

**Statement of James X. Dempsey  
Executive Director  
Center for Democracy & Technology<sup>1</sup>**

**before the  
House Committee on the Judiciary  
Subcommittee on the Constitution**

**“Anti-Terrorism Investigations and the Fourth Amendment After September 11:  
Where and When Can the Government Go to Prevent Terrorist Attacks?”**

**May 20, 2003**

Mr. Chairman, Mr. Nadler, Members of the Subcommittee, thank you for the opportunity to testify today at this important hearing. We commend Chairman Sensenbrenner and Mr. Conyers and you, Chairman Chabot and Mr. Nadler, for the oversight you are conducting of the effectiveness of the nation's counter-terrorism laws and their implications for civil liberties. The Center for Democracy and Technology urges you to continue this process, and we look forward to being of assistance to you however we can. In my testimony today, I make specific suggestions for further avenues of oversight.

**I. SUMMARY**

The main points I wish to make today are these: The threat terrorism poses to our nation is imminent and grave. The government must be provided with strong legal authorities to prevent terrorism to the greatest extent possible and to punish it when it occurs. These authorities must include the ability to infiltrate organizations, collect

---

<sup>1</sup> 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 computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

information from public and private sources, and carry out wiretaps and other forms of electronic surveillance. These legal powers, however, must be subject to checks and balances; they must 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 the checks and balances, weak in some key respects before 9/11, have been seriously eroded by the PATRIOT Act and Executive Branch actions. Prior to 9/11, the government had awesome powers but failed to use them well. Those failures had little if anything to do with the rules established to protect privacy. The changes in the PATRIOT Act were hastily enacted – mistakes were made that Congress should rectify, by reasserting standards and checks and balances and by practicing ongoing, nonpartisan, detailed oversight, starting with close scrutiny of the government's claims that the PATRIOT Act changes have been vital to recent successes.

In response to the specific question posed by the title of this hearing, my central point is that, both before 9/11 and now, the government had and still has authority to go anywhere and collect any information to prevent terrorist attacks. Before 9/11, the exercise of that authority domestically was controlled and focused – the government had to have some minimal basis to suspect that some criminal conduct was being planned or that there was some minimal connection with a foreign terrorist group. Under the changes that have been made since 9/11, the FBI is authorized by the Attorney General to go looking for information about individuals with no reason to believe they are engaged in, or planning, or connected to any wrongdoing. Before 9/11, mosques and political events were not off-limits and the FBI did go into religious and political gatherings to collect information – where it had some minimal reason for believing that there was some

connection between that mosque or political meeting and terrorism. Now, FBI agents can apparently wander down the street and visit mosques or political meetings like anyone else – on a whim. Before 9/11, the FBI was not prohibited from use of commercial databases. But under the PATRIOT Act and other laws, the FBI may have the authority to scoop up entire databases of information, including data on persons suspected of no wrongdoing. Our laws are totally inadequate to deal with the reality of decentralized commercial databases and the new techniques of data mining.

Both before 9/11 and today, the only question has ever been one of standards, checks and balances and procedures. With the changes adopted since 9/11, domestic law enforcement and intelligence agencies have fewer standards to guide them and are subject to less oversight and accountability to check up on their performance. The result, I fear, is unfocused investigative activity that is bad for security and bad for civil liberties.

I will concentrate today on the surveillance issues that I understand are the Subcommittee's main interest, but for purposes of context, I must briefly mention that some of the greatest abuses of civil liberties since 9/11 do not flow from the PATRIOT Act and have not been the subject of Congressional authorization or scrutiny, including:

- secret arrests of hundreds and maybe more than 1000 people;
- the detention of many of those for days, weeks or even longer without charges, even though Congress had set a 7 day limit even for non-citizens detained as suspected terrorists;
- abuse of the material witness statute to hold people without charges;
- the blanket closing of deportation hearings;
- the indefinite detention of two American citizens in military prisons without criminal charges;
- selective targeting of immigrants for enforcement based on their religion.<sup>2</sup>

---

<sup>2</sup> Many of these abuses are detailed in the report of the Lawyers Committee for Human Rights, "Imbalance of Powers: How Changes to U.S. Law and Policy since 9/11 Erode Human Rights and Civil Liberties," [PDF] March 11, 2003, online at [http://www.lchr.org/us\\_law/loss/imbalance/powers.pdf](http://www.lchr.org/us_law/loss/imbalance/powers.pdf).

