Statement of Gregory T. Nojeim
Director
Project on Freedom, Security & Technology
Center for Democracy & Technology

before the
House Homeland Security Committee
Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment

Homeland Security Intelligence: Its Relevance and Limitations

March 18, 2009

Chair Harman, Ranking Member McCaul, and Members of the Subcommittee, thank you for the opportunity to testify this morning about homeland security intelligence on behalf of the Center for Democracy & Technology.*

Introduction and Summary

Without a definitive decision to do so, and on something of an ad hoc basis, government agencies at the federal, state and local level have created a vast domestic intelligence apparatus. Until recently, collection, analysis and dissemination efforts have been disjointed and uncoordinated, which may offer some comfort to civil libertarians. Now, a variety of efforts are underway to integrate the information that is being collected and to share it more widely. The goal, of course, is laudable: to collect and connect the dots that might reveal a terrorist scheme. However, there is no overall theme to this collection and sharing effort, no guiding principles. We

* The Center for Democracy and Technology is a non-profit, public interest organization dedicated to keeping the Internet open, innovative and free. Among our priorities is preserving the balance between security and freedom after 9/11. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues. CDT has offices in Washington, DC and in San Francisco, CA.

continue to see homeland intelligence efforts that classify legitimate political activity as "terrorism" and that spy on peaceful activists; the revelations about the Maryland State Police are the latest example that has come to light. Also, there is a trend toward the collection of huge quantities of information with little or no predicate through "suspicious activity reports." There seems to us a high risk that this information will be misinterpreted and used to the detriment of innocent persons. Meanwhile, the security "bang per byte" of information gathered may be diminishing. While "stove piping" was yesterday's problem, tomorrow's problem may be "pipe clogging," as huge amounts of information are being gathered without apparent focus. All of this is occurs in the context of a powerful digital revolution that makes it easier than ever to collect, store, exchange and retrieve information in personally identifiable ways, making it available far removed from the context in which it was collected.

In our testimony today, we will consider what homeland security intelligence is and will identify some of the efforts being made to collect and share it. Then, we will turn to the risks to civil liberties posed by homeland security intelligence activities and offer some ideas on how they can be addressed.

What Is Homeland Security Intelligence and What Risks Does It Pose?

So far, the term "homeland security intelligence" has not been officially defined.[1] "Homeland security *information*" is statutorily defined as any information that relates to the threat of terrorist activity and the ability to prevent it, as well as information that would improve the response to terrorist activity or the identification or investigation of a suspected terrorist or terrorist organization. *Homeland Security Act of 2002, Pub. L. 107-296, Section 892(f)(1), 6 U.S.C. 482(f)(1).* From what we can tell, the homeland security intelligence system is equally broad. The definition of homeland security information is as significant for what it does not say as for what it says: it does not distinguish between information collected abroad and information collected in the U.S.; it does not distinguish between information regarding foreign terrorist organizations and information regarding domestic terrorist groups; it does not distinguish among information collected under criminal investigative powers, information collected under the national security powers applicable to "foreign intelligence" or counterintelligence, and information collected under regulatory or administrative authorities or from open sources; it does not

[1] CRS Report, Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches (August 18, 2006).

distinguish between information collected by federal agencies and information collected by state, local or tribal governments; and it does not distinguish between information collected with terrorism in mind and information collected for other purposes. It is broad enough to encompass all of these, and to some degree that is appropriate, since one of the reasons why the planning of the 9/11 attacks went undetected is that agencies observed various artificial distinctions that prevented information sharing and collaboration.

However, with such an all-encompassing definition, the cycle of collecting, sharing and using homeland security information or homeland security intelligence clearly poses risks to constitutional values of privacy, free expression, free association and democratic participation. The solution lies, we believe, not in a narrower definition, but in clear rules as to what can be collected and retained, under what standard and subject to what supervision, with whom it can be shared, and how it can be used. So far, this system of rules remains incomplete, while the creation of a broad homeland security intelligence system progresses apace.

