir.com/global/products/fusion_center_guidelines_law_enforcement.pdf.
[14] Congressional Research Service, Fusion Centers: Issues and Options for Congress 10, January 18, 2008, *available at* http://fpc.state.gov/documents/organization/102652.pdf.
[15] *Id.* at 20.
[16] DHS CPO, Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, December 11, 2008, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf.
[17] *Id.* at iii–iv.

committee to interact with their local privacy advocacy communities; and to listen to and address concerns whenever possible."[18] When addressing the important principle of use limitation, the PIA notes only that "[t]he sharing occurs within the general confines of a nexus to terrorism and protecting the homeland."[19] The PIA solution to "ambiguous lines of authority, rules, and oversight" is to assume that training "will mitigate this concern."[20] The most encouraging part of the Fusion Center PIA is the Office's commitment to revisit the question as the program develops.[21]

Merely writing the PIA does not provide this necessary oversight. Neither does "encouraging" fusion centers to take certain actions without mandating those actions as conditions of receiving funding. The Department of Homeland Security has the ability to require that fusion centers participating in the program satisfy privacy requirements like those recommended in the PIA. To fulfill the statutory mission of assuring that new programs do not erode citizens' privacy, the Chief Privacy Officer is obligated to restrict the implementation of such programs. As such, while the Office has promised to revisit the question of Fusion Center privacy, in the meantime the individual centers are moving forward with little oversight and no privacy requirements.

Whole Body Imaging

Airport security has undergone significant changes since the terrorist attacks of Sept. 11, 2001. Recently, the Transportation Security Administration (TSA) announced a proposal to purchase and deploy "Whole Body Imaging" X-ray machines to search air travelers at all airports. TSA said it believes that use of the machines is less invasive than pat-down searches. However, these machines, which show detailed images of a person's naked body, are equivalent to a "virtual strip search" for all air travelers. This proposal, along with the agency's controversial plan to profile air travelers, shows extraordinary disregard for the privacy rights of air travelers.

The backscatter machines allow a highly realistic image to be reconstructed. In the case of airline-passenger screening, the image is of the traveler's nude form. The image resolution of the technology is high, so the picture of the body presented to screeners is detailed enough to show genitalia. These images are not necessarily temporary - screeners can save the body images to the system's hard disk or floppy disk for subsequent viewing on either "the system monitor or on any IBM compatible personal computer with color graphics."[22]

---

[18] *Id.* at 28.
[19] *Id.* at 23.
[20] *Id.* at 26–27.
[21] *Id.* at 31–32.
[22] Rapiscan Systems, Rapiscan Secure 1000 Frequently Asked Questions, #10, *available at* http://www.rapiscansystems.com/sec1000faqs.html#10

In 2009, the TSA announced that Whole Body Imaging would replace metal detectors at airport security checkpoints.[23] This was a marked departure from the earlier promises by the agency that the technology would only be used for secondary screening of air travel passengers. In response to a statement[24] from the Privacy Coalition, a nonpartisan coalition of consumer, civil liberties, educational, family, library, labor, and technology organizations, the TSA issued a statement of its own, promising that the agency would "continue to listen to the public, and . . . constantly look for ways to improve our outreach and education."[25] Rather than take the opportunity to review privacy concerns, the agency has chosen to address the issue only as a matter of outreach and education.

The PIA for the pilot program, issued during the reporting period, is similarly directed towards education.[26] It focuses almost entirely on separation between the agent viewing the image and the person being scanned, as well as on constant reassurance that the ability to save images will be disabled. It also focuses on the fact that the whole body imaging will be an option for travelers, a fact that no longer seems certain with the recent announcement of planned expansion.

Perhaps most troubling about the whole body imaging program is its almost complete absence from the CPO's annual report. It is mentioned only twice: once in passing as a topic of an outreach briefing,[27] and again in a list of security programs undertaken by TSA in a discussion of component programs.[28] This second mention highlights the same features of the program described in the PIA, but does not discuss the April 2009 policy change. With that announcement, the scope of whole body imaging dramatically increased in the months between the PIA's release almost a year ago and the Annual Report's release last month. Surely the report should have noted this change and its effects.

