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

before the
House Committee on the Judiciary
and the
House Select Committee on Homeland Security

"The Terrorist Threat Integration Center (TTIC) and its Relationship with the Departments of Justice and Homeland Security"

July 22, 2003

Chairman Sensenbrenner, Chairman Cox, Ranking Member Conyers, Ranking Member Turner, Members of the Committees, thank you for the opportunity to testify today at this important hearing. We commend you for beginning public oversight of the Terrorist Threat Integration Center (TTIC), its role in the nation's counter-terrorism efforts, its relationship with the Departments of Justice and Homeland Security, and its implications for civil liberties. The Center for Democracy and Technology believes that it was a serious mistake for the President to place the TTIC under the Director of Central Intelligence, because it appears to have been cut loose from the oversight mechanisms that Congress specifically created for the intelligence fusion and analysis function that Congress placed at the Department of Homeland Security. Regardless of where TTIC is organizationally located, there are major unanswered questions about the collection,

---

[1] The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media. Our core goals include enhancing privacy protections and preserving the open architecture of the Internet. Among other activities, CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for

dissemination and consequences of intelligence information that the Executive Branch and these Committees need to address. We urge you, therefore, 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. The government must develop a strong organizational structure capable of preventing terrorism to the greatest extent possible and swiftly punishing it when it occurs. Information sharing and analysis are central to success. It is now clear that, before 9/11, the government was unable to use effectively the information that it was collecting. Moreover, it is clear that privacy laws and constitutional principles were not the main barriers to collection, sharing or analysis. Even before the changes put into place by the PATRIOT Act, the government had very broad authority to infiltrate organizations, collect information from public and private sources, and carry out wiretaps and other forms of electronic surveillance. Overseas, of course, there were few, if any, rules. Since 9/11, the power of the government to collect information domestically has been further expanded. Legal barriers against sharing law enforcement information with intelligence agencies have been eliminated. But information sharing and sound analysis cannot be legislatively mandated. With the TTIC, the President has created a structure that he believes will be better able to conduct analysis and promote information sharing. The first important question the Committees are asking today is whether this new structure will in fact produce better sharing and analysis.

---

computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

At the same time, the Committees are appropriately asking what will be the effect of this new organization on civil liberties. The government's powers, even in this time of crisis, must be subject to checks and balances. Within the United States, surveillance and data gathering should be exercised with a focus on potential violence, guided by the particularized suspicion principle of the Fourth Amendment, and subject to executive, legislative and judicial controls. Yet checks and balances were seriously eroded by the USA PATRIOT Act and Executive Branch actions. When Congress created the Department of Homeland Security in 2002, it attempted to partially address these concerns by creating internal oversight mechanisms in the new Department. If the TTIC is not brought back under the DHS, Congress should respond by establishing standards for sharing of information and its consequences and should establish internal oversight mechanisms for TTIC. Finally, these Committees should continue practicing ongoing, nonpartisan, and in-depth oversight.

II. WHERE IS THE OVERSIGHT OF TTIC?

When Congress passed the PATRIOT Act, it specifically directed the Inspector General of the Department of Justice to designate an official who would review information and receive complaints alleging abuses of civil rights and civil liberties by employees and officials of the Department of justice. The DOJ is required to make public announcements on how to contact this official. And the official is required to submit to the Judiciary Committees a semi-annual report detailing the complaints and findings. PATRIOT Act, Pub. L. No. 107-56, sec. 1001. Last week, such a report was presented to the Judiciary Committee.

Where is the similar function for the TTIC?

When Congress created the Homeland Security Department and gave it responsibility for threat integration and analysis, Congress recognized that the new Department's powers required close internal and external oversight. Congress created within the Homeland Security Department two oversight offices – one for privacy (Sec. 222) and one for civil rights and civil liberties (Sec. 705). Homeland Security may be the only department in government that has such statutorily mandated offices. The Privacy Officer is specifically directed by legislation to take primary responsibility for issues such as:

> (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; and
> (5) 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.

The DHS Civil Rights and Civil Liberties Officer also has an express statutory charge to:

> (1) review and assess information alleging abuses of civil rights, civil liberties, and racial and ethnic profiling by employees and officials of the Department; and
> (2) make public through the Internet, radio, television, or newspaper advertisements information on the responsibilities and functions of, and how to contact, [his office].

Where are the comparable officers for the TTIC?

Other questions could be asked: Who has control over the budget for TTIC? When the FBI's Counterterrorism Division is transferred to TTIC, will the Judiciary Committee still have authorization authority over the Counterterrorism Division?

Who is the FOIA officer for the TTIC? Judicial and Executive Branch interpretations have weakened the Freedom of Information Act as a mechanism for oversight and accountability, but it remains an important element of the system of checks and balances.

What guidelines will govern the dissemination of intelligence from the TTIC to state and local officials? Will those guidelines be public?

These are not concerns that are at odds with the mission of ensuring that intelligence collection, analysis, and dissemination are organized effectively to support the war on terrorism. To the contrary, the answers to these questions will help determine whether TTIC is doing its job. Because the analysis function at DHS is subject to a specific statutory charter, while TTIC lacks one, and because DHS is subject to oversight mechanisms, while TTIC apparently has none, we recommend that TTIC be brought back within DHS.

III. THE NEED FOR A TTIC CHARTER AND GUIDELINES ON INFORMATION SHARING AND ITS CONSEQUENCES

Regardless of where it resides, TTIC needs a charter – something more binding than the testimony you are receiving from government officials today – to delimit what it can and cannot do, including how it can acquire information, how that information can be used, and how individuals obtain redress. In order to appreciate why this is so important, let me describe briefly the domestic intelligence system as it exists today.