In particular, this Subcommittee should be concerned about two distinct problems: (1) the continuing, even if isolated, collection of information on First Amendment activities; and (2) the newly expanded efforts to collect, exchange and use "suspicious activity reports" based on the thinnest of suspicions. Both issues involve the collection, retention and dissemination of information collected without either the criminal predicate or the "agent of a foreign power" standard found in FISA.[2] Intelligence activities not tethered to the criminal predicate are dangerous to liberty because they can cast a wide net, may encompass First Amendment activities, and tend to be more secretive because the information collected is not likely to be subject to the after-the-fact scrutiny afforded by the criminal justice system. In both cases, the risks are exacerbated by the otherwise appropriate application of digital technologies for storage, retrieval and dissemination. For example, although proponents of SARs argue that they are an extension of long-standing police practices, the power of information technology and the creation of nationwide sharing systems greatly magnify the risks that information will be taken out of context or misinterpreted, resulting in false inferences and unjustified adverse action.

In recommending serious application of the criminal predicate, we are not arguing against the need to prevent acts of terrorism before they occur. We are not seeking

[2] CDT has made recommendations for improving both the criminal investigative authorities and FISA in order to provide better privacy protection while still empowering the government to collect the information it needs, but we focus today on the collection of information outside of either a criminal predicate or the FISA standards.

to force agencies with homeland security obligations to limit themselves to prosecuting past crimes. Furthermore, we fully recognize and support the integration, properly controlled, of domestic intelligence information with information collected overseas and information collected in the U.S. under the authorities of the Foreign Intelligence Surveillance Act and related laws. Instead, we are calling for adherence to a standard that focuses on the intentions, capabilities and future actions of enterprises planning or otherwise involved in illegal activity. And we are calling for rules that take into account the ability of modern information technology to store and retrieve personally identifiable information on an unprecedented basis.

Who Collects Homeland Security Intelligence Information?

As the Subcommittee well knows, multiple agencies at the federal level collect and analyze information that fits under the homeland security intelligence umbrella.

Within the Department of Homeland Security alone, there is a departmental Office of Intelligence and Analysis and there are intelligence activities within several of the Department's components as well, including the U.S. Citizenship and Immigration Service, the Coast Guard, Customs and Border Protection, Immigration and Customs Enforcement, and the Transportation Security Administration.

Outside of the DHS, federal agencies charged with collecting or analyzing information that could be considered homeland security intelligence include:

- The FBI, which conducts counterintelligence, counterterrorism and intelligence activities primarily, but not exclusively, within the United States.
- The CIA, which collects foreign intelligence and conducts counterintelligence and counterterrorism activities related to national security primarily, but not exclusively, outside of the U.S.
- The State Department's Bureau of Intelligence and Research.
- The Drug Enforcement Administration, which collects intelligence about organizations involved in growing and distributing controlled substances.
- The Department of Energy, which assesses nuclear terrorism threats.
- The Treasury Department, which collects information relating to the financing of terrorist organizations.
- Intelligence entities within the Department of Defense, including the Defense Intelligence Agency, the National Security Agency, and the National Reconnaissance Office (whose capabilities are available for domestic collection).

Outside of the federal government, state, local, and tribal police forces of varying sizes also engage in the collection of homeland security intelligence. The level of

sophistication of these efforts varies widely. For example, the New York City Police Department has a sophisticated intelligence operation, which has grown and operates with little public oversight. Likewise, the Los Angeles Police Department has a very sophisticated intelligence gathering and integration program. Other cities, as well as tribal police forces, have much less sophisticated operations.

