

**Statement of Viet D. Dinh
Assistant Attorney General,
Office of Legal Policy
United States Department of Justice
Subcommittee on the Constitution
Committee on the Judiciary
United States House of Representatives**

May 20, 2003

Good afternoon, Mr. Chairman and Members of the Subcommittee. I appreciate the chance to testify today about the Justice Department's ongoing efforts to protect the lives of innocent Americans, and our commitment to doing so within the limits of the Fourth Amendment's guarantee of individual privacy. After 9/11, the Attorney General gave me a simple yet powerful directive: "Think outside the box, but never outside of the Constitution." Those instructions have been the Department's guidepost ever since.

In the 20 months since the atrocities of September 11, 2001, this Administration and Congress have worked hard to give our men and women in blue the tools they need to keep America safe, such as the USA PATRIOT Act and the revised Attorney General's investigative guidelines. Each of these new authorities incorporates long-settled precedent from the Supreme Court regarding privacy rights and other constitutional norms. In many cases, these new tools simply enable officials to use information to which other government entities already have access. In other instances, they give agents permission to use information that already is available to other members of the public.

This afternoon, I will discuss three matters that I hope will be of use to the Subcommittee. First, I will trace the development of Fourth Amendment jurisprudence to the contemporary understanding that it protects individual privacy. Second, I will discuss how the USA PATRIOT

Act gave terrorism investigators access to information that other government officials already possess or lawfully could possess – in particular, how the Act encouraged the sharing of information and coordination among intelligence and law-enforcement personnel; and how the Act enabled courts to subpoena business records in *all* investigations, not just routine criminal cases. Third, I will discuss how the USA PATRIOT Act and Justice Department policies have enabled investigators to collect information that terrorism suspects voluntarily have disclosed to other members of the general public – in particular, how the revised Attorney General’s investigative guidelines gave law enforcement the same access to public places and information that all other Americans enjoy; and how the Act facilitated the gathering of non-private routing and addressing information about electronic communications.

The Fourth Amendment from Trespass to Privacy

Over the course of the twentieth century, the Fourth Amendment came to be understood as protecting certain forms of individual privacy – what Justice Brandeis called the “right to be let alone – the most comprehensive of rights and the right most valued by civilized men”¹ – not just as preventing unauthorized government trespass onto landowners’ private property.

The traditional “trespass” conception of the Fourth Amendment is typified by the 1928 case *Olmstead v. United States*.² In holding that law enforcement did not carry out an “unreasonable search or seizure” when it conducted a warrantless telephone wiretap, the Supreme Court reasoned that “[t]he evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.”³ According to the

¹ *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

² 277 U.S. 438 (1928).

³ *Id.* at 464.

Court, no trespass, no violation. But *Olmstead* also contained the seeds of a new understanding of the Fourth Amendment. In dissent, Justice Brandeis emphasized that “[s]ubtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.”⁴

Less than four decades later, in *Katz v. United States*,⁵ the Supreme Court held that warrantless government wiretapping can constitute an unreasonable search or seizure. The Court effectively adopted Justice Brandeis’s “privacy” reading of the Fourth Amendment: “[T]he Fourth Amendment protects people, not places.”⁶ In response to *Katz*, Congress enacted Title III of the 1968 Omnibus Crime Control and Safe Streets Act,⁷ which governs electronic surveillance for federal criminal offenses. Congress subsequently enacted the Electronic Communications Privacy Act (“ECPA”), which addresses government access to stored communications,⁸ and establishes statutory standards and procedures for the use of pen registers and trap and trace devices.⁹

Katz left open the question what standards and procedures apply to government surveillance in national-security investigations.¹⁰ But in the 1972 *Keith* decision,¹¹ the Supreme Court squarely held that the Fourth Amendment is applicable in domestic-security investigations:

⁴ *Id.* at 478 (Brandeis, J., dissenting).

⁵ 389 U.S. 347 (1967).

⁶ *Id.* at 351.

⁷ 18 U.S.C. §§ 2510-22.

⁸ *Id.* §§ 2701-12.

⁹ *Id.* §§ 3121-27.

