Statement of Jerry Berman
President
Center for Democracy & Technology[1]

before the
Subcommittee on Crime, Terrorism and Homeland Security
of the House Judiciary Committee
and the
Subcommittee on Intelligence and Counterterrorism
of the House Select Committee on Homeland Security

"Progress in Consolidating Terrorist Watchlists –
The Terrorist Screening Center (TSC)"

March 25, 2004

Chairman Coble, Chairman Gibbons, Ranking Member Scott, Ranking Member McCarthy, Members of the Subcommittees, thank you for the opportunity to testify today. I am President of the Center for Democracy and Technology. We commend you for holding this public oversight hearing on the Terrorist Screening Center (TSC), its role in the nation's counter-terrorism efforts, its relationship with federal, state and local agencies, and its implications for civil liberties. Better information sharing, including the sharing of terrorist watch list entries, is critical to our nation's efforts to combat terrorism. Information sharing will be effective only if it is managed well, with some entity within the Executive Branch having clear responsibility for implementation; if it takes full advantage of available technology, which can be leveraged both to facilitate appropriate information sharing and to protect privacy; and if it is subject to guidelines and oversight mechanisms that will protect civil liberties. Specifically with regard to the consolidation of terrorist watch lists taking place at TSC, there are serious unanswered

[1] The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties, privacy, and democratic values for the digital age.

questions about how various Executive Branch agencies are working together, which agency is (or should be) ultimately responsible, how state and local authorities participate, what it means to have an integrated watch list, what criteria there are for entering data, for sharing it and for using it as the basis of action, and what guidelines and oversight mechanisms apply to protect privacy and civil liberties. We urge you to seek answers to these questions and to continue this oversight process, and we look forward to being of assistance to you however we can.

I. INTRODUCTION

The threat terrorism poses to our nation is imminent and grave. There is no doubt that hostile groups are continuing to plan attacks in this country and abroad. To prevent terrorism to the greatest extent possible and to swiftly punish it when it occurs, the government must have adequate legal authorities and must develop a strong organizational structure. Improved intelligence collection and better sharing of information are central to success. One key component of terrorism prevention efforts is the creation, maintenance and use of watch lists. It is now clear that, before 9/11, the government was unable to use effectively the information that it was collecting. In particular, before 9/11 the government knew two of the hijackers by name and knew that they were very likely al Qaeda members planning an attack, but that information was not made available in a timely fashion to the border control authorities, so those men were able to enter the country. And that information was not available to airline security, so those men were able to board the aircraft on September 11. Clearly, it is a desirable and urgent goal to make better use of information technology to share information about individuals known to be terrorists.

II. MANAGEMENT, OVERSIGHT AND THE USE OF TECHNOLOGY

As the Markle Foundation Task Force on National Security in the Information Age has found, steps have been taken at the federal, state, and local levels to broaden the sharing of terrorist-threat data among government agencies at all levels and to improve analysis of terrorism-related information.[2] To date, however, the government is still a long way from having a dynamic, distributed network for sharing and analysis of information, including watch list data. The sharing of terrorist-related information between relevant agencies at different levels of government has been only marginally improved in the last year, and remains haphazard. It is still comprised of multiple systems that cannot communicate with each other and institutional barriers to sharing information. It is not the result of a carefully considered network architecture that optimizes the abilities of all of the players.[3]

Nor is there a clear framework for agencies' individual responsibilities. The Terrorist Screening Center, as part of the FBI, has been tasked with creating a consolidated watch list and disseminating appropriate watch list information to government officials and private sector entities. But watch listing involves multiple agencies at various levels of government, and it is not clear who within the Executive Branch is ultimately responsible. TSC is a crucial link in the

---

[2] The Markle Foundation Task Force on National Security in the Information Age, co-chaired by Zoe Baird and Jim Barksdale, is comprised of leading experts from the fields of national security, technology, and privacy. Its members have extensive experience in and out of government at the federal and state level, in both the legislative and executive branches. The Task Force has published two reports, "Protecting America's Freedom in the Information Age"(2002) and "Creating a Trusted Information Network for Homeland Security" (2003), containing recommendations to strengthen national security while protecting civil liberties. While I quote liberally from the reports of the Task Force, I speak only on behalf of CDT.