Some of the entities that engage in intelligence collection operate under guidelines. Indeed, there is no lack of guidelines on domestic intelligence. The guidelines in place include:

- The Attorney General's Guidelines for Domestic FBI Operations (September 29, 2008) http://www.usdoj.gov/ag/readingroom/guidelines.pdf.
- Department of Justice, Office of Justice Programs, Global Justice Information Sharing Initiative ("Global"), "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era – Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels -- Law Enforcement Intelligence, Public Safety, and the Private Sector" (2006) http://www.it.ojp.gov/documents/fusion_center_guidelines.pdf.
- Program Manager - Information Sharing Environment (PM-ISE), Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment (2006) http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf. See http://www.ise.gov/pages/privacy-implementing.html for related materials.
- PM-ISE, Nationwide Suspicious Activity Reporting Initiative – Concept of Operations (December 2008) http://www.ise.gov/docs/sar/NSI_CONOPS_Version_1_FINAL_2008-12-11_r5.pdf . For further information on governance of the SARs program, see http://www.ise.gov/pages/sar-initiative.html.
- Law Enforcement Intelligence Unit (LEIU), Criminal Intelligence File Guidelines (revised March 2002) http://www.it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf.
- LAPD, Major Crimes Division Standards and Procedures (March 18, 2003) http://www.lapdonline.org/search_results/content_basic_view/27435.
- Memorandum of Agreement Between the Attorney General and the Director of National Intelligence on Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center of Terrorism Information Contained within Datasets Identified as Including Non-Terrorism Information and Information Pertaining Exclusively to Domestic Terrorism (2008) http://fas.org/sgp/othergov/intel/nctc-moa2008.pdf.

Remarkably, there does not seem to be a set of intelligence guidelines for the Department of Homeland Security or for any of its intelligence-collecting

components. However, the main problem we see is not the lack of guidelines per se, but the fact that the guidelines that have been issued so far fail to provide adequate guidance. They either permit intelligence collection without a predicate, as the Attorney General guidelines do,[3] or they provide generic, unhelpful guidance, stating that "all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders," as the ISE guidelines do. We appreciate that guidelines must be tailored to the nature and mission of the entity, the places where it conducts its operations (whether primarily within the U.S. or abroad), and the type of information it collects. However, there does not seem to be a set of principles that guides the overall intelligence effort and protects civil liberties. There are a lot of cooks in the homeland security intelligence kitchen, and they are each using different recipes.

Who Shares and Analyzes Homeland Security Intelligence Information?

As the 9-11 Commission found, and numerous other reports have confirmed, better sharing of intelligence and criminal information is needed to uncover and head off terrorist plans. Just last week, the Markle Foundation Task Force on National Security in the Information Age called for a recommitment to information sharing:

> The President and Congress must reaffirm information sharing as a top priority, ensuring the policy makers have the best information to inform their decisions. … If there is another terrorist attack on the United States, the American people will neither understand nor forgive a failure to have taken this opportunity to get the right policies and structures in place.[4]

A number of information-sharing structures have been established that could be effective in heading off terrorist attacks by sharing homeland security intelligence information. However, they have overlapping missions and insufficient guidance to protect civil liberties.

Information Sharing Environment: The ISE, created by Congress and housed in the Office of the Director of National Intelligence, is a potentially revolutionary effort to

---

[3] CDT's analysis of the Attorney General Guidelines can be found here: http://cdt.org/publications/policyposts/2008/16.

[4] Markle Foundation Task Force on National Security in the Information Age, *Nation at Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, p. 1. CDT was represented on the steering committee that produced the report and it receives financial support from the Markle Foundation.

create a means for sharing terrorism, law enforcement and homeland security information across federal agencies and among state, local and tribal police forces. The types of information that will be exchanged are broadly defined, and tens of thousands of law enforcement and intelligence officials will have access to the information.

The ISE is scheduled to go operational this summer. However, the privacy guidance for the ISE is woefully inadequate. For example, the guidance calls for agencies to develop redress mechanisms to handle complaints about decisions made based on faulty information, but at the same time allows them to decide not to adopt redress mechanisms on the ground that they would be inconsistent with the agency's mission.[5]

National Counterterrorism Center: The NCTC employs more than 500 people, drawn from 16 federal departments and agencies to integrate and analyze counterterrorism intelligence, much of which fits under the homeland security intelligence umbrella. It produces detailed assessments to help senior policy makers make decisions. To facilitate information sharing, the NCTC has access to more than 30 intelligence, military and law enforcement networks. Unlike the ISE – which operates more as a pointer system to data maintained by various agencies – the NCTC also takes in copies of data from other agencies, creating its own depository of data that is analyzed and shared. Among other functions, the NCTC maintains a consolidated repository of information about the identities of terrorists from which is derived, among other subsets of data, the watchlist used to screen airline passengers.