¹⁰ *See Katz*, 389 U.S. at 358 n.23 (“Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.”).

¹¹ *United States v. United States District Court (“Keith”)*, 407 U.S. 297 (1972).

We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.¹²

At the same time, the *Keith* Court emphasized that different rules could be appropriate in national-security investigations – including cases of terrorism – than the standard procedures for criminal investigations:

Given [the] potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.¹³

In 1978, Congress responded to the Court's invitation by enacting the Foreign Intelligence Surveillance Act ("FISA").¹⁴ FISA establishes standards applicable to surveillance of foreign powers and agents of foreign powers – including electronic surveillance, physical searches, and use of pen registers and trap and trace devices – in relation to the investigation of such matters as international terrorism and espionage.

Facilitating Information Sharing and an Integrated Antiterrorism Campaign

One of the USA PATRIOT Act's most important innovations was the amendments it made to FISA, which allow national-security personnel and their law-enforcement counterparts to coordinate their efforts to keep America safe. Acts of terrorism are simultaneously criminal offenses and threats to our national security. Our response likewise must transcend the boundaries of an organizational chart.

¹² *Id.* at 320.

¹³ *Id.* at 322.

¹⁴ 50 U.S.C. §§ 1801-62.

Before the USA PATRIOT Act, a metaphorical “wall” between the intelligence community and federal law enforcement often precluded vital information sharing. This wall, which derived from certain court decisions,¹⁵ was established in written Department guidelines in July 1995. Under this interpretation, FISA could be used only if the “primary purpose” of an investigation was to protect the national security; evidence could be gathered to prosecute a foreign terrorist only if that purpose was clearly secondary. While information could be “thrown over the wall” from intelligence officials to prosecutors, the decision to do so always rested with national-security personnel – even though law enforcement agents pursuing a criminal investigation are in a better position to determine what evidence is pertinent to their case. These legal rules created what the Foreign Intelligence Surveillance Court of Review has termed “perverse organizational incentives,” expressly discouraging cooperation in the fight against terrorism.¹⁶ With apologies to Robert Frost, “[s]omething there is that doesn’t love a wall.”¹⁷

The USA PATRIOT Act finally permitted the coordination between intelligence and law enforcement that is vital to protecting the nation’s security. Specifically, section 218 displaced the outmoded “primary purpose” standard, allowing the use of FISA when a “significant purpose” of an investigation is foreign intelligence. The Justice Department since has developed procedures to allow the use of certain FISA-derived information in criminal prosecutions. And on November 18, 2002 the FISA Court of Review held that these procedures are consistent with

¹⁵ See, e.g., *United States v. Truong*, 629 F.2d 908 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982).

¹⁶ See *In re Sealed Case*, 310 F.3d 717, 743 (FISCR 2002).

¹⁷ Robert Frost, *Mending Wall*, reprinted in *THE NEW OXFORD BOOK OF AMERICAN VERSE* 395-96 (R. Ellmann ed. 1976).

the Fourth Amendment, reasoning “that FISA as amended is constitutional because the surveillances it authorizes are reasonable.”¹⁸

Both before and since the Court of Review’s decision, the Justice Department has fostered extensive cooperation among national-security and law-enforcement personnel. The Attorney General instructed all United States Attorneys to review their intelligence files, with the intent of discovering whether there was a basis to bring criminal charges against the subjects of intelligence investigations. On October 1, 2002, the Attorney General directed every U.S. Attorney to develop a plan to monitor terrorism and intelligence investigations, and to ensure that information about terrorist threats is shared with other agencies and that criminal charges are considered. Almost 4,500 intelligence files have been reviewed as part of this process, and information from this review has been incorporated in numerous cases.

The USA PATRIOT Act’s revisions to FISA already are producing important dividends in the war on terror. Department of Justice prosecutors recently were able to obtain the indictment of Sami al-Arian, an alleged member of a Palestinian Islamic Jihad (PIJ) cell in Tampa, Florida. PIJ is alleged to be one of the world’s most violent terrorist outfits, and is responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. Section 218 of the USA PATRIOT Act, as well as the Department’s implementing rules, enabled criminal investigators finally to obtain and consider systematically the full range of evidence of the PIJ operations in which al-Arian allegedly participated.