## II. US v. MILLER AND THE DRAGNET APPROACH OF SECTION 215 AND NATIONAL SECURITY LETTERS

In the 1970s, the Supreme Court issued a series of momentous decisions holding that citizens lose their constitutional rights in information provided to third parties in the course of commercial transactions. United States v. Miller, 425 U.S. 435 (1976), held that there is no constitutional privacy interest in the records held by banks showing who has paid you money, to whom you have paid money, amounts, dates, etc. Smith v. Maryland, 442 U.S. 735 (1979), held that telephone users have no constitutional privacy interest in the transactional information that shows who is calling them, whom they are calling, when, how often and for how long. Fast forward through the digital revolution, and the “business records” exception has become a gaping hole in the Fourth Amendment. Under current law, you have no constitutional privacy right in any of the data you generate as you go about your daily life, using credit cards, building access cards, or Easy Passes, making travel plans, or buying things. Taken together, the transactional data generated every time you dial your telephone, write a check, send an email, or go to the doctor can provide a full picture of your life, your work, your interests and your associations, but it is, under current law, constitutionally unprotected.

The PATRIOT Act exploited this situation, granting broad authorities beyond anything contemplated in US v. Miller or Smith v. Maryland. Section 215 of the Act amended the Foreign Intelligence Surveillance Act to authorize the government to obtain a court order from the FISA court or designated magistrates to seize “any tangible things (including books, records, papers, documents, and other items)” that an FBI agent claims are “sought for” an authorized investigation “to protect against international terrorism or

clandestine intelligence activities.” The subject of the order need not be suspected of any criminal wrongdoing whatsoever; indeed, if the statute is read literally, the order need not name any particular person but may encompass entire collections of data related to many individuals. Section 505 of the PATRIOT Act similarly expanded the government’s power to obtain telephone and email transactional records, credit reports and financial data with the use of a document called the National Security Letter (NSL), which is issued by FBI officials without judicial approval.<sup>3</sup> Sections 507 and 508 granted authority to the Attorney General or his designee to obtain a court record for disclosure of education records.

In the past, the government could obtain a person’s records from a bank, credit bureau, telephone company, hospital, or library in the course of a criminal investigation. In addition, prior to the PATRIOT Act, in international terrorism investigations, the FBI had the power to compel disclosure of credit, financial and communications records with National Security Letters and travel records under the predecessor of Section 215. However, Congress had set a straightforward and relatively low standard that required some factual predicate and particularized focus: the government had to have reason to believe that the records being sought pertained to an “agent of a foreign power” – an intelligence officer, for example, or a member of an international terrorist organization. Reason to believe is a very low standard, much lower than probable cause.

The PATRIOT Act eliminated both the “agent of a foreign power” standard and the reason to believe standard, giving the FBI access with National Security Letters to

---

<sup>3</sup> CDT has prepared a detailed memo on data mining, which discusses Section 215 and the NSLs: “Privacy’s Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data,” May 19, 2003, available online at <http://www.cdt.org>.

specific categories of records in intelligence investigations with no factual basis to believe that the records pertained to a possible terrorist. And Section 215 created a massive catch-all provision that gave the FBI the ability to compel anyone to disclose any record or tangible thing that the FBI claims is “sought in connection with” an investigation of international terrorism or “clandestine intelligence activities,” even if the record does not pertain to a suspected spy or international terrorist.