E-Guardian: E-Guardian can be thought of as the FBI's own version of the ISE. It permits the sharing of unclassified information relating to terrorism with 18,000 entities, including state and local law enforcement entities. It also helps them submit their own information to the FBI. According to a DOJ Inspector General's report, its

---

[5] In February 2007, CDT issued an analysis of the ISE privacy guidelines. http://www.cdt.org/security/20070205iseanalysis.pdf. We noted that the guidelines never actually define what privacy is. The title and text of the guidelines refer to "other legal protections," but never explain what those are either. The guidelines never mention the First Amendment or free speech. The cover memorandum to the guidelines includes one reference to Fair Information Practices, and the guidelines themselves contain some of the FIPs. However, there is no engagement with the challenges of applying the Fair Information Practices in the terrorism context. CDT is preparing a further major study of all of the privacy materials associated with the ISE; our results should be available early this summer.

companion system, Guardian, which contains terrorism tips and reports by federal agencies, suffers from numerous data integrity failures, including failure of supervisors to conduct a review to determine whether a threat was adequately addressed, and failure to create a complete record for fully 30% of examined records.[6]

Fusion Centers: State and local governments have created at least 58 fusion centers to improve information sharing across all levels of government to prevent terrorism and other crimes, and in some cases, to respond to public health and other emergencies. Non-federal law enforcement entities, such as state police, are the lead agencies in most of the centers, though most have federal personnel, usually from the FBI and DHS. The National Strategy on Information Sharing that President Bush issued in October 2007 indicates that the federal government will provide grants, training and technical assistance, and Congress has appropriated funds to provide financial support to fusion centers. Each fusion center is different, but there continue to be questions about their mission and effectiveness and they face significant challenges. Officials in over half of the fusion centers contacted by the Government Accountability Office for a recent report said that they had encountered challenges in accessing federal information systems, while at the same time over half reported that the heavy volume of information they were receiving and the existence of multiple systems with redundant information were difficult to manage.[7]

Joint Terrorism Task Forces: JTTFs are comprised of federal, state and local law enforcement officers and specialists. The JTTF concept pre-dated 9/11 by several decades but was expanded after 9/11 and there are now 100 JTTFs, including one in each of the FBI's 56 field offices nationwide. DHS entities involved in JTTFs include Customs and Border Protection and Immigration and Customs Enforcement. Fifteen other federal law enforcement and intelligence agencies are involved in one or more JTTFs.

---

[6] U.S. Department of Justice, Office of the Inspector General Audit Division, November 2008, *The FBI's Terrorist Threat and Suspicious Incident Tracking System*, http://www.usdoj.gov/oig/reports/FBI/a0902/final.pdf.

[7] Testimony of Eileen R. Larence, Director of Homeland Security and Justice Issues at the Government Accountability Office before a subcommittee of the Senate Committee on Homeland Security and Governmental Affairs, April 17, 2008, http://hsgac.senate.gov/public/_files/LarenceTestimony.pdf, pp. 8-9.

What Civil Liberties Violations Have Been Uncovered?

Monitoring of Peaceful Political Activity: Despite the secrecy surrounding the collection of homeland security intelligence, a number of abuses and instances of misguided focus on peaceful activity have already been uncovered, revealing a shocking lack of priorities that is inexplicable in a time of genuine threats. The ACLU has compiled some of these reports;[8] we mention only a few of the more egregious ones here:

