



November 16, 2011

Secretary Janet Napolitano
Department of Homeland Security
U.S. Department of Homeland Security
Washington, D.C. 20528

Re: Creation of a Federated Information-Sharing System

Dear Secretary Napolitano:

The American Civil Liberties Union (ACLU) is a non-partisan organization of more than a half million members, countless additional activists and supporters, and 53 affiliates nationwide dedicated to the preservation of individual privacy rights and other civil liberties under the Constitution. We are writing today to request a meeting regarding the Department's plan to expand its internal information-sharing and create a federated information sharing network. Because of DHS's size and the broad scope of information it collects, any new information-sharing agreements would raise significant privacy concerns. If DHS is planning to create a new information-sharing network, debate over those efforts must occur in a fully transparent process. The Department must evaluate privacy considerations in the design stage in order to determine if such a system is appropriate, the correct levels of information-sharing, if any, and the best ways to mitigate potential harms.

At its October 5, 2011 meeting, the DHS Data Privacy and Integrity Advisory Committee (DPIAC) produced two reports, one from its Policy Subcommittee and one from its Technology Subcommittee, which evaluate the privacy and technology challenges inherent in integrating DHS information systems.¹ According to the report from the DPIAC Policy Subcommittee, DHS "is in the process of creating a policy framework and technology architecture for enhancing DHS's information-sharing

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

¹ The DPIAC is a federal advisory committee tasked with providing guidance to the DHS Secretary and DHS Chief Privacy office "on programmatic, policy, operational, administrative, and technological issues within the DHS that relate to personally identifiable information (PII), as well as data integrity and other privacy-related matters." Department of Homeland Security, Data Privacy and Integrity Advisory Committee Charter, May 3, 2010. http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_charter_050310.pdf

capabilities.”² Current systems “essentially comprise a series of stovepipes, to support the unique functions of the distinct DHS components. The new information-sharing project aims to create a federated system to facilitate efficient and effective data sharing among the various DHS components.”³ The DPIAC reports provide no further detail about the scope or mandate of this “new information-sharing project”.

Such a potentially expansive information-sharing project raises a host of technical and policy issues. There are six main considerations to address at the outset of any such project.

1. Is the information sharing necessary? As an initial matter, DHS must establish the need for its component agencies to engage in further information-sharing. What are the specific problems a federated information system aims to ameliorate?

Information sharing between agencies is far from an unfettered good. Information collected for one purpose is frequently unsuitable for another purpose and in some cases may be improper or illegal. When an immigration attorney crosses the border, Customs and Border Patrol (CBP) claims the authority to search and copy the contents of his or her laptop. That laptop is likely to contain information on current clients – many of whom may have active cases before the US Customs and Immigration Service (USCIS). But sharing that information with USCIS would be improper and could violate an individual’s constitutional rights.

Similarly, information collected by one agency could be of limited value or low accuracy. The Secret Service is required to collect information about and investigate any threat against the President. However, it has an institutional understanding of the limitations of this kind of data. Most such leads are incorrect, inaccurate or otherwise baseless. It would be very dangerous if other agencies without the Secret Service’s institutional knowledge were to obtain access to this system and use its data for other purposes. Imagine if an anonymous tip that an individual was a threat was enough to bar the person from domestic air travel or force him or her to undergo a strip search at the border.

These concerns are particularly acute because the predicate for searching this new federated system remains unclear or unstated. The DPIAC appropriately notes that any information-sharing system must have a privacy policy that governs, among other things “the purposes for which the system may be searched.”⁴ Because of DHS collects and retains such a broad swath of information on innocent Americans, this purpose must be much clearer and the authorized uses must be much more narrowly defined. Any search of a federated database should be predicated on a reasonable and articulable link to terrorism or criminality.