The implications of this change are enormous. Previously, the FBI could get the credit card records of anyone suspected of being a foreign agent. Under the PATRIOT Act, broadly read, the FBI can get the entire database of the credit card company. Under prior law, the FBI could get library borrowing records only with a subpoena in a criminal investigation, and generally had to ask for the records of a specific patron. Under the PATRIOT Act, broadly read, the FBI can go into a public library and ask for the records on everybody who ever used the library, or who used it on a certain day, or who checked out certain kinds of books. It can do the same at any bank, telephone company, hotel or motel, hospital, or university – merely upon the claim that the information is “sought for” an investigation to protect against international terrorism or clandestine intelligence activities.

How these provisions are actually being applied is the subject of great uncertainty, at least as far as one can tell from the public discussion to date. The DOJ and the FBI could be much more forthcoming, for example, about what they are doing in libraries. Up to now, the ambiguous statements of FBI officials have only fanned suspicion and distrust.

Congress should closely inquire into the DOJ's interpretation of Section 215 and the National Security Letter authorities. The DOJ and FBI have never actually said how they are interpreting Section 215 and the new NSL authorities. The further questions submitted by Chairman Sensenbrenner on April 1, 2003 are a good start, but the Committee should also ask: Is the DOJ interpreting and using Section 215 and the NSL authorities to obtain access to entire databases, i.e., without naming individuals to whom the records pertain? If not, why shouldn't the statute be revised to clarify the particularized suspicion standard?

I have heard it argued that these changes merely conform the intelligence standard to the criminal standard, since investigators in criminal cases can obtain anything with a subpoena issued on a relevance standard. First of all, the standard in Section 215 and two of the three NSL statutes is less than relevance – it is “sought for.” Second, a criminal case is at least cabined by the criminal code – something is relevant only if it relates to the commission of a crime. But on the intelligence side, the government need not be investigating crimes – at least for non-U.S. persons, it can investigate purely legal activities by those suspected of being agents of foreign powers. The standard for opening an investigation is far less than probable cause, and once an investigation is opened, under the PATRIOT Act changes, an agent can get anything from anyone by say “I am seeking this in connection with an open investigation.”

Moreover, there are other crucial protections applicable to criminal subpoenas that are not available under Section 215 and the NSLs. For one, third party recipients of criminal subpoenas can notify the record subject, either immediately or after a required delay. Section 215 and the NSLs prohibit the recipient of a disclosure order from ever

telling the record subject, which means that the person whose privacy has been invaded never has a chance to rectify any mistake or seek redress for any abuse. Secondly, the protections of the criminal justice system provide an opportunity for persons to assert their rights and protect their privacy, but those adversarial processes are not available in intelligence investigations that do not end up in criminal charges.

I look forward to the day when Smith v. Maryland and US v. Miller are placed in the same category as the discredited Olmstead decision of 1928 – decisions based on an unduly cramped understanding of privacy, unsuited to changing technology. Kyllo v. United States, 533 U.S. 27 (2001), the case requiring a warrant for infra-red searches of homes, showed that the Supreme Court is sensitive to ensuring that changes in technology do not render privacy. Meanwhile, Congress should statutorily re-establish the requirement of particularized suspicion and require some factual showing on the part of government officials seeking access to records.

### **III. THE NEED FOR CLOSE CONGRESSIONAL SCUTINY 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 this Committee is how the FBI 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. The FBI's Trilogy project includes plans for data mining. According to an undated FBI presentation obtained by the

Electronic Privacy Information Center, the FBI's use of "public source" information (including proprietary commercial databases) has grown 9,600% since 1992.<sup>4</sup>

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? This week, the Defense Department will be releasing a report on the Total Information Awareness ("TIA") project at the Pentagon's Defense Advanced Research Projects Agency ("DARPA"), which hopefully will illuminate some of these issues. Among the questions to be asked specifically of the FBI is how the PATRIOT Act authorities discussed above and the changes in the FBI guidelines discussed below might relate to its data mining plans.

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 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 to government uses of commercial databases is one way to look at setting guidelines for data mining. But some of the principles are simply inapplicable and others need to have greater emphasis. For example, perhaps one of the most important elements of guidelines for data mining would be rules on the interpretation and

---

<sup>4</sup> <http://www.epic.org/privacy/publicrecords/cpfbippt.pdf>.