- **Maryland State Police Surveillance of Peaceful Anti-War and Anti-Death Penalty Activists** - As reported in the Washington Post: "Undercover Maryland State Police officers conducted surveillance on war protesters and death penalty opponents [from March 2005 until May 2006] … ." "Organizational meetings, public forums, prison vigils, rallies outside the State House in Annapolis and e-mail group lists were infiltrated by police posing as peace activists and death penalty opponents, the records show. The surveillance continued even though the logs contained no reports of illegal activity and consistently indicated that the activists were not planning violent protests."[9] The state police classified 53 nonviolent activists as terrorists and entered their names in state and federal terrorism databases.[10]
- **Reporting on Lobbying Activities and Concern about Tolerance**: The North Central Texas Fusion System distributes a bi-weekly Prevention Awareness Bulletin to over 1500 staff in 200 Texas agencies. The bulletin issued on February 19, 2009, under the headline "Middle Eastern Terrorist groups and their supporting organizations have been successful in gaining support for Islamic goals in the United States and providing an environment for terrorist organizations to flourish," cited incidents ranging from the installation of footbaths at the Indianapolis airport to the Treasury Department's hosting of a conference entitled "Islamic Finance 101," as signs of growing tolerance for "Shariah law and support of terrorist military activity against Western nations." The report expressly singled out "lobbying activities" and concluded by warning that "it is imperative for law enforcement officers to report these types of

---

[8] http://www.aclu.org/privacy/gen/32966pub20071205.html.

[9] Lisa Rein, "Police Spied on Activists in Md.," July 18, 2008 p, A1, http://www.washingtonpost.com/wp-dyn/content/article/2008/07/17/AR2008071701287_pf.html

[10] Lisa Rein, "Md. Police Put Activists' Names on Terror Lists," October 8, 2008, P. A1 http://www.washingtonpost.com/wp-dyn/content/article/2008/10/07/AR2008100703245.html

activities to identify potential underlying trends emerging in the North Central Texas region."[11]

- **Compiling Nationwide Lists of Marches and Rallies:** At least as of 2006, the Intelligence Branch of the Federal Protective Service in DHS was compiling a "Protective Intelligence Bulletin," mainly by using a "media reporting service" available on the Internet. The March 3, 2006 bulletin,[12] 17 pages long, listed dozens of events such as a "Three Years Is Too Many Demonstration" by the Central Vermont Peace and Justice Center to be held at 1400 hours on the sidewalk in front of Main Street Park in Rutland. Recipients were advised that the Bulletin should be shredded or burned when no longer required.

These reports are reminiscent of the 1960s or 1970s in their confusion between peaceful dissent and violent activity. The misallocation of resources alone is cause for serious concern when the nation faces genuine threats. The potential for a chilling of the exercise of First Amendment rights compounds the concern. Department heads and elected officials, especially appropriators, at the federal, state and local level should hesitate before supporting continuation or expansion of homeland intelligence activities until there are rules in place that require a focus on the potential for violence, training programs that distinguish between political activity and terrorist activity, and oversight mechanisms to ensure that prohibitions against First Amendment monitoring are being adhered to.

Overbroad collection of information with SARs. State, local, tribal and federal entities are collaborating to develop a nationwide system of Suspicious Activity Reporting. The SARs system is just getting off the ground, but so far, the standards for the program suggest that much innocent activity will be tracked. For example, photographing bridges is described as a suspicious activity, even though such sites are regularly photographed by tourists, journalists and photography buffs.

The risks we are concerned with develop when such "suspicious activity" is recorded and shared with information identifying the person engaged in the "suspicious activity." What prevents the mistaken conclusion that a person is a terrorist because he or she is the subject of two or more SARs, each reporting on innocent behavior? Won't the next official who encounters the same person in a different context and files a SAR to report other innocent activity assume that his or her suspicion is confirmed because of the initial SAR in the system? Will the subject even know how the data is being used or what further scrutiny he faces? How does

---

[11] The North Central Texas Fusion System Bulletin is available on the Defending Dissent website, http://www.defendingdissent.org/spying.html.

[12] The Bulletin is posted here: http://www.defendingdissent.org/ICECalendar.pdf.

an individual ever prove the legitimacy of his activity when the object of the process is not evidence but only suspicion? Taking in huge amounts of personally-identifiable information about innocent activity and creating self-generating affirmations that make it more likely that yet more information will be taken in does not seem to be the most effective way of conducting intelligence.