Determinations about access to a database, the purposes for which a database may be used, and the precedent conditions required to justify use are necessary to the creation of any

² Data Privacy and Integrity Advisory Committee, Policy Subcommittee, Report No. 2011-____, Privacy Policy Recommendations for a Federated Information-Sharing System, Oct. 5, 2011, pg 1. (report not yet numbered) http://www.dhs.gov/files/committees/gc_1161274938888.shtm

³ *Id.*

⁴ *Id.* at 7.

system. DHS has 230,000 employees.⁵ Most of them should not have access to the vast majority of information in DHS databases. Careful consideration of the purpose and necessity of information-sharing is vital in order to determine what information DHS employees need in order to properly perform their duties.

2. How will information-sharing exacerbate existing problems with DHS systems?

Many DHS systems contain information which is incorrect or wildly prejudicial. Some civil liberties advocates argue that the collection of much of that information is improper. Further dissemination of it, even to a limited extent, would dramatically exacerbate that problem and harm innocent people. Suspicious Activity Reporting (SAR) programs, like the “America’s Waterways Watch” program or “See Something, Say Something” encourage the reporting of innocuous activities like photography or operating a boat “with no apparent destination” as suspicious behavior to the Coast Guard or other DHS components, even though there is no reasonable basis to believe these commonplace activities indicate the occurrence of criminal or terrorist activity.

Likewise, behavioral detection programs like the Transportation Security Administration’s (TSA) SPOT program use unreliable subjective indicators. Factors such as appearing arrogant or complaining about airport security procedures serve as justification for sending people to secondary airport screening, where the agency collects and retains information about these travelers. It is entirely inappropriate for to distribute such information broadly through DHS.

3. What procedures are in place to minimize information collection? DHS collects enormous amounts of information about innocent people. Examples of DHS data collection include:

- benefit information from the Federal Emergency Management Agency (FEMA),
- traveler information from CBP and TSA,
- work history from the E-Verify program,
- permit and payment information from the Coast Guard,
- naturalization records from USCIS, and
- personal information like social security number, date of birth, and email address from a wide variety of sources.

Will DHS limit sharing of this information on innocent people or purge it from the system? Just because an ordinary American has had an encounter with DHS does not mean that his or her movements, work history, or other data should be open to widespread scrutiny. Data minimization procedures are critical in assuring appropriate limitations on all uses of information.

⁵ Department of Homeland Security, 2011 Budget in Brief, http://www.dhs.gov/xlibrary/assets/budget_bib_fy2011.pdf

4. How will the system address pattern-based searching? Pattern-based searches pose a serious threat to privacy because they typically involve searches for types of behavior that do not necessarily indicate wrongdoing. This type of investigative method is invasive but often ineffective. Because most patterns loosely correspond to terrorist or criminal activity and because there are many more innocent people than there are criminals or terrorists, these investigations end up targeting almost exclusively innocent individuals. It is a core tenet of our society that government and law enforcement should only investigate individuals suspected of wrongdoing. Pattern-based searches turn this principle on its head by assuming everyone should be a subject of investigation and placing the burden on individuals to prove themselves innocent.

DPIAC shares this concern. The Committee specifically noted:

We also assume that the system would permit queries based only on specific PII [personally identifiable information], such as a name, an address, or a phone number. Given this assumption, there is little risk of users searching for potential patterns that conceivably could identify potential persons of interest. A system that would allow such pattern searches raises a far more significant set of privacy issues. Should the proposed system be altered to allow for pattern-based searches, this analysis would need [to] be revisited.⁶

Unfortunately the assumption referenced in the DPIAC quote may be incorrect. According to a recent Government Accountability Office report, DHS has at least six different systems that rely on pattern-based analysis.⁷ The GAO report identifies a series of problems with the programs, recommends reforms, and concludes “Until such reforms are in place, DHS and its component agencies may not be able to ensure that critical data mining systems used in support of counterterrorism are both effective and that they protect personal privacy.”⁸

Given DHS’s use of pattern-based analysis and the problems with DHS’s existing systems, the transparency of the Department’s efforts to integrate pattern-based searches is vital.