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 moving forward with implementation. 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.

#### **IV. THE FBI GUIDELINES: IMPACT ON CIVIL LIBERTIES AND SECURITY - THE NEED FOR CONGRESSIONAL OVERSIGHT AND RE-ESTABLISHMENT OF MEANINGFUL LIMITS**

On May 30, 2002, Attorney General John Ashcroft issued revised Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (“Domestic Guidelines”). The Attorney General claimed that the changes were necessary to free the FBI from unnecessary constraints in the fight against international terrorism. Yet the guidelines the Attorney General changed were not applicable to international terrorism. And the types of things the Attorney General said he wanted to permit – visiting mosques, surfing the Net – were never prohibited under the old guidelines.

The FBI is subject to two sets of guidelines, a classified set for foreign intelligence and international terrorism investigations (“International Terrorism Guidelines”), and an unclassified set on general crimes, racketeering and domestic terrorism.<sup>5</sup> Last year, the Attorney General changed the Domestic Guidelines. He has not yet changed the International Guidelines, which relate to investigations of Osama bin Laden and Al Qaeda. (The Department of Justice may be reviewing the International Guidelines. This Committee should find out what is going on and insist on being fully consulted.) The International Terrorism Guidelines in some ways give the FBI even more latitude than the domestic guidelines. The irony is that the FBI’s failed investigations of the Osama bin Laden group were conducted under those looser guidelines, reinforcing the conclusion that the problem before 9/11 was not the limits imposed by law or policy but the failure of the FBI to use the authority and information it already had.

-- **The Role of Congress**

In the 1960s, the FBI conducted wide-ranging investigations and neutralization efforts against non-violent activity across the political spectrum. While there were acts of violence being carried out on America’s streets, the FBI’s COINTELPRO program and

---

<sup>5</sup> The old domestic guidelines are at <http://www.usdoj.gov/ag/readingroom/generalcrimea.htm>. A heavily redacted copy of the international guidelines can be downloaded in PDF from <http://www.usdoj.gov/ag/readingroom/terrorismintel2.pdf>. Both sets of guidelines relate to investigations in the United States. The difference between the two sets of guidelines has to do with the nature of the organization being investigated. The foreign guidelines govern investigations inside the United States of international terrorism organizations (such as al Qaeda or Hamas), groups that originate abroad but carry out activities in the US, and their agents. In the past, the domestic guidelines governed investigations of terrorist groups that originate in the US – e.g., white supremacists and animal rights activists.

related efforts focused on politics. The exercise was essentially worthless from a security standpoint: it produced no advanced warning of any violent activity. By the mid-70s, there was a reaction against this approach, within the Justice Department, the FBI itself, the Congress and the public at large. Internal and external investigations of the abuses led to the adoption of guidelines by Attorney General Edward Levi, which set standards for FBI "domestic security" investigations.

The initial issuance and subsequent major revisions of the FBI Guidelines were undertaken in conjunction with Congressional consultation and oversight. In effect, the Guidelines had a "quasi-legislative" status. Indeed, the Guidelines were adopted in lieu of legislation. A major debate in the 1970s was over the framing of a statutory charter for the FBI. (The CIA has a legislative charter; the FBI does not.) After Attorney General Levi issued the guidelines, Congress dropped the push for a legislative charter, based on two grounds: (i) Executive Branch claims that the guidelines embodied all the protections that would be included in a charter but did so with greater detail, providing just the right mix of guidance and flexibility to the FBI, and (ii) the understanding that Guideline changes would be subject to prior Congressional review and public input. Every subsequent Attorney General (except Attorney General Ashcroft) consulted with this Committee on guidelines changes. When Attorney General William French Smith undertook major revisions of the guidelines at the beginning of the Reagan Administration, the effort was accompanied by over a year of consultation, public debate, and Congressional hearings. Never before has an Attorney General undertaken major revisions to the FBI Guidelines without any prior consultation with the relevant Committees of Congress.