What Can Be Done To Address These Problems and Properly Focus Homeland Security Intelligence?

Require DHS entities to follow principles of fair information practices, including the minimization principle. The internationally-accepted principles of Fair Information Practice ("FIPs") establish a useful framework for using information to make fair decisions about people. There is no single authoritative statement of the FIPs, but the DHS Privacy Office on December 29, 2008 issued a memorandum[13] adopting FIPs as its privacy policy framework, and indicated that it would seek to apply them to the "full breadth and diversity of DHS programs and activities." The DHS Privacy Office language is attached as an appendix. If implemented, these principles would require DHS to:

- Give notice of collection and use of Personally Identifiable Information (PII)
- Seek consent, to the extent practicable, for collection and use of PII
- Articulate the purpose for collecting PII
- Collect only PII that is necessary to accomplish the specified purpose
- Use PII only for the purpose specified
- Ensure that PII collected is accurate, relevant, timely and complete
- Safeguard PII against unauthorized access and improper disclosure
- Audit actual use of PII to demonstrate compliance with these principles

Clearly, not all of these concepts can be implemented in the homeland security context in the way that they are applied in the government benefits context, where they originated. One cannot, for example, seek consent from the next Mohammed Attah for the sharing of information about his plotting with al-Qaeda operatives among elements of the intelligence community. However, the principles do offer an excellent framework for analyzing intelligence collection practices. While the DHS Privacy Office took its action at the end of the last Administration, the new leadership of DHS could carry forward this effort to develop department-wide policies in the detail necessary for effective implementation.

[13] *Privacy Policy Guidance Memorandum*, issued December 29, 2008 by Hugo Teufel III, Chief Privacy Officer, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

Applying these principles to, for example, the functioning of fusion centers, would help alleviate the civil liberties concerns that they have created. Indeed, the DHS Privacy Impact Assessment (PIA) [14] for the Fusion Center Initiative, also issued last December, goes some distance toward accomplishing this goal. The Subcommittee should use its oversight authority to see that the recommendations in the PIA are being implemented.

However, because state and local governments run the fusion centers, the PIA recognizes that adoption of effective privacy guidelines to implement FIPS at each fusion center is largely within the control of local agencies. Materials that will address the privacy protections required of fusion centers participating in the ISE are still under development. The DHS Office of Intelligence and Analysis, which leads the effort to create effective fusion centers, could also work with the DHS Privacy Office to ensure that the fusion centers it helped create comply with these principles, especially the "Data Minimization" principle. Full fusion center compliance would mean that only the information necessary to accomplish the center's purposes would be collected.

Require a criminal predicate where appropriate. Probably the single most effective civil liberties protection that could be imposed on the collection and sharing of homeland security intelligence that includes personally identifiable information would be to require criminal predication. This means that information is collected or shared only because it has some degree of relevance to a violation of the law. Requiring a criminal predicate in effect requires the person who gathers or shares information to focus on potential wrongdoers, and not on everyone else. Conversely, failure to require a tie to crime invites reliance on inappropriate predicates for collection and sharing of information, such as fear fostered by fiery speech, or by race and religion.

Requiring a criminal predicate for the collection and sharing of PII through homeland security intelligence is not inconsistent with the purpose of an intelligence system because at bottom, these systems are designed to prevent, investigate or respond to terrorist activity that is a crime.

This principle is captured in 28 CFR Section 23, the guidelines that govern federally funded criminal intelligence systems. These systems are used to exchange information much of which constitutes homeland security intelligence information. The guidelines provide that any federally-funded project shall collect and maintain criminal intelligence information concerning an individual or organization only if

---

[14] *U.S. Department of Homeland Security Privacy Impact Assessment for the Department of Homeland Security State, Local and Regional Fusion Center Initiative,* December 11, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf.

there is reasonable suspicion that the individual or organization is involved in criminal conduct. *28 CFR Section 23.20(a)*. To the extent that fusion centers operate federally funded criminal intelligence systems, those systems are bound by this regulation. Still, there is considerable concern that the protections of the reasonable suspicion standard are diluted when federally-funded fusion centers collect and share vast amounts of SAR information that does not meet the standard. We would suggest that this is an area ripe for oversight by this Subcommittee.