¹⁸ *Id.* at 746.

Enabling Courts to Subpoena Records in All Types of Investigations

In the same way that national-security officers must be allowed to coordinate their antiterrorism efforts with law-enforcement personnel, the Department firmly believes that terrorism investigators must be able to use the same tools available in routine criminal investigations. For that reason, section 215 of the USA PATRIOT Act authorized courts in terrorism and national-security cases to subpoena business records – which have long been available in ordinary criminal investigations.

For years, grand juries investigating ordinary crimes have been able to issue subpoenas to all manner of businesses. In the 1997 Gianni Versace murder investigation, a Florida grand jury subpoenaed records from public libraries in Miami Beach.¹⁹ In the Unabomber case during the mid-1990s, federal grand juries reportedly wanted to learn who had checked out the four books cited in the “Unabomber Manifesto,” and therefore subpoenaed records from a number of university libraries on the west coast.²⁰ And in the 1990 Zodiac gunman investigation, a grand jury in New York subpoenaed records from a public library in an effort to learn who had checked out books written by a Scottish occult poet believed to be the gunman’s inspiration.²¹

Section 215 simply authorized the FISA court to issue similar orders in national security investigations. These judicial orders conceivably could issue to bookstores or libraries but section 215 certainly does not single them out. The words “library” and “bookstore” appear nowhere in the USA PATRIOT Act. Nevertheless, libraries and bookstores should not be allowed to become safe havens for terrorists.

¹⁹ See Lydia Martin, *Agents Seek Cunanan Link to Missing Library Book*, MIAMI HERALD, July 24, 1997, at A19.

²⁰ See Gary Marx and Peter Kendall, *Unabomber Path Leads back to Utah*, CHICAGO TRIBUNE, Sept. 25, 1995, at 1.

²¹ See *Library Files Checked In Zodiac Investigation*, N.Y. TIMES, July 18, 1990, at B4.

Moreover, the USA PATRIOT Act goes to great lengths to protect the privacy rights of libraries, other affected entities, and their patrons. First, the FBI cannot obtain records under section 215 unless it receives a court order. Agents cannot unilaterally force people to turn over any information; they must appear before a court and convince it that they need the records.²² Second, section 215 has an extremely narrow scope. It can only be used in international terrorism and espionage investigations; it is not available to investigate ordinary crimes, or even domestic terrorism.²³ Third, section 215 expressly protects the First Amendment, banning the FBI from using the exercise of First Amendment rights as a pretext for seeking records.²⁴ Fourth, and finally, section 215 provides for thorough congressional oversight. Every six months, the Attorney General is required to “fully inform” Congress on how it is being used.²⁵ The Justice Department furnished Congress with the required information most recently on December 31, 2002.

Allowing Law Enforcement Equal Access to Public Information

FBI agents should have the same access to public places, events, and information that all other members of the general public enjoy. If terrorists open their meetings to the public, FBI agents ought to be able to accept the invitation. And if a child can use the internet to look up information that is relevant to potential terrorist activity, the FBI should be able to do the same. The revised Attorney General’s investigative guidelines eliminated these counterproductive

²² See 50 U.S.C. § 1861(b)(1), (c)(1).

²³ See *id.* § 1861(b)(2).

²⁴ See *id.* § 1861(a)(1), (a)(2)(B).

²⁵ *Id.* § 1862.

restrictions that prevented federal law enforcement from collecting information that was already in the public domain.

Under the old guidelines, there was no clear authority for agents to attend events held open to the general public – for example, meetings, speeches, and demonstrations – unless they already had obtained evidence that some sort of criminal activity was afoot. The old guidelines likewise generally barred the FBI from accessing publicly available information on the internet except when investigating a specific case. Thus, for example, during the fall 2001 anthrax investigation, an FBI agent might have been able to log on to an internet site to gather information about anthrax – but could not have accessed the same web page to gather information about another biotoxin such as smallpox.