-- **Major Concerns with the Changes**

A major change brought about by the Ashcroft Guidelines is that they authorize investigative activity in the absence of any indication of criminal conduct. The central feature of the Levi/Smith/Thornburgh guidelines was the criminal standard: the FBI could initiate a full domestic counter-terrorism investigation when facts and circumstances reasonably indicated that two or more people were engaged in an enterprise for the purpose of furthering political goals through violence. FBI agents could conduct quite intrusive preliminary investigations on an even lower standard. The old guidelines allowed FBI agents to go into any mosque or religious or political meeting if there was reason to believe that criminal conduct was being discussed or planned there, and, in fact, over the years the FBI conducted terrorism investigations against a number of religious organizations and figures, ranging from the white supremacist Christian Identity Movement to the African-American Church of Yahweh. Separate guidelines even allowed undercover operations of religious and political groups, subject to close supervision.

Under the Levi/Smith/Thornburgh guidelines, once an investigation or even a preliminary inquiry was opened, the FBI could use any and all public source information (including the Internet) to collect personally-identifiable information relevant to the investigation. In fact, an investigation could consist solely of the collection of newspaper articles and Internet material and the indexing of that information by name. The evidence could in fact consist largely or exclusively of information about the exercise of First Amendment rights. The only requirement was that there first had to be some minimal reason to believe that something illegal was being planned.

Now, the FBI is cut loose from that standard, with no indication as to how it should prioritize its efforts or avoid chilling First Amendment rights.

**Visiting Religious and Political Meetings** -- The new guidelines purport to give the FBI authority to attend public meetings of a religious or political nature, without any scintilla of suspicion of criminal or terrorist activity. The problem is compounded by poor guidance on what can be recorded and the lack of time limits on the retention of data acquired.

In the past, under the Domestic Guidelines, the FBI was guided by the criminal nexus – in deciding what mosques to go to and what political meetings to record, it had to have some reason to believe that terrorism might be discussed. Under the new guidelines, even before opening a preliminary inquiry, the FBI can go to mosques and political meetings. How will it decide which ones to go to? We fear it will be on the basis of politics, religion, or ethnicity.

**Should FBI Agents Surf the Net Like Teenagers?** -- According to justifications issued by the DOJ with the new guidelines, FBI agents previously could not conduct online searches under the term "anthrax," even after the initial appearance of the anthrax letters. That is absurd - there was an ongoing investigation. Anyhow, no privacy rights or civil liberties are implicated in searches - before or after the appearance of the anthrax letter - for words like "anthrax." That is not what the guidelines were about. The question is whether the FBI can make searches for "Palestinian rights" or other terms with a political, ethnic or religious significance, as the starting point for an investigation. The change either authorizes politically guided investigations or it authorizes fishing expeditions

**Pursuing Investigations That Turn Up Nothing** -- Finally, the revisions decreased the internal supervision and coordination at various stages of investigation, in particular expanding the scope and duration of preliminary inquiries (by definition, these are cases that are opened on *less than* reasonable indication of criminal or terrorist conduct), encouraging the use of more intrusive techniques with no sense of prioritization and allowing intrusive investigations to go on for periods without producing results and without internal review or any outside or independent scrutiny.<sup>6</sup>

Preliminary inquiries can use all techniques except two: mail openings and wiretaps. This means that the FBI can use informants, Internet searches, undercover operations, and physical and photographic surveillance. Under the old guidelines, if 90 days of investigation turned up no indication of criminal activity, the investigation could be continued only with HQ approval. Under the new guidelines, preliminary inquiries can continue 1 year without HQ approval. This means that the FBI can conduct an investigation, using highly intrusive techniques, for one year (and longer with HQ approval) even if the investigation is turning up no reasonable indication of criminal activity.