Guard Against Circumvention of Applicable Guidelines. Circumvention of 28 CFR Section 23 requirements illustrates another danger of inappropriate use of intelligence sharing mechanisms such as fusion centers. Another circumvention problem that has not yet been adequately addressed relates to the investigative guidelines under which many law enforcement entities operate and under which the FBI operates. These guidelines can take a number of forms and will have a variety of provisions designed to protect civil liberties. For example, often following litigation, a police department may adopt guidelines that prohibit it from conducting surveillance of protest activity except when directly tied to criminal activity. The FBI operated under Attorney General Guidelines that included such a restriction, but it was largely removed in 2002. Such restrictions are designed to protect against a chilling of controversial political speech.

However, a partner agency, with which the restricted agency may share information through the ISE, a fusion center, or another mechanism, may have no such limitations. It could conduct the surveillance that its partner agency is specifically barred from conducting and share the fruits with the restricted agency. The civil liberties protections embedded in the guidelines that govern activity of the restricted agency would be circumvented. To our knowledge, no adequate mechanism or binding and enforceable rule precludes the circumvention of such guidelines. The circumvention problem can flow across state and local agencies, and from or to federal agencies that participate in the information sharing enterprise.

Avoid redundancies. As we mentioned above, there are already a lot of cooks in the intelligence information sharing and collection kitchen. The Subcommittee should guard against adding more just because a specific new need for information has been identified. The first step should be to ask whether the information needed is already being collected and shared through a system that could be employed to this purpose.

Take a comprehensive look at homeland security intelligence collection now taking place. The Subcommittee, in exercising its oversight role, should sample intelligence products developed by DHS components to more fully ascertain what is being collected, how it is used, and whether it is useful in preventing terrorism. The Subcommittee should consider whether more targeted collection efforts would be

more effective. Finally, the Subcommittee should review the training materials that DHS entities use. The review should be conducted with an eye toward ascertaining whether DHS officials are being trained to avoid inappropriate surveillance, such as the monitoring of death penalty opponents by the Maryland State Police.

The Subcommittee could also identify processes that work at one agency and that might be a source of useful guidance to another component or agency facing similar challenges. For example, the Transportation Security Administration has developed redress procedures for air travelers who believe they have been watch-listed inappropriately. While the procedures are not perfect and there are reports that some travelers have found them ineffective, they are an example of an approach to redress in a security environment from which lessons could be learned and applied to other security environments.

Conduct an independent assessment of the value of SARs reporting. The Subcommittee should test whether SARs reporting is both effective and efficient in preventing terrorism. This may involve commissioning a GAO study or conducting an independent staff level assessment. SARs reporting may or may not be the best way to collect the "dots" that need to be connected to head off terrorist attacks; whether it is or is not should be tested. Because the SARs reporting system will result in the collection of so much information about innocent activities, it seems that it would be good to know at the front end that the results are likely to be worth the risks.

Conclusion

Many entities at the federal, state and local level gather and share homeland security intelligence. More and more information is being collected and shared about innocent activity, creating increased risks to civil liberties. Some of these risks have matured into abuses, including the monitoring of First Amendment activity without adequate cause. Oversight that is focused on ensuring adherence to principles of Fair Information Practices, requiring a criminal predicate to support collection and sharing of personally identifiable information, and compliance with strong privacy protective guidelines would enhance both liberty and security.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

Please contact: Brock Meeks
Director of Communications
202-637-9800

Appendix: Principles of Fair Information Practices as Articulated by the DHS Privacy Office[15]

- Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).

- Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

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

- 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).

- Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

- Data Quality and Integrity: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

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

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

---

[15] *Privacy Policy Guidance Memorandum*, issued December 29, 2008 by Hugo Teufel III, Chief Privacy Officer, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf