

CENTER FOR DEMOCRACY & TECHNOLOGY**Our Mission / Get Involved / Staff / Publications / Links / Search CDT / Jobs / Action!**

October 3, 2001

Testimony, Speeches & Filings

Statement of James X. Dempsey Deputy Director Center for Democracy & Technology

before the House Committee on the Judiciary

on Legislative Measures to Improve America's Counter-Terrorism Programs

September 24, 2001

Summary

Mr. Chairman, Mr. Conyers, members of the Committee, thank you for the opportunity to speak at this briefing on the momentous question of improving our nation's defenses against terrorism in a manner consistent with our fundamental Constitutional liberties.

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 more than 50 computer, communications, and public interest organizations, companies and associations working on information privacy and security issues.

CDT joins the nation in grief and anger over the devastating loss of life resulting from the September 11 terrorist hijackings and attacks against the World Trade Center and the Pentagon. Like many, our relatively small staff had friends and acquaintances killed in those heinous acts. We fervently support the efforts of our government to hold accountable those who direct and support such atrocities.

It is clear that improvements need to be made in America's counter-terrorism procedures, and it appears there are many things that can be done without harming civil liberties. But we know from history that measures hastily undertaken in times of peril - particularly measures that weaken controls on government exercise of coercive or intrusive powers -- often infringe civil liberties without enhancing security. In the current climate, it is all the more important to act deliberately and ensure that our response is balanced and properly targeted. If we give up the constitutional freedoms fundamental to our democratic way of life, then the terrorists will have won.

In that regard, Mr. Chairman, we commend you and the Committee for holding this briefing to consider the legislative proposals put forth by the Administration. Through the hearing process you and the American public must try to understand three things:

1. what is being proposed,
2. how it would affect current law, including the intelligence reforms put in place 25 years ago, and
3. whether the changes are responsive to deficiencies that the September 11 attack may have revealed.

CDT is at your disposal and at your staff's disposal to help answer these questions. Quite honestly, though, I must say that this one session is not likely to resolve the major questions raised by all the proposals. Some of the more fundamental changes being proposed by the Justice Department will best be deferred for more consideration.

If there are specific authorities immediately needed by the current investigators into the September 11 attacks, those authorities could be separated from the rest of the proposals and considered as quickly as possible.

Just as President Bush and his military advisers are taking their time in planning their response, to ensure that they hit the terrorist targets with a minimum of collateral damage, so it is incumbent upon this Congress to avoid collateral damage to the Constitution.

Overview Comments on Administration Proposals

The Administration's Anti-Terrorism Act of 2001 would expand federal government authorities, including the authorities of the intelligence agencies, to conduct electronic surveillance and otherwise collect information on US citizens. Some of the changes are quite fundamental. The bill includes numerous, complex provisions extending the surveillance laws (while raising many questions about how they will be implemented) and altering the long-standing distinction between criminal investigations and foreign intelligence investigations. Upon our hurried analysis over the last several days, this is what we have concluded:

- Many of the changes are not related to security concerns raised by the September 11 terrorist attacks.
- Many, particularly those related to electronic surveillance, are not limited to terrorism cases, but would be permanent changes affecting all investigations. Some have been on the Justice Department's wish list for some time. Some were proposed last year in response to the denial of service attacks on the Web sites of Yahoo and E-Bay.
- A theme that runs throughout the changes, particularly the changes to FISA, is the elimination of judicial review and the substitution of unreviewable discretion of FBI agents.
- The question of information sharing is a very difficult one; it merits being addressed carefully and it is one where a balanced solution may be achieved, yet it is hard to do so at the same time that the standards in the statutes are being lowered. More information sharing between law enforcement and intelligence agencies should call for the strict maintenance of standards within their respective spheres, not a further lowering of the standards. This is especially true under FISA, where the standards were set low on the

understanding that the information would not be used in criminal cases.

In terms of the issues within the jurisdiction of this Committee, these are our top concerns:

- **Section 101. Modification of Authorities Relating to Use of Pen Registers and Trap and Trace Devices.** Most of these changes were considered and rejected by the Committee last year as flawed. The Committee concluded then that rather than being broadened, the pen register and trap and trace statute need to be amended to raise the standard for government access and to build in greater accountability.
- **153. Foreign Intelligence Information.** Allows the FBI to collect evidence for criminal cases under the looser standards of foreign intelligence investigations -- an end-run around the relatively stringent requirements for wiretaps in criminal cases and a breach of the understanding that led to enactment of FISA.
- **Section 155. Pen Register and Trap and Trace Authority.** Eliminates the only meaningful statutory control that exists on use of pen registers and trap and trace devices in intelligence cases.
- **Section 156. Business records.** Allows access to any business records upon the demand of an FBI agent, with no judicial review or oversight.
- **Sec. 157. Miscellaneous national-security authorities.** Amends several key privacy laws, allowing much greater access to banking, credit, and other consumer records in counter-intelligence investigations, with no judicial review at all.
- **Sec 352. Delayed Notice for Searches.** Affects all criminal cases, allowing the government to delay the notice of searches that is a bedrock Fourth Amendment protection from mistaken or abusive searches and seizures. Delayed notice has been allowed in only the most extraordinary circumstances, and only with substantial judicial supervision

The Administration's bill has two kinds of provisions that give rise to concerns: those that would lower the standards for government surveillance and those that address the difficult question of information sharing.

In terms of collection standards, our law enforcement and intelligence agencies already have broad authority to monitor all kinds of communications, including email. Both the criminal wiretap statute and the Foreign Intelligence Surveillance Act already cover terrorism. For some time, it has been recognized that those standards need to strengthen the standards for government surveillance. We see no justification for the changes proposed in the Administration bill that weaken those standards. We are particularly opposed to changes that would eliminate the judicial review that can be the most important protection against abuse.

The Foreign Intelligence Surveillance Act allows the FBI to conduct electronic surveillance and secret physical searches in the US, including surveillance of US citizens, in international terrorism investigations. FISA also authorizes court orders for access to certain business records. As you know, the standards under FISA are much lower than the standards for criminal wiretaps, and in return, the surveillance is supposed to be focused on the collection of intelligence, not criminal evidence. The FISA court, which last year approved more than 1000 surveillance requests, has denied only one request in its 22 year history.

The legal and oversight system for intelligence sprang not just from a concern about civil liberties, but also from a concern about improving the efficacy of intelligence gathering.

Distinct from the Administration's unsupportable desire to avoid judicial controls on its authority, perhaps the central and most important problem facing the Congress is the question of information sharing. For many years, this has been recognized as a very difficult question; it is one that will be especially difficult to resolve satisfactorily given the pressure-cooker atmosphere of this time. We want to work out a balanced solution. But it cannot be done by wiping away all rules and barriers. Any solution needs to preserve the fundamental proposition that the CIA and other intelligence agencies should not collect information on US citizens in the US. A first step should be to develop a better understanding of the extent to which the problems are institutional as compared to legal.

Comments on Specific Provisions

- **Sec. 101. Modification of Authorities Relating to Use of Pen Registers and Trap and Trace Devices.** **Expands, in vague and potentially broad terms, the government's ability to get information about Internet communications under a loose standard. Also allows any magistrate in the country to issue a pen register or trap and trace order that can be served multiple times, anywhere in the country.** - The government claims that it already has authority to collect, under the very weak provisions of the pen register and trap and trace statute, transactional data about Internet communications. But the existing statute, intended to collect telephone numbers, is vague as applied to the Internet. Section 101 compounds the vagueness. It would add the words "addressing" and "routing" to the description of what pen registers and trap and trace devices collect. What do these words mean?
We are concerned that the provision would be cited as expanding the scope of what the government collects, creating a more intrusive form of surveillance. Internet addressing information can be much more revealing than phone numbers and might include information about the content of communications; a URL, for example, which may fit the proposed statutory definition of "addressing" information, may include a specific search term entered into a search engine or the title of a specific book bought at Amazon.com. The bill provides no details on how this content would be separated from other addressing information. *This provision is constitutionally suspect as it could allow government access to content information with minimal judicial oversight, specifically prohibited in a recent DC Circuit Court ruling.* (See *USTA v. FCC.*)
The standard for pen registers is so low as to be meaningless: people whose communications are targeted need not be suspected of any crime; probable cause is not required, only mere "relevance" to some ongoing investigation; courts have no authority to review these orders. Before extending nationwide scope to these orders, the process for their approval needs to be given some meaningful judicial approval. Congress now should use the language approved by the House Judiciary Committee last year in H.R. 5018.
- **Sec 103. Authorized Disclosure** **Allows disclosure of information obtained from wiretaps with any executive branch official.** This is clearly too broad, especially in light of the vague language in 18 USC 2517 that allows sharing when appropriate to the proper performance of the duties of the official **making** or receiving the disclosure. We have three concerns: (1) That the CIA and other intelligence agencies should not begin compiling files on US persons. (2) That the sharing of information should be subject to prior judicial approval. (3) This provision should be narrowed, so that it authorizes disclosures to personnel with intelligence, protective, public health or safety, or immigration duties, to the extent that such disclosure is related to proper performance of the official duties of the officer receiving the disclosure, and with the proviso that nothing therein authorizes any change in the existing authorities of any intelligence agency. (Rather than amending the definition section of Title III, it might be better to build these concepts directly into section 2517.)
- **Sec. 105. Use of Wiretap Information from Foreign Governments.** **Allows use of surveillance information from foreign governments, even if it was seized in a manner that would have**