Broadening the FBI's surveillance authority threatens civil liberties and wastes resources while increasing the risk of intelligence failures. The salient identifiable cause

---

<sup>6</sup> The period for preliminary inquiries with no supervisory review has increased from 90 to 180 days. Preliminary inquiries may go on for up to one year without notifying Headquarters. While the time limitations have increased, the levels of authorization have decreased. Authority for extensions in preliminary inquiries – cases that are producing no reasonable indication of criminal conduct - has been reduced from FBI Headquarters to a Special Agent in Charge. Likewise, authority for the initiation and review of full investigations has been reduced from a Director or Assistant Director to a Special Agent in Charge.

of the September 11 intelligence failure was the inability of the FBI and other agencies to use the information they already had. The guidelines are likely to compound that defect, thereby producing no improvement in security.

-- **Congressional Oversight is Necessary**

Consistent Congressional oversight is vital to protect our security and our civil liberties. Attorney General Ashcroft changed the FBI Guidelines with the stroke of a pen without prior notice or consultation with Congress. This is not only unprecedented, but does not bode well for Congressional oversight over FBI activity to ensure both protection of constitutional rights and success in the fight against terrorism.

In responding to the issues raised by the guideline changes, we recommend the following steps:

- Require through appropriations language prior notice and meaningful consultation before future guideline changes can take effect, including changes in the International Guidelines
- Require the adoption, following Congressional consultation and comment, of Guidelines for collection, use, disclosure and retention of public event information. Such guidelines should include a provision specifying that no information regarding the First Amendment activities of a US person or group composed substantially of US persons can be disseminated outside the FBI except as part of a report indicating that such person or group is planning or engaged in criminal activity.
- Provide resources and authority to the General Accounting Office and the DOJ Inspector General to collect and analyze information on implementation of the anti-terrorism guidelines and to submit to Congress public and classified reports on their

impact on an open society, free speech, and privacy and benefits and costs to national security.

## **V. RECTIFYING FLAWS IN THE SURVEILLANCE LAWS**

We should not lose sight of the fact that before the PATRIOT Act there were concerns that the checks and balances in the surveillance laws were insufficient. As a result of the digital revolution more information is more readily available to government investigators than ever before. The judges have not aggressively regulated electronic surveillance. Last year, only one government application for electronic surveillance was turned down. For each of the prior three years (1999-2001), not a single judge anywhere in the country, state or federal, turned down a single request for surveillance in any case, criminal or intelligence. The minimization requirement has been judicially eviscerated. The Congress could start by taking up the helpful changes to surveillance law developed and passed by the House Judiciary Committee in the 106th Congress, under H.R. 5018, including:

- Heightened protections for access to wireless location information, requiring a judge to find probable cause to believe that a crime has been or is being committed. Today tens of millions of Americans are carrying (or driving) mobile devices that could be used to create a detailed dossier of their movements over time - with little clarity over how that information could be accessed and without an appropriate legal standard for doing so.
- A meaningful standard for use of expanded pen registers and trap and trace capabilities, requiring a judge to at least find that specific and particularly facts

reasonably indicate criminal activity and that the information to be collected is relevant to the investigation of such conduct.

- Addition of electronic communications to the Title III exclusionary rule in 18 USC §2515 and add a similar rule to the section 2703 authority and the pen register and trap and trace authority. This would prohibit the use in any court or administrative proceeding of email or other Internet communications intercepted or seized in violation of the privacy standards in the law.
- Require high-level Justice Department approval for applications to intercept electronic communications, as is currently required for interceptions of wire and oral communications.
- Require statistical reports for §2703 disclosures, similar to those required by Title III.

Beyond these changes, there are issues raised by the PATRIOT Act that need to be addressed:

- Require more extensive public reporting on the use of FISA, to allow better public oversight.
- Make the use of FISA evidence in criminal cases subject to the Classified Information Procedures Act.
- Limit the use of secret searches.

## **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. Legal standards should focus on perpetrators of crime, avoid indulging in guilt by association, maintain procedures designed to identify the guilty and exonerate the innocent, insist on limits on surveillance authority, and bar political spying.

For more information, contact:

Jim Dempsey  
(202) 637-9800 x112  
[jdempsey@cdt.org](mailto:jdempsey@cdt.org)  
<http://www.cdt.org>