The revised guidelines, issued in May 2002, represent a significant step forward in the war on terrorism. These new rules make explicit that an FBI agent may visit any public place to which members of the general public are invited, unless the Constitution or a federal law prohibits them from doing so, for the specific purpose of detecting or preventing terrorism:

For the purpose of detecting or preventing terrorist activities, the FBI is authorized to visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally. No information obtained from such visits shall be retained unless it relates to potential criminal or terrorist activity.²⁶

The guidelines also strengthen the FBI's intelligence-gathering capabilities by making plain that agents may access public information online, even when not linked to a particular criminal investigation, for the purpose of detecting or preventing terrorism:

²⁶ The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, Part VI.A.2.

The FBI is authorized to carry out general topical research, including conducting online searches and accessing online sites and forums as part of such research on the same terms and conditions as members of the public generally.²⁷

For the purpose of detecting or preventing terrorism or other criminal activities, the FBI is authorized to conduct online search activity and to access online sites and forums on the same terms and conditions as members of the public generally.²⁸

The new guidelines contain a number of safeguards designed to preserve First Amendment, Fourth Amendment, and other constitutional norms. First, FBI agents may visit a public event or conduct internet research under the new authorizations only “on the same terms and conditions as members of the public generally.”²⁹ Next, agents may conduct such visits only for a single, narrow purpose: “detecting or preventing terrorist activities.”³⁰ Third, agents are expressly prohibited from keeping any information from these visits “unless it relates to potential criminal or terrorist activity.”³¹ Fourth, agents may not use these new authorities to keep files on people on the basis of their constitutionally protected activities.³² Next, the guidelines stress that investigative activities may not be based solely on persons’ exercise of their legal rights.³³ Sixth, and finally, the guidelines specifically order agents to comply with all relevant laws, including the Constitution, when conducting all investigations³⁴

The revised Attorney General’s guidelines fit comfortably within the Supreme Court’s long-settled jurisprudence that there is no reasonable expectation of privacy in information

²⁷ *Id.* Part VI.B.1.

²⁸ *Id.* Part VI.B.2.

²⁹ *Id.* Part VI.A.2; *id.* Part VI.B.2.

³⁰ *Id.* Part VI.A.2

³¹ *Id.*

³² *Id.* Part VI.C.1

³³ *Id.* Part I.

³⁴ *Id.* Introduction, § C.

voluntarily turned over to third parties. In fact, the Supreme Court has already held that government observation of public places is consistent with the First and Fourth Amendments. In *Laird v. Tatum*,³⁵ the Court held that the Army did not unconstitutionally “chill” the plaintiffs’ exercise of their First Amendment rights by collecting publicly available information about potential insurrections and other civil disturbances. The Court found especially significant the fact that the Army gathered information from “the news media and publications in general circulation,” as well as from “agents who attended meetings that were open to the public.”³⁶ As is true under the new guidelines, “the information gathered is nothing more than a good newspaper reporter would be able to gather by attendance at public meetings and the clipping of articles from publications available on any newsstand.”³⁷

Enabling the Collection of Non-Private Information About Internet Communications

Courts must be able to allow law enforcement to track the communications of terrorists regardless of which medium they choose to use. No one type of communication should be beyond the reach of court-approved, and Fourth Amendment sanctioned, surveillance. That is why section 216 of the USA PATRIOT Act has proven to be one of the most vital new authorities in the war on terrorism. Section 216 clarified that courts can authorize the use of “pen registers” and “trap and trace devices” – which track the numbers a particular telephone dials or receives – to obtain the same sort of routing and addressing information about internet communications. By law, pen/trap devices cannot be used to collect the content of communications.

³⁵ 408 U.S. 1, 6 (1972).

³⁶ *Id.* at 6.

³⁷ *Id.* at 9 (citation omitted).