[3] Markle Foundation Task Force, "Creating a Trusted Information Network for Homeland Security," at 7 (Dec. 2003), *available at* <http://www.markletaskforce.org>.

information chain, but who is ensuring the coordination of information sharing across the government, including the sharing of TSC information? Who is in charge of establishing the guidelines and safeguards for government-wide information sharing efforts?[4]

The Markle Task Force concluded that, for effective information sharing, the Executive Branch must clarify the respective roles, responsibilities, and authorities of the players responsible for homeland security information. The respective roles of the TSC, TTIC, the DCI's Counterterrorist Center (CTC), the Department of Homeland Security, the FBI and its JTTFs, and the Defense Department's Northern Command (NORTHCOM) are not clearly defined. As long as this remains true, there will be turf battles among agencies and gaps in information sharing and analysis.[5] Most significantly, without defined roles, responsibilities and oversight, civil liberties will fall through the cracks.

Resolving these issues is no easy matter. Information technology has much to offer in achieving the compelling national goal of preventing terrorism. At the same time, government use and dissemination of personal information raises privacy and related due process issues. Current privacy laws are not well-suited to the modern digital data environment. It is necessary to adopt new policies for collection and access, use, disclosure and retention of information, and for redress and oversight, as will be discussed further below. Technology itself should also be part of the solution. The same technology that permits the accumulation, sharing and analysis of

[4] This question is all the more important because the watch list consolidation task was initially given to DOJ's Terrorist Tracking Task Force, then moved to DHS, then seemingly to TTIC, and now is back within DOJ at the FBI's Terrorist Screening Center.

[5] Markle Foundation Task Force, "Creating a Trusted Information Network for Homeland Security," at 26 Exh. F (Dec. 2003), *available at* <http://www.markletaskforce.org>.

information also allows for the incorporation into information sharing systems of features that protect information from abuse or misuse.

A key finding of the Markle Task Force is that technologies exist *today*, *off-the-shelf*, that can both facilitate information sharing and protect privacy. The second Markle Foundation Task Force report explains in detail how commercially available technologies can be adopted to create a government-wide information sharing network.[6] The Task Force calls this the SHARE Network, for "Systemwide Homeland Analysis and Response Exchange." It is important that your Committees encourage TSC to fully leverage the security- and privacy-protective capabilities of existing technology.

III. WATCH LISTS, PRIVACY AND CIVIL LIBERTIES

Information sharing, including the sharing of watch list entries, is a crucial building block in combating terrorism. The improvement of watch lists is a daunting task. In April 2003, the GAO issued a report on federal watch lists, finding that nine agencies maintain 12 different watch lists, that the lists contain overlapping but different information, and that the agencies had different policies governing when and how information on the lists is shared with others. It also found that sharing is constrained by the watch lists' differing technological architectures.[7]

---

[6] *See* Markle Foundation Task Force, "Creating a Trusted Information Network for Homeland Security," at 16-19 (Dec. 2003), *available at* <http://www.markletaskforce.org>. Appendix G of the Task Force's second report, at pages 144-148, sets forth in detail the technology needed to implement the sharing network.

[7] GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated To Promote Better Integration and Sharing*, GAO-03-322 (April 2003), *available at* <http://www.gao.gov/new.items.d03322.pdf>.

Improving these watch lists is not simply a matter of putting them all together into a single list of names. Each of these watch lists was created for a different purpose, using different criteria. Some include only foreign nationals; others include citizens. Some watch lists are comprised of persons who are subject to exclusion from the U.S., but are not otherwise subject to arrest or detention. Others are subject to arrest on a criminal warrant. Still others are citizens or foreign nationals subject to neither arrest nor detention, but having some interest to intelligence or law enforcement agencies. In any given category, for some people, the government has a high level of assurance that they are dangerous terrorists. Others are suspected of being dangerous, but on thin evidence. Others are soundly believed to be associated with a terrorist group but are not suspected of being involved in any illegal conduct.