5. Will the system use commercial data? Commercial databases containing information about American consumers have widespread and well demonstrated problems. They are frequently inaccurate because many began as marketing databases for advertisers where accuracy is a much less significant concern. Their use by private companies for background checks and other purposes has harmed many Americans. Companies have wrongfully terminated employees or denied them employment opportunities based on inaccurate information in these systems.⁹ Often, these databases wrongly describe a person as having a criminal record because the record is mistakenly combined with that of other people who share the same name. Imagine if such errors were to become part of screening for air travel, border crossings, or scrutiny from DHS intelligence analysts.

⁶ DPIAC Report at 3.

⁷ GAO-11-742, *Data Mining DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism*, Sept. 2011. The report identifies the following systems as utilizing pattern based analysis: Analytical Framework for Intelligence (AFI), Automated Targeting System (ATS)/ATS-Passenger (ATS-P), Citizen and Immigration Data Repository (CIDR), Data Analysis and Research for Trade Transparency System (DARTTS), ICE Pattern Analysis and Information Collection (ICEPIC), TECSa/TECS Modernization (TECS-Mod)

⁸ *Id* in Findings.

⁹ For more information on the harms from commercial data brokers please see our letter of November 2, 2009 to the Senate Judiciary Committee available here: http://www.aclu.org/files/assets/ltr_support_S1490.pdf.

If DHS integrated the almost limitless amount of commercial information into its systems, it would also have a detrimental effect on free speech and other First Amendment protected activities. Many sources of commercial information are based on precisely this type of information. Membership organizations from across the political spectrum share mailing lists. Political affiliations appear on voter lists. Reading and viewing habits are traded between companies to improve marketing lists and consumer targeting. Imagine a CBP agent quizzing an American on his or her membership in a particular organization before allowing reentry into the country or a TSA agent asking a flyer about the magazines to which they subscribe. Monitoring by the government of such personal and protected activity is certain to influence whether individuals join particular groups or subscribes to certain magazines. They are likely to steer away from controversial or unpopular topics for fear of attracting government scrutiny. This type of chilling effect on the First Amendment could violate the constitution.

6. Will information be shared outside DHS? DHS is a participant in many information-sharing programs, including Joint Terrorism Task Forces and state and local fusion centers. These operations often include a host of federal, state and local government agencies as well as private companies, any of which may gain access to DHS data because of permissive information-sharing policies. If all of these participants are able to access DHS information-sharing systems, then the system is essentially boundless. It will contain a wide array of information on most or all Americans and the information will be accessible to local, state and federal law enforcement officers, intelligence agencies, employees of DHS, and possibly even employees of private corporations.

In addition to these six main issues, we also share the fears raised in the DPIAC report that a federated information-sharing system would create other privacy concerns and significant technical hurdles. Issues include:

- integrating data collected in different forms and for different purposes;
- assuring this integration does not result in errors that wrongly link the records of different people;
- clearly delineating audit controls and redress procedures;
- assuring DHS takes only limited exceptions to the Privacy Act;
- guaranteeing that secondary uses do not violate the agreements the agency entered into when it collected the information; and
- automating privacy and data quality controls so that information receives the same protections and clearly understood limitations wherever it is accessed.

All of these problems must be addressed before any system can become operational.

There is a need for an open and transparent process in the creation of any DHS information-sharing system. The Department interacts with millions of Americans every day. It must do so in a way that not only keeps them safe, but also protects their privacy. We urge DHS to make public any plans to create a federated information system immediately and to develop a

process for soliciting and considering input from the public and from technical, privacy, and security experts on the best way to proceed with that effort. In addition, we would greatly appreciate having the opportunity to meet with those Department staff charged with overseeing the process of creating any information-sharing system well in advance of a department commitment to any particular course of action. Please contact Legislative Counsel Chris Calabrese at (202) 715-0839 with any questions or comments about this letter and to arrange for any such meeting.

Sincerely,



Laura W. Murphy
Director, Washington Legislative Office



Christopher Calabrese
Legislative Counsel



Michael German
Senior Policy Counsel

cc: Chief Privacy Officer Mary Ellen Callahan