While acknowledging the new policy in the report would have been helpful, if the Chief Privacy Officer were satisfying her statutory duty to assure that new technologies do not erode the privacy protections of American citizens, the new policy would not have been implemented in the first place. Due to its extremely invasive nature, the whole body imaging technology is almost by definition a new technology that erodes the privacy protections of American citizens. Implementing such technology for every traveler that passes through an airport security checkpoint regardless of suspicion is exactly the type of action that the Chief Privacy Officer should be preventing in satisfaction of her statutory obligations. An independent privacy officer

---

[23] *See* Joe Sharkey, Whole-Body Scans Pass First Airport Tests, N.Y. TIMES, Apr. 6, 2009, *available at* http://www.nytimes.com/2009/04/07/business/07road.html.
[24] Letter from Privacy Coalition to Secretary Janet Napolitano, May 31, 2009, *available at* http://epic.org/privacy/airtravel/backscatter/Napolitano_ltr-wbi-6-09.pdf.
[25] Letter from Acting Administrator Gale D. Rossides to Lillie Coney, June 19, 2009, *available at* http://privacycoalition.org/dhs-reply-wbi_ltr.pdf.
[26] DHS CPO, Privacy Impact Assessment for TSA Whole Body Imaging, Oct. 17, 2008, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbi.pdf.
[27] Annual Report at 10.
[28] Annual Report at 59.

not subject to the Secretary would have been able to act much more effectively to satisfy this statutory duty.

Closed-Circuit Television (CCTV) Surveillance

In December 2007, the Privacy Office conducted a two-day workshop to discuss and examine "best practices" for use of closed-circuit television (CCTV) surveillance by the government. The resulting report summarized the various panels and presented some useful conclusions for how to best protect privacy while implementing such programs.[29] While this report contained a number of recommendations, it is not clear from either the activities of the Department or the Annual Report that the recommendations have been implemented in any way.

The 2007 workshop had several conclusions for CCTV privacy best practices. They strongly recommended that localities implementing CCTV provide cost-benefit analysis of the decision to employ CCTV, opportunities for community involvement in the process, and most importantly, written policies addressing privacy and civil liberties concerns, including, at minimum, the following:

1. Definition of appropriate use;
2. Access rights for those whose images are identified and
3. Security controls governing the
4. Appropriate limits on the location of cameras;
5. Monitoring for inappropriate uses;
6. Retention policies;
7. Adequate training of personnel with access to the systems; and
8. Internal and external auditing.[30]

The report then concluded that "all of the Workshop panelists cited the importance of public support from within the community about the use of cameras and strongly supported drafting and implementing policies to protect privacy and civil liberties before undertaking CCTV programs."[31]

Nevertheless, even though the report is now almost two years old, the Department of Homeland Security has failed to turn its "best practices" into *actual* practices. Meanwhile, the Department continues to issue grants for CCTV development.[32] The DHS grant application, which localities must complete in order to apply for funding for such projects, would be an

[29] DHS CPO, CCTV: Developing Privacy Best Practices, Dec. 17 and 18, 2007, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.
[30] *Id.* at 14–15.
[31] *Id.* at 15.
[32] *See, e.g.*, DHS, Secretary Napolitano Announces More than $355 Million in Recovery Act Funding for Airport Security Projects, Oct. 1, 2009, *available at* http://www.dhs.gov/ynews/releases/pr_1254405418804.shtm.

excellent place to require policies of the type recommended by the report. Instead, it makes no mention of any such policies, either as requirements or even as recommendations.[33]

The Annual Report touts the 2007 workshop in its "Reporting and Inquiries" section, but makes no statement at all about implementing its recommendations, or planning to do so in the future.[34] As such, there is no indication that the Chief Privacy Officer has taken any action to prevent the erosion of privacy through the use of CCTV. This failure to act is especially grievous because the results of the 2007 workshop demonstrate a clear path that the Office could follow to implement safeguards. Instead the workshop report has languished for almost two years, while the Department has proceeded ahead with the CCTV program, funding programs in many localities and airports across the country.

Suspicionless Electronic Border Searches

Another major erosion of privacy in recent years has come in the form of suspicionless border searches of electronic devices. The Privacy Impact Assessment on this issue was published after the reporting period,[35] but the issue is mentioned briefly in the annual report.[36] In short, agents of U.S. Customs and Border Protection (CBP) and agents of U.S. Immigration and Customs Enforcement (ICE) claim broad powers to search any person and his or her personal belongings when crossing the border into the United States, even in the absence of any suspicion of wrongdoing.

As the PIA makes clear, the legal authority for suspicionless border searches is well established with respect to *physical* searches of travelers' belongings.[37] The Office then goes on in the Assessment to note that "[t]he second and more central privacy concern is the sheer volume and range of types of information available on electronic devices as opposed to a more traditional briefcase or backpack."[38] The PIA acknowledges, quite correctly, that "[w]here someone may not feel that the inspection of a briefcase would raise significant privacy concerns because the volume of information to be searched is not great, that same person may feel that a search of their laptop increases the possibility of privacy risks due to the vast amount of information potentially available on electronic devices."[39]

Yet after acknowledging these increased risks and the ways in which electronic searches may not fall under the same analysis as that used in physical searches, the report does little to mitigate these risks. In fact, the stated intent of the Assessment is not to reduce these risks or prevent the erosion of privacy. Instead, "CBP and ICE have conducted this Privacy Impact