As the Markle Task Force found, to date, no government-wide guidelines have been issued concerning how individuals get placed on — and removed from — a watch list; how accuracy is maintained and errors are corrected across lists; or how information on the lists is shared among agencies and with private companies.[8] Furthermore, if there is a watch list "hit," law enforcement and security personnel may not be clear on how to respond. A police officer conducting a routine traffic stop, an airline screener and an immigration official would each react differently to the same "hit." Any one of them might react differently depending on whether the "hit" is an individual who is a known, dangerous terrorist, or is merely someone with tangential ties to someone who is subject to an investigation, assuming that specific information were made available to the officer on the front lines. The question before us today is whether TSC is resolving any of these critical issues.

---

[8] *See* Markle Foundation Task Force, "Creating a Trusted Information Network for Homeland Security," at 9 (Dec. 2003), *available at* <http://www.markletaskforce.org>.

There are a number of fundamental questions associated with the watch list activities of the TSC: The first is who meets the standard (or standards) for inclusion on the TSC watch list? Is TSC establishing those standards, or is TSC following the different standards of the different agencies' lists? According to Secretary of Homeland Security Ridge, the current TSC list includes 50,000 names, but only some small subset of those individuals are wanted criminals.[9] How did the rest of the names get on that list? Who determines which watch list entries are shared and with whom? Given the necessarily wide range of criteria and the wide ranges of uses to which a consolidated list might be put, these are not easy questions. At the least, however, the criteria must be publicly stated and subject to debate and oversight. This might involve both a criterion of proximity to terrorist activity (e.g., member, associate, associate of associate) and a criterion representing a certain threshold of information justifying the inclusion (e.g., reason to believe based on specific and articulable facts).

A related concern is data quality. Little information is publicly available about how U.S. watch lists are compiled and maintained, but numerous reports have suggested that current watch lists are deeply flawed.[10] As an FBI official explained last year to a congressional subcommittee with respect to FBI watch lists, "many times there is insufficient data that [could be used to] accurately make a determination that it was in fact [the person on the list] because there's no date

---

[9] *See Fiscal Year 2005 Appropriations for the Department of Homeland Security: Hearing Before the Subcomm. on Homeland Security of the House Appropriations Comm.*, 108th Cong. (Mar. 4, 2004) (statement of Secretary Tom Ridge).

[10] *See* documents obtained by the Electronic Privacy Information Center through FOIA, *available at* http://www.epic.org/privacy/airtravel/foia/watchlist foia analysis.html; GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (April 2003), *available at* www.gao.gov/new.items/d03322.pdf; Ann Davis, *Boarding Impasse: Why a 'No Fly List' Aimed At Terrorists Delays Others*, Wall St. J. (Apr. 22, 2003), at A1.

of birth, biographical data or other relational type of data."[11] The adoption of data quality standards is therefore critical. If a watch list contains inaccurate or incomplete data, it will be very difficult to compare data against that list. In particular, name-only matches are meaningless; more information is necessary to determine whether an individual is, in fact, the person listed. In terms of the government's use of data, this suggests that watch lists need to be verified to ensure they are accurate, complete and up to date, and this is particularly important if watch lists become the centerpiece of any screening system.

Another fundamental question concerns dissemination. A determination has been made to add TSC watch list entries to the National Crime Information Center (NCIC) so that when state and local officials run queries through NCIC, "hits" are returned if an individual is on the TSC list. This represents a significant change in the purpose of NCIC, and it comes shortly after the FBI announced it would no longer consider NCIC bound by the accuracy and data quality requirements of the Privacy Act.