Almost a quarter of a century ago, the Supreme Court squarely held, in the context of telephone surveillance, that the use of pen/trap devices does not constitute a “search” within the meaning of the Fourth Amendment. This is so because “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,” and “when he used his phone, petitioner voluntarily conveyed numerical information to the telephone company.”³⁸ The same is true of internet communications, in which routing and addressing information is voluntarily disclosed to internet service providers. As a result, nothing in the Constitution requires law enforcement to establish probable cause, or obtain a court order, before using a pen/trap device. (Congress, by statute, has established procedural requirements that exceed those imposed by the Fourth Amendment.³⁹)

Since the USA PATRIOT Act became law in October 2001, Justice Department field investigators and prosecutors have used the amended pen/trap statute in a number of terrorism and other criminal cases. Section 216 was used in the investigation of the murder of *Wall Street Journal* reporter Daniel Pearl, to obtain information that proved critical to identifying some of the perpetrators. It also has been used to collect routing information about the internet communications of (1) terrorist conspirators; (2) at least one major drug distributor; (3) thieves who obtained victims’ bank account information and stole the money; (4) a four-time murderer; and (5) a fugitive who fled on the eve of trial using a fake passport.

Section 216 has proven as effective at safeguarding Fourth Amendment values as it has at bringing terrorists to justice. The USA PATRIOT Act preserved all pre-existing statutory

³⁸ *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

³⁹ *See* 18 U.S.C. §§ 3121-27.

standards: now, as before, law enforcement must get court approval before installing a pen register.⁴⁰ And now, as before, law enforcement must show that the information sought is relevant to an ongoing investigation.⁴¹

In fact, the USA PATRIOT Act's revisions to the pen/trap statute actually have *enhanced* privacy protections. The Act made explicit what was already implicit in the prior provision, namely, that an agency deploying a pen/trap has an affirmative obligation to use "technology reasonably available to it" that restricts the information obtained "so as not to include the contents of any wire or electronic communications."⁴² The Act also made explicit that a pen/trap is not to be viewed as an affirmative authorization for the interception of content: "such information shall not include the contents of any communication."⁴³

The Justice Department is committed to complying with the USA PATRIOT Act's mandate that law enforcement not use pen registers to capture the content of communications. On May 24, 2002, the Deputy Attorney General issued a memorandum to field offices instructing them on how to prevent "overcollection" – i.e., the inadvertent gathering of communication content – when using pen/trap devices. In particular, he ordered that:

(1) law enforcement must "operate a pen register or trap and trace device in a manner that, to the extent feasible with reasonably available technology, will minimize any possible overcollection while still allowing the device to collect all of the limited information authorized";

(2) if "an agency's deployment of a pen register does result in the incidental collection of some portion of 'content,' it is the policy of this Department that such 'content' may not be used for any affirmative investigative purpose, except

⁴⁰ See *id.* § 3123(a)(1).

⁴¹ See *id.* § 3122(b)(2).

⁴² *Id.* § 3123(c).

⁴³ *Id.* § 3127(3).

in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to the national security”]; and

(3) “The Assistant Attorney General for the Criminal Division (AAG) should ensure that the Criminal Division provides appropriate guidance, through amendments to the United States Attorneys’ Manual or otherwise, with respect to any significant general issues concerning what constitutes the ‘content’ of a communication.”⁴⁴

The Deputy Attorney General’s directive will help guarantee effective implementation of section 216, while protecting the privacy of internet users by ensuring that only addressing information – and not the content of their communications – is collected and used.

The Justice Department’s mission since the September 11 terrorist attacks has been as clear as it is essential: preserving the lives of innocent Americans along with the constitutional rights and liberties that make us as a people the envy of the world. In particular, we have dedicated ourselves to ensuring that all efforts to gather information about potential deadly terrorist attacks comply with the strictures of the Fourth Amendment’s guarantee of individual privacy. Together with Congress, we have given investigators access to terrorism-related information that other governmental entities already have acquired, or lawfully could acquire. And we have enabled law enforcement to make use of information that can be retrieved by anyone in the public domain.

On behalf of the Administration, I thank you for your commitment to keeping America both safe and free, and we look forward to continuing our partnership. I would be happy to answer any questions that you may have.

⁴⁴ Memorandum from Deputy Attorney General Larry D. Thompson Re: Avoiding Collection and Investigative Use of “Content” in the Operation of Pen Registers and Trap and Trace Devices, at 4-5 (May 24, 2002).