violated the Fourth Amendment. Section 105 makes surveillance information collected about Americans by foreign governments (so long as U.S. officials did not participate in the interception) admissible in U.S. courts even if such interceptions would have been illegal in the U.S. Such a provision is ripe for abuse and provides unhealthy incentives for more widespread foreign surveillance of U.S. individuals.

- **Sec. 151. Period of Orders of Electronic Surveillance of Non-United States Persons Under Foreign Intelligence Surveillance.**
Allows secret searches and electronic surveillance for up to one year without judicial supervision. Under current law, the FISA Court can order a wiretap of a "non-US person" for a period of 90 days, after which the government must report to the court on the progress of the surveillance and justify the need for further surveillance. The court can authorize physical searches for up to 45 days. The amendment would extend both time frames to one year, meaning that after the government's initial ex parte showing there would be no judicial review for one year. We think this is too long. We recommend that the current time frames be retained for the initial approval. (After all, they are already far longer than the 30 days for which criminal wiretaps, including criminal wiretaps in terrorism cases, can be approved.) If, after 90- days of electronic surveillance or 45 days of physical searches, the government can show a continuing justification for the surveillance or search authority, then we would agree that the court could authorize a longer surveillance. We would recommend one year for electronic surveillance, 180 days for physical searches (thus preserving the current law's recognition that physical searches are more problematic than electronic searches and need to be authorized for shorter periods of time).
- **Section 153. Foreign Intelligence Information**
Allows the FBI to collect evidence for criminal cases under the looser standards of foreign intelligence investigations -- an end-run around the relatively stringent requirements for wiretaps in Title III. This section, which merely changes the word "the" to "a," would actually make a fundamental change in the structure of the wiretap laws. It would permit the government to use the more lenient FISA procedures in criminal investigations which have any counter-intelligence purposes and would destroy the distinctions which justified granting different standards under FISA in the first place. Under existing law, FISA can be used only if foreign intelligence gathering is "the" purpose of the surveillance. The proposed provision would permit FISA's use if this is "a" purpose, even if the primary purpose was to gather evidence for a criminal prosecution. This is an extraordinary change in the law which has no justification.
- **Section 154. Foreign Intelligence Information Sharing**
With no standards, permits the sharing of grand jury information, Title III wiretap information, and any other "foreign intelligence information" acquired in a criminal case with many different federal officials not involved in law enforcement. This is a sweeping change in the law. "Foreign intelligence information" is not defined. The provision places no limits on the purpose for which the information may be shared, and no limit on its reuse or redisclosure. It requires no showing of need and includes no standard of supervisory review or approval. As written, a criminal investigator could share with White House staff information collected about foreign policy critics of the Administration. The provision, at the very least, should be drastically curtailed.
- **Section 155. Pen Register and Trap and Trace Authority**
Eliminates the only meaningful statutory control that exists on use of pen register and trap and trace devices in intelligence cases. The law currently requires a showing that the person being surveilled is a foreign power, an agent of a foreign power or an individual engaged in international terrorism or clandestine intelligence activities. This amendment would eliminate that standard and permit the use of FISA for pen registers whenever the government claimed that it was relevant to an ongoing intelligence investigation. Contrary to the DOJ's assertion in its section-by-section, this is not the same as the standard for pen registers in criminal cases. There, the surveillance must be relevant to an ongoing criminal investigation, which is moored to the criminal law. There is no similar constraint on foreign intelligence investigations, since they can be opened in the absence of any suspicion of criminal conduct. This provision ignores the fact that the government was granted the special rules of FISA only for situations that involved intelligence gathering about foreign powers.
- **Section 156. Business records**
Allows access to any business records upon the demand of an FBI agent, with no judicial review or oversight. Traditionally, the FBI had no ability to compel disclosure of information in intelligence investigations. The compulsory authorities were limited to criminal cases, where the open, adversarial nature of the system offered protections against abuse. For example, in criminal cases, including international terrorism cases, the FBI can obtain grand jury subpoenas, under the supervision of the prosecutor and the court, where the information is relevant to a criminal investigation. The FBI has no ability to invoke the power of the grand jury in intelligence investigations, since those investigations are conducted without regard to any suspicion of criminal activity. In 1998, in an expansion of intelligence powers, FISA was amended to give the FBI a new means to compel disclosure of records from airlines, bus companies, car rental companies and hotels: Congress created a procedure allowing the FBI to go to any FISA judge or to a magistrate. The FBI had only to specify that the records sought were for a foreign intelligence or international terrorism investigation and that there were specific and articulable facts giving reason to believe that the person to whom the records pertain is an agent of a foreign power. This is not a burdensome procedure, but it brought the compulsory process under some judicial control. The Administration's bill would repeal the 1998 changes and permit the use of "administrative subpoenas" rather than an application to a court to get any business records under FISA. An administrative subpoena is a piece of paper signed by an FBI agent. There is no judicial review, no standard of justification, no oversight. Particularly in intelligence investigations, which are not even limited by the scope of the criminal law and in which there is no involvement of the US Attorney's Office, FBI agents should not have such unreviewable discretion to compel disclosure of personal information.
- **Sec. 157. Miscellaneous national-security authorities**
Allows much greater access to banking, credit, and other consumer records in counter-intelligence investigations. Current provisions of law allow the federal government to obtain sensitive banking, credit, and other consumer records under the relaxed and secretive oversight of FISA - but only when there are "specific and articulable" facts showing that the target consumer is "a foreign power or the agent of a foreign power." Section 157 would eliminate these essential requirement, mandating disclosure of this sensitive consumer data simply if an FBI official certifies that they are needed for a counterintelligence investigation (and with an ex parte court order for access to credit reports). Section 157 would eliminate the "agent of a foreign power" standard in-
 - The Fair Credit Reporting Act, allowing access to records from consumer reporting agencies (including the names of all financial institutions where accounts are held, all past addresses and employers, and credit reports);
 - the Financial Right to Privacy Act, broadly allowing access to financial records; and
 - the Electronic Communications Privacy Act, allowing access to telephone and toll billing records, and, newly added, all "electronic communication transactional records."
 As such, the Section would greatly increase access to the personal information of consumers or groups who are not agents of foreign powers. And in each case access the institutions granting access to consumer information would be prohibited from disclosing that information or records had been obtained.