It also raises the fundamental question of consequences: What do police officers on the beat do when they get a TSC "hit" for someone who is not subject to arrest? How does the system handle, for example, someone the FBI just wants to track but doesn't want that person to know they are tracking him? What information is provided to state and local officials about how to respond, and what ability do they have to communicate immediately with federal officials?

Likewise, what do airline screeners and private sector entities do with this information if they are screening an individual and get a "hit"? How widely will watch list information be

---

[11] *See Can the Use of Factual Data Analysis Strengthen National Security? – Part One: Hearings Before the Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census of the House Comm. on Gov't Reform*, 108th Cong. at 9 (May 6, 2003) (statement by William L. Hooten).

available to the private sector? Will it be used to deny someone a job? TSC cannot share information about individuals indiscriminately with public and private entities, both for security reasons and to protect civil liberties.

A further fundamental question is redress. What are the due process rights associated with being denied a job or other privilege on the basis of a watch list entry? TSC's watch list is going to be used by government agencies and private entities for a variety of screening processes, from employment to airline security. Serious consequences will result for individuals who end up on the TSC watch list, from being denied the ability to board an airplane to being denied jobs in the private sector. Such denials of basic rights cannot be taken lightly. It is critical that a redress process is in place and careful oversight is conducted.

I also want to call your attention to an important First Amendment issue. The TSC Director has stated that the consolidated TSC watch list will include "domestic terrorist" entries obtained from the FBI. But who is a "domestic terrorist? We cannot place individuals on a watch list for exercising their First Amendment rights. Yet we know, for example, that just last month the FBI served a subpoena on Drake University about an anti-war conference held there, and that last year New York police officers questioned anti-Iraq war demonstrators about their political activities and associations.

For purposes of TSC's work, how is a "domestic terrorist" defined? Does the term "domestic terrorist" include an anti-abortion activist who breaks the law by blocking access to abortion clinics or who may be organizationally or ideologically related to those who have killed doctors or committed arson at clinics? Does it include members of Earth First or other radical environmental groups that have engaged in illegal acts and have been investigated by the FBI as domestic terrorist organizations? This concern is amplified by the fact that the only statutory

definition of "domestic terrorism" in the U.S. Code is overbroad. As defined in the USA PATRIOT Act, the term "domestic terrorism" casts a wide net, and potentially covers political protesters engaging in civil disobedience.[12] This broad definition blurs the line between "terrorism" and aggressive or unseemly political activity protected by the First Amendment.

IV. CONCLUSION

It is clear that the compilation and use of watch lists is a fundamental and urgent component of our nation's response to terrorism. Many questions remain about the Terrorist Screening Center's approach to this task. Questions include:

- What consequences might result from an individual being on the TSC list?
- For what purposes will agencies and private entities be permitted to access this information?
- What guidelines are in place to govern the sharing of information with private entities?
- When private entities use TSC's information for screening employees and other uses, how will government information be protected?
- What redress do individuals have if they are denied a job by a private company? unable to board an airplane? arrested?
- Ultimately, how can individuals challenge the fact that they are subject to a watch list entry?
- Who has oversight of TSC?

As the Markle Task Force concluded, the need to create an effective network for sharing counter-terrorism information is more urgent than ever. Terrorism remains a continuing threat

[12] *See* Pub. L. No. 107-56, § 802, codified at 18 U.S.C. § 2331(5).

around the world. And the potential for terrorists to use weapons of mass destruction raises the stakes considerably. Building the technical architecture, changing agency cultures, establishing new rules and procedures, and securing the necessary funding all take time. It is therefore imperative that the Executive Branch and Congress implement the measures necessary to create an information sharing network that would empower federal, state and local officials to be full and active partners in protecting our security, and that would be governed by guidelines designed to protect our liberties. Watch lists are a critical aspect of that network, but also raise the stakes on civil liberties.

We commend the Committees for holding this hearing. We urge you to continue the process of oversight and we look forward to working with you to achieve the inextricably linked goals of enhancing our national security and protecting our constitutional liberties.