---

[33] Fiscal Year 2009, Homeland Security Grant Program Guidance and Application Kit, Nov. 2008, *available at* http://www.fema.gov/pdf/government/grant/hsgp/fy09_hsgp_guidance.pdf.
[34] Annual Report at 77–78.
[35] DHS CPO, Privacy Impact Assessment for the Border Searches of Electronic Devices, August 25, 2009, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf.
[36] Annual Report at 54–55.
[37] PIA for Electronic Border Searches, *supra* note 35, at 2–4.
[38] *Id.* at 2.
[39] *Id.*

Assessment (PIA) to enhance public understanding of the authorities, policies, procedures, and privacy controls related to these searches."[40] As with the TSA's whole body imaging letter, the rest of the PIA reads like an outreach tool, an opportunity for the agencies themselves to explain to the public why they have the right to invade privacy so extensively. It describes in some form the limitations that exist on the agencies' ability to share the data, but makes almost no prospective conclusions about ways that privacy invasions could be reduced or eliminated.

The Annual Report's treatment of the issue focuses primarily on the "relative rarity of these searches"[41] when compared to the number of travelers crossing America's border each year. Indeed, the cited numbers do show that the searches are relatively rare. Nevertheless, the agency refuses to release any guidelines for future searches, and refuses to even release retrospective descriptions of what motivated the rare searches that have already taken place. This does little to assuage fears that CBP and ICE retain the substantial power to invade travelers' privacy for no reason and with no recourse.

Yet again, the approach of an independent Privacy Officer to this topic could have been very different. The CPO's approach to this and many issues has been as an insider, a member of the team seeking to implement the broadest plan possible. As such, the Office's PIA is not a solution to problems raised, but rather a justification for the Department's behavior.

Exemptions to the Privacy Act of 1974

The Office also certifies the Department's requests for exemptions to its obligations under the Privacy Act of 1974.[42] Since the Department's founding, the Department and its component agencies have implemented a ridiculous number of exemptions for itself under the Privacy Act.[43] These exemptions have the practical effect of limiting the privacy rights of Americans that would otherwise be enforced under the Privacy Act.[44] For each of these exemptions, the Chief Privacy Officer had the opportunity to reject the request, but instead authorized the exemption. In many cases, the CPO's signature appears in the proposed or final rulemaking.[45]

Conclusion

---

[40] *Id.* at 3.
[41] Annual Report at 54.
[42] 5 U.S.C. § 552a.
[43] *See, e.g.*, 6 C.F.R. App'x C (2008) (listing all Privacy Act exemptions for DHS); 49 C.F.R. § 1507.3 (2008) (listing all Privacy Act Exemptions issued for the TSA), 44 C.F.R. § 6.86–87 (2008) (listing all Privacy Act Exemptions issued for FEMA).
[44] *See, e.g.*, TSA: Part 1507 Privacy Act – Exemptions, Regulatory History, *available at* http://www.tsa.dhs.gov/research/laws/regs/editorial_1780.shtm (showing series of rulemakings that resulted in the large number of exemptions currently present in the Code of Federal Regulations).
[45] *See, e.g.*, Privacy Act of 1974: Implementation of Exemptions; Advanced Passenger Information System, 72 Fed. Reg. 48346 (proposed Aug. 23, 2007).

The DHS CPO has shown an extraordinary disregard for the statutory obligations of her office and the privacy interests of Americans. Outreach is certainly important, but the job of Chief Privacy Officer is not to provide public relations for the Department of Homeland Security. The job as defined in the statute is to protect the privacy of American citizens, through investigation and oversight. If an internal office cannot achieve this, then the situation calls for an independent office that can truly evaluate these programs and make recommendations in the best interests of the American public.

We urge the Committee to promptly open an investigation into this simple question:

> Has the Chief Privacy Officer of the Department of Homeland Security complied with the statutory obligations of the office?

Sincerely,

American Association of University Professors
American Civil Liberties Union
Asian American Legal Defense Committee
Bill of Rights Defense Committee
Consumer Federation of America
Center for Financial Privacy and Human Rights
Consumer Action
Cyber Privacy Project
Electronic Privacy Information Center
Fairfax County Privacy Council
Gun Owners of America
Identity Project
Internet Collaboration Coalition
Liberty Coalition
National Center for Transgender Equality
People for the American Way
Privacyactivism
Privacy International
Privacy Rights Now Coalition
Rutherford Institute
U.S. Bill of Rights Foundation

Individuals:
Former Congressman Bob Barr
Bruce Schneier, Security Expert, Editor Crypto-Gram
Philip Friedman, Consumer Attorney
Grayson Barber, Princeton University Fellow, Center for Information Technology Policy
Pablo G. Molina, Georgetown University Law Center
Edward G. Viltz, Founding President of the Public Interest Registry
Deborah Hurley, Chair, EPIC Board of Directors