- **Section 158. Disclosure of educational records**
Amends the law protecting education records to permit access to them. While this might be justified in terrorism cases, the provision covers all cases involving "national security" and is far too sweeping.
- **Section 159. Presidential Authority. Does not appear to permit judicial challenge to seizure of property.** At the very least, there must be such opportunity. A second provision allows the use of secret evidence. Use of such evidence, if ever permitted, must be on a much higher standard than that the information is properly classified, as provided here. The government must be required to persuade a court that the disclosure to the party would result in imminent and serious harm and the court must require the government to provide sanitized information to the party.
- **Sec. 352. Notice.**
Allows secret searches through delayed notice for all warrants or court orders. For any warrant or court order to search or seize property relating to a federal criminal offense, notice of the search or seizure could be delayed if it could interfere with lawful investigations. Notice is a bedrock Fourth Amendment protection from mistaken or abusive searches and seizures. Delayed notice has been allowed in only the most extraordinary circumstances, such as wiretapping, and only with substantial judicial supervision. Section 352 represents a major erosion of this key Fourth Amendment requirement of notice.

Conclusion

Again, Mr. Chairman, and Members of the Committee, we commend you for holding this briefing. Frankly, however, given the scope of what the Administration is asking for, we do not believe that this single session is sufficient to understand many of the proposals being put forth. We urge you to seek a consensus bill, leaving for later resolution the more complex issues.

[Free Speech](#) | [Data Privacy](#) | [Government Surveillance](#) | [Cryptography](#) | [Domain Names](#) | [International](#) | [Bandwidth](#) | [Security](#) | [Internet Standards, Technology and Policy Project](#) | [Terrorism](#) | [Authentication](#) | [Right to Know](#)

[Our Mission](#) / [Get Involved](#) / [Staff](#) / [Publications](#) / [Links](#) / [Search CDT](#) / [Jobs](#) / [Action!](#)

[Our Mission](#) / [Get Involved](#) / [Staff](#) / [Publications](#) / [Links](#) / [Search CDT](#) / [Jobs](#) / [Action!](#)

[Previous Headlines](#) | [Legislative Tracking](#) | [CDT's Privacy Policy](#)



©2001 [The Center For Democracy & Technology](#)
1634 Eye Street NW, Suite 1100
Washington, DC 20006
(v) 202.637.9800
(f) 202.637.0968

Technical concerns about this site: webmaster@cdt.org
Concerns or opinions about issues: feedback@cdt.org