Collection Standards: The FBI, the nation's domestic intelligence agency, has both intelligence and law enforcement surveillance powers. In international terrorism investigations, the FBI can exercise either or both sets of powers for maximum collection. Under both the criminal wiretap statute and the Foreign Intelligence Surveillance Act, courts rarely if ever deny requests for electronic surveillance. For access to stored records, the criminal grand jury is a powerful, wide-ranging tool, and Section 215 of the PATRIOT Act gives the FBI the authority to obtain a court order on a minimal showing to compel disclosure of any record in the name of international counter-terrorism.

It has been said that TTIC will not be a collection agency. But it is also said that TTIC will be involved in tasking – that is, in telling other agencies what to collect. Increasingly, CIA agents are working closely with FBI agents. That is in some ways highly desirable and long overdue. But doesn't it mean that the CIA, especially with the TTIC and its tasking function operating under the Director of Central Intelligence, now has access to the very "police, subpoena, or law enforcement powers or internal security functions" that the National Security Act denied to the DCI?

Dissemination: At the same time, the PATRIOT Act broke down the limits on sharing law enforcement information with intelligence agencies. (There were never any statutory limits on sharing intelligence information with law enforcement agencies.) And sharing of information with state and local officials has become a major topic of discussion.

Consequences: What is most significant about this sea-change is that information collected domestically can now be shared and used outside of the confines of

the criminal justice system. In the past, information collected with grand jury powers or Title III powers had to be kept confidential and could be used against a person only when they were accorded the full panoply of due process rights in the criminal justice system. Intelligence information supported the foreign policy process or was used in spy-versus-spy operations, but after the reforms of the Church Committee era was not supposed to be used in ways that affected the rights of Americans outside the criminal justice system. Now that information can be used domestically for other barely defined counter-terrorism and protective purposes. We need to put clearer definition on how that information can be used and what the consequences can be, starting with TTIC.

IV. THE NEED FOR CLOSE CONGRESSIONAL SCRUTINY OF THE EFFECTIVENESS AND PRIVACY IMPLICATIONS OF DATA MINING AND ESTABLISHMENT OF GUIDELINES FOR ANY APPLICATION OF THE TECHNOLOGY

One important avenue of oversight for these Committees is whether, and if so how, the TTIC intends to use the technique known as data mining, which purports to be able to find evidence of possible terrorist preparations by scanning billions of everyday transactions, potentially including a vast array of information about Americans' personal lives such as medical information, travel records and credit card and financial data. We know that other agencies are pursuing this technology, which seems to assume government access to personal information about everyone from any source. The Pentagon's Defense Advanced Research Projects Agency is carrying out research on its Total (now Terrorism) Information Awareness program. The FBI's Trilogy project includes plans for data mining. According to an undated FBI presentation obtained under the FOIA by the Electronic Privacy Information Center, the FBI's use of "public source" information (including proprietary commercial databases) has grown 9,600% since

1992.[2] And the Homeland Security Act provided DHS with explicit authorization to develop data mining technologies.

Two kinds of questions must be asked about data mining.

- First, is the technique likely to be effective?
- Secondly, assuming it can be shown to be effective, what should be the rules governing it?

Current laws place few constraints on the government's ability to access information for terrorism-related data mining. Under existing law, the government can ask for, purchase or easily demand access to most private sector data. Unaddressed are a host of questions:

- Who should approve the patterns that are the basis for scans of private databases and under what standard?
- What should be the legal rules limiting disclosure to the government of the identity of those whose data fits a pattern?
- When the government draws conclusions based on pattern analysis, how should those conclusions be interpreted?
- How should they be disseminated and when can they be acted upon?

Adapting the Privacy Act of 1974 to government uses of commercial databases is one way to look at setting guidelines for data mining. But some of the principles reflected in the Privacy Act are simply inapplicable and others need to have greater emphasis. For example, perhaps one of the most important elements of guidelines for data mining – one that is not part of the Privacy Act – would be rules on the interpretation

---

[2] http://www.epic.org/privacy/publicrecords/cpfbippt.pdf.

and dissemination of hits and on how information generated by computerized scans can be used. Can it be used to conduct a more intensive search of someone seeking to board an airplane, to keep a person off an airplane, to deny a person access to a government building, to deny a person a job? What due process rights should be afforded when adverse actions are taken against individuals based on some pattern identified by a computer program? Can ongoing audits and evaluation mechanisms assess the effectiveness of particular applications of the technology and prevent abuse?

All of these questions must be answered before TTIC (and DHS) move forward with implementation of data mining techniques on commercial databases. Congress should limit the implementation of data mining until effectiveness has been shown and guidelines on collection, use, disclosure and retention have been adopted following appropriate consultation and comment.

V. CONCLUSION

We need limits on government surveillance and guidelines for the use of information not merely to protect individual rights but to focus government activity on those planning violence. The criminal standard and the principle of particularized suspicion keep the government from being diverted into investigations guided by politics, religion or ethnicity. A set of guidelines needs to be issued for the unique intelligence tasking, fusion, analysis and dissemination function now contemplated for TTIC. We believe that those guidelines can best be developed and implemented within the structure of the DHS, with the statutory charter and oversight mechanisms that Congress established.

But first, Congress needs to know what is going on. It needs to see a public, binding charter for TTIC, to define its tasking or collection authorities and protect against mission creep. Congress could start by inquiring into TTIC's use, if any, of commercial databases. And the question of consequences and redress looms large.

For more information, contact:

Jerry Berman
(202) 637-9800
jberman@cdt.org
http://www